International Zurich Seminar on Communications
February 29 – March 2, 2012
Sorell Hotel Zürichberg, Zurich, Switzerland

Proceedings
Acknowledgment of Support

The International Zurich Seminar on Communications (IZS) is organized jointly by the IEEE Switzerland Chapter on Digital Communication Systems and the Department of Information Technology and Electrical Engineering of ETH Zurich.
Conference Organization

General Co-Chairs
Helmut Bölcskei and Amos Lapidoth

Technical Program Committee

Ezio Biglieri                          Nikolai Nefedov
Pierre Chevillat                      Bernhard Plattner
Bernard Fleury                        Igal Sason
Martin Hänggi                        Jossy Sayir
Walter Hirt                          Giorgio Taricco
Gerhard Kramer                       Emre Telatar
Frank Kschischang                    Emanuele Viterbo
Hans-Andrea Loeliger                  Pascal Vontobel
Stefan Mangold                       Michèle Wigger
Thomas Mittelholzer                  Armin Wittneben
Stefan Moser                         Raymond Yeung

Organizers of Invited Sessions

Emmanuel Abbe                        Emanuele Viterbo
Uri Erez                             Michèle Wigger
Ioannis Kontoyiannis

Local Organization

Conference Secretaries               Web and Publications
Rita Hildebrand                      Michael Lerjen
Silvia Tempel


Table of Contents

Keynote Talks

**Wed 09:00 – 10:00**  
*Gerhard Kramer, TU München*  
Progress on Relaying and Noisy Network Coding

**Thu 09:00 – 10:00**  
*Peter Winzer, Alcatel-Lucent*  
Spatial Multiplexing and MIMO for Fiber Capacities beyond 100 Tb/s

**Fri 09:00 – 10:00**  
*Mitchell Trott, HP Labs*  
Why is Wyner-Ziv coding for video so difficult?

Session 1  
Invited session organizer: Michèle Wigger

*The Multiple Access Channel with Correlated Sources and Cribbing Encoders….  8  
E. Amir and Y. Steinberg

*The Source Coding Side of Secrecy  11  
P. Cuff

*A Comparative Study of Cooperation for the Two-User Interference Channel  12  
D. Tuninetti

*Refinement of the Random Coding Bound  15  
Y. Altuğ and A. B. Wagner

*Source Coding with Side-Information at the Receivers and an Application  19  
M. Wigger

Session 2: Shannon Theory  
Chaired by Michael Gastpar

On Gaussian Channels with MMSE Interference  20  
R. Bustin and S. Shamai (Shitz)

On the Gaussian Listening-Helper Source-Coding Problem  24  
S. I. Bross and H. Permuter

*Invited papers are marked by an asterisk.*
Upper-Bounding Rate Distortion Functions based on the Minimum Mean-Square Error ................................................................. 28
M. Dörpinghaus, M. Rüngeler, and R. Mathar

On the Information Loss in Memoryless Systems: The Multivariate Case ........ 32
B. C. Geiger and G. Kubin

One-Bit Quantizers for Fading Channels ......................................................... 36
T. Koch and A. Lapidoth

Session 3 Wed 15:30 – 16:50
Invited session organizer: Ioannis Kontoyiannis

*Model Switching and other Unconventional Fun with Experts ................. 40
S. de Rooij

*Some Old and New Relations between Information and Estimation .......... 43
K. Venkat and T. Weissman

*Polar Martingales of Maximal Spread .................................................. 44
E. Abbe

*Sumset Differential Entropy Bounds ...................................................... 48
I. Kontoyiannis

Session 4 Thu 10:20 – 12:00
Invited session organizer: Emmanuel Abbe

*Latest and Greatest on Spatially Coupled Codes
R. Urbanke

*Coding Theory and Compressed Sensing through Convex Relaxations ........ 49
A. Saber Tehrani and A. G. Dimakis

*Hybrid Coding
Y.-H. Kim

*Polar Coding
E. Telatar

*Competitive Classification
A. Orlitsky

Session 5: Coding I Thu 13:20 – 15:00
Chaired by Hans-Andrea Loeliger

Polar Codes for the Deterministic Broadcast Channel .............................. 51
N. Goela, E. Abbe, and M. Gastpar
Polar Codes for Coordination in Cascade Networks................................. 55
R. Blasco-Serrano, R. Thobaben, and M. Skoglund

Polar Codes for Degraded Relay Channels........................................... 59
M. Karzand

Unambiguous Decoding of Generalized Reed–Solomon Codes beyond Half the
Minimum Distance................................................................. 63
A. Zeh, A. Wachter, and M. Bossert

Iteration-Constrained Design of IRA Codes.......................................... 67
A. Grant, I. Land, and G. Wang

Session 6: Coding II Thu 15:30 – 17:10
Chaired by Alex Grant

The Relation between Block Length and Reliability for a Cascade of AWGN
Links....................................................................................... 71
R. Subramanian

Secure Multiplex Coding over Interference Channel with Confidential Mes-
sages................................................................. 75
X. Li and R. Matsumoto

Polymer Expansions for Cycle LDPC Codes........................................ 79
N. Macris and M. Vuffray

Factoring Linear Trellises................................................................. 83
D. Conti and N. Boston

Information Theoretic Authentication and Secrecy Codes in the Splitting Model... 87
M. Huber

Session 7 Fri 10:20 – 12:00
Invited session organizer: Uri Erez

*Anti-Structure Problems................................................................. 91
R. Zamir

*Real-Time Coding of Markov Sources over Erasure Channels: When is Binning
Optimal?..................................................................................... 95
A. Khisti, F. Etezadi, and M. Trott

*Spinal Codes
D. Shah

*SuperNyquist Rateless Coding for Intersymbol Interference Channels............ 99
U. Erez and G. W. Wornell

*Successive Compute-and-Forward...................................................... 103
B. Nazer
Session 8
Invited session organizer: Emanuele Viterbo

*What are Good Coding Schemes for Multicast in Heterogeneous Wireless Networks?
E. Soljanin

*Tunable Sparse Network Coding ................................................................. 107
S. Feizi, D. E. Lucani, and M. Médard

*Coding for Wireless Communications
M. Bossert

*The Flatness Factor in Lattice Network Coding: Design Criterion and Decoding Algorithm ................................................................. 111
J.-C. Belfiore and C. Ling

*Wideband non-coherent Wireless Communications
E. Viterbo

Session 9: Communication Theory
Fri 15:30 – 17:10
Chaired by Tobias Koch

Analysis of the Stochastic Channel Model by Saleh & Valenzuela via the Theory of Point Processes ................................................................. 115
M. L. Jakobsen, T. Pedersen, and B. H. Fleury

A. Schenk and R. F. H. Fischer

G. Levin and S. Loyka

Complexity Analysis for ML-based Sphere Decoder Achieving a Vanishing Performance-Gap to Brute-Force ML Decoding ........................... 127
A. Singh, P. Elia, and J. Jaldén

Symbol-by-Symbol APP Decoding based on Supercode Decoding ............... 131
J. Freudenberger and U. Kaiser
The Multiple Access Channel with Correlated Sources and Cribbing Encoders

Eliron Amir and Yossef Steinberg
Dept. of EE, Technion, Israel

I. NOTATION

A discrete memoryless multiple access channel (MAC) is a quadruple \(\{X_1, X_2, P_{Y|X_1,X_2}, Y\}\) where \(X_1, X_2\) are the input alphabets, \(Y\) the output alphabet, and \(P_{Y|X_1,X_2}\) a transition probability matrix from \(X_1 \times X_2\) to \(Y\). For shorthand notation, we will refer to the MAC by \(P_{Y|X_1,X_2}\). A source pair is a triplet \([U, V, P_{U,V}]\) where \(P_{U,V}\) is a distribution on \(U \times V\). We use the following notation: random variables are denoted by uppercase letters. Sequence of \(n\) letters from alphabet \(X\) is denoted by \(x^n\), and the substring \(x_1, x_1+1, \ldots, x_j\) as \(x^j\). When the dimension \(n\) is understood from the context, \(n\)-vectors are denoted by boldface letters: \(x^n = x\). Similar notation holds for random variables and random vectors, e.g., \(V, U, U^n\), etc. The channel and source are assumed memoryless, thus probabilities of \(n\)-sequences are given by

\[
P_{Y|X_1,X_2}(y|x_1,x_2) = \prod_{i=1}^{n} P_{Y|X_1,X_2}(y_i|x_{1,i}, x_{2,i})
\]

\[
P_{U,V}(u,v) = \prod_{i=1}^{n} P_{U,V}(u_i,v_i)
\]

II. PROBLEM DEFINITION AND PREVIOUS RESULTS

We investigate a joint source-channel coding schemes for the discrete memoryless MAC with cribbing encoders. The sources, \(U\) and \(V\), deliver their output to two separate encoders 1 and 2. An \((n, m, \epsilon)\) joint source channel code for the source \(P_{U,V}\) and the MAC \(P_{Y|X_1,X_2}\) with strictly causal cribbing encoder consists of \(m + 1\) encoding functions

\[
f_1 : U^n \rightarrow X_1^n
\]

\[
f_{2,i} : V^n \times X_1^{i-1} \rightarrow X_{2,i} \quad i = 1, \ldots, m
\]

and a decoding function

\[
d^m : Y^n \rightarrow U^n \times V^n
\]

such that the probability of error is bounded from above by \(\epsilon\):

\[
P_e = \Pr\{(a^n,v^n) \neq d^m(y^n)\} = \sum_{(u,v) \not\in (d^m \times V^n)} P_{U,V}(u,v) \cdot \Pr\{d^m(y^n) \neq (u,v)\} \leq \epsilon
\]

We say that encoder 2 is the cribbing encoder, as reflected in (1b). The rate of the code is defined as \(\rho = n/m\). A source pair \((U, V)\) is said to be transmissible via the MAC \(P_{Y|X_1,X_2}\) with strictly causal cribbing at rate \(\rho\) if for every \(\epsilon > 0\), \(\delta > 0\), and sufficiently large \(n\) there exists an \((n, n/(\rho - \delta), \epsilon)\) code for the source pair and the channel.

We will examine also the model of causal cribbing, where the cribbing encoder sees the output of the other encoder without the delay of (1b), that is, when the sequence of \(m\) encoders at channel input 2 is of the form

\[
f_{2,i} : V^n \times X_1^i \rightarrow X_{2,i} \quad i = 1, \ldots, m
\]

The definition of transmissibility of a source pair via the channel remains as in the case of strictly causal cribbing, with the only difference that (2) replaces (1b). The joint probability mass function for strictly causal cribbing is given by

\[
P(u, v, x_1, x_2, y) = \prod_{i=1}^{n} P_{U,V}(u_i,v_i) \prod_{i=1}^{n} P_{Y|X_1,X_2}(y_i|x_{1,i},(u^n), x_{2i}(v^n), x_{1,i}^{-1}(u^n))
\]

and for causal cribbing by

\[
P(u, v, x_1, x_2, y) = \prod_{i=1}^{n} P_{U,V}(u_i,v_i) \prod_{i=1}^{n} P_{Y|X_1,X_2}(y_i|x_{1,i}(u^n), x_{2i}(v^n), x_{1,i}^{-1}(u^n))
\]

We are interested in finding conditions for transmissibility of a source via the MAC with causal and strictly causal cribbing. We start by stating previous relevant results, on capacity regions of MAC with cribbing, and on distributed source coding.

Theorem 1. F. Willems & E. C. van der Meulen [4]: The capacity region for the strictly causal cribbing communication model is the collection of all pairs \((R_1, R_2)\) such that

\[
R_3 \leq H(X_1 \mid W)
\]

\[
R_2 \leq I(X_2; Y \mid X_1, W)
\]

\[
R_1 + R_2 \leq I(X_1, X_2; Y)
\]

for some distribution of the form

\[
P_{W,X_1,X_2,Y}(w, x_1, x_2, y) =
\]

\[
P_W(w) P_{X_1|W}(x_1 \mid w) \cdot P_{X_2|W}(x_2 \mid w) P_{Y|X_1,X_2}(y \mid x_1, x_2)
\]

and \(|W| \leq \min\{|X_1|, |X_2| + 1, |Y| + 2\}

The capacity region for the causal cribbing communication model is given by the collection of all rate pairs \((R_1, R_2)\) such that

\[
R_3 \leq H(X_1)
\]

\[
R_1 \leq I(X_2; Y \mid X_1)
\]

\[
R_1 + R_2 \leq I(X_1, X_2; Y)
\]
for
\[ P_{X_1,X_2,Y}(x_1,x_2,y) = P_{X_1,X_2}(x_1,x_2) P_{Y|X_1,X_2}(y | x_1,x_2) \] (10)

**Theorem 2.** Slepian-Wolf [3]: For the distributed source coding problem with source \((U, V)\) drawn i.i.d \(\sim P_{U,V}\), the achievable rate region is given by:

\[
\begin{align*}
H(U | V) &\leq R_1 \\
H(V | U) &\leq R_2 \\
H(U,V) &\leq R_1 + R_2
\end{align*}
\] (11) (12) (13)

**III. STATEMENT OF RESULTS**

**Theorem 3.** A source \((U, V)\) is transmissible via the MAC \(P_{Y|X_1,X_2}\) with strictly causal cribbing at rate \(\rho = 1\) if
\[
\begin{align*}
H(U | V) &\leq H(X_1 | W, V) \\
H(V | U) &\leq I(Y; X_2 | W, U, X_1) \\
H(U,V) &\leq I(Y; X_1, X_2 | U)
\end{align*}
\] (14) (15) (16)

for some
\[
P_{Y|W,U,X_1,X_2,Y}(w,u,v,x_1,x_2,y) = P_W(w) P_{U,V}(u,v) P_{X_1|W,U}(x_1 | w,u) \cdot P_{X_2|Y,V}(x_2 | y, x_1) \] (17)

where \(P_W(\alpha) = P_U(\alpha)\) and \(W = U\).

The proof of Theorem 3 is omitted due to space considerations.

**Theorem 4.** A source \((U, V)\) is transmissible via the MAC \(P_{Y|X_1,X_2}\) with causal cribbing at rate \(\rho = 1\) if and only if there exists a joint input distribution \(P_{X_1,X_2}\) such that:
\[
\begin{align*}
\rho H(U | V) &\leq H(X_1) \\
\rho H(V | U) &\leq I(Y; X_2 | X_1) \\
\rho H(U,V) &\leq I(Y; X_1, X_2)
\end{align*}
\] (18) (19) (20)

The proof of the converse part of Theorem 4 is omitted. Two proofs of the achievability part of Theorem 4, based on Theorem 3 and based on a separation argument, are given in Section V.

Further results on transmission with distortion, and different models of cribbing, are reported elsewhere.

**IV. DISCUSSION**

As shown in Section V, Theorem 4 implies that a source \(P_{U,V}\) is transmissible via the MAC \(P_{Y|X_1,X_2}\) with causal cribbing at rate \(\rho\) if and only if the Slepian-Wolf region scaled by \(\rho\) intersects the capacity region of the MAC with causal cribbing. This implies that with causal cribbing, a separation strategy, where we use a Slepian-Wolf code to compress the source and a channel code to transmit the source codewords via the MAC, is optimal. In view of this, let us examine the achievability result for strictly causal cribbing. By Theorem 3, the following inequalities are sufficient conditions for the source \(P_{U,V}\) to be transmissible via the channel \(P_{Y|X_1,X_2}\) with strictly causal cribbing at rate \(\rho = 1\):
\[
\begin{align*}
H(U | V) &\leq H(X_1 | W) \\
H(V | U) &\leq I(Y; X_2 | W, X_1) \\
H(U,V) &\leq I(Y; X_1, X_2)
\end{align*}
\] (21) (22) (23)

for some
\[
P_{W,U,V,X_1,X_2,Y}(w,u,v,x_1,x_2,y) = P_W(w) P_{U,V}(u,v) P_{X_1|W}(x_1 | w) \cdot P_{X_2|Y,V}(x_2 | y, x_1) \] (24)

where \(P_W(\alpha) = P_U(\alpha)\) and \(U = W\).

By concatenating a Slepian-Wolf code that compresses the source, with a channel code for the MAC with strictly causal cribbing. Unfortunately, this is not the case - conditions (20)-(22) do not imply separation. This is demonstrated in the following example.

**Example 1.** Consider the joint source \((U, V)\) where \(U \sim \text{Bernoulli}(1/2)\), \(V = U\), and the binary MAC given by:
\[
P_{Y|X_1,X_2}(y|x_1,x_2) = \begin{cases} 1 & \text{if } x_1 = x_2 \\ 0 & \text{otherwise} \end{cases}
\]

where \([\cdot]\) is the indicator function. Thus, if \(x_1 = x_2\) the inputs are connected directly to the output. If \(x_1 \neq x_2\) the output is uniformly distributed on \([0,1]\), independently of the inputs.

The Slepian-Wolf rate region for this source is given by
\[
R_1 + R_2 \geq 1
\] (25)

We claim that the capacity region of this MAC with strictly causal cribbing does not contain the line \(R_1 + R_2 = 1\). Indeed, by (5)
\[
\begin{align*}
R_1 + R_2 \leq I(X_1, X_2; Y) &\leq 1 - H(Y|X_1, X_2) \\
&\leq 1
\end{align*}
\]

where the last inequality holds with equality only if \(Y\) is a deterministic function of \(X_1\) and \(X_2\). Since by (6) we have the Markov relations \(X_1 \to W \to X_2\), \(H(Y|X_1, X_2) = 0\) only if \(X_1\) and \(X_2\) are determined by \(W\). But this, in turn, implies that \(R_1 = R_2 = 0\), by (3) and (4). Therefore the capacity region of this MAC with strictly causal cribbing does not contain the line \(R_1 + R_2 = 1\).

It is easy to verify that the source \((U, V)\) is transmissible via the channel at rate \(\rho = 1\). We can employ single letter code: connect \(U\) and \(V\) directly to \(X_1\) and \(X_2\), respectively. Moreover, transmissibility can be verified directly from conditions (20)-(22): the conditional entropies on the left hand side are 0, so we can choose \(P_W = P_U\), \(X_1 = X_2 = W\), and the transmissibility conditions are satisfied. Hence, (20)-(22) (and therefore also Theorem 3) predict that the source can be transmitted via the MAC with strictly causal cribbing, yet it cannot be transmitted by a separation strategy.

**V. PROOF OF THE ACHIEVABILITY PART OF THEOREM 4**

**Proof:** The achievability part of Theorem 4 can be proved based on Theorem 3, or based on a separation argument. We first give a proof based on separation.

Given three nonempty intervals \(I_1 = [a, b]\), \(I_2 = [c, d]\), and \(I_3 = [e, f]\), a necessary and sufficient condition for the existence of a pair \((R_1, R_2)\) such that \(R_1 \in I_1, R_2 \in I_2,\) and \(R_1 + R_2 \in I_3\), is that the endpoints satisfy
\[
a + c \leq f \quad \text{and} \quad b + d \geq e
\] (26)

We claim that the capacity region of this MAC with strictly causal cribbing does not contain the line \(R_1 + R_2 = 1\). Indeed, by (5)
If the source $P_{U,V}$ and the channel and input distribution $P_{Y|X_1,X_2}$, $P_{X_1,X_2}$ satisfy (17), (18), and (19), then necessarily the intervals

\[ I_1 = \{ \rho H(U \mid V), H(X_1) \} \]

(26)

\[ I_2 = \{ \rho H(V \mid U), I(Y; X_2 \mid X_1) \} \]

(27)

\[ I_3 = \{ \rho H(U,V), I(Y; X_1, X_2) \} \]

(28)

are nonempty. By basic properties of information functions we have

\[
\rho H(U|V) + \rho H(V|U) \leq \rho H(U, V) \\
\leq I(X_1; X_2; Y) \\
= I(X_1; Y) + I(X_2; Y|X_1) \\
\leq H(X_1) + I(X_2; Y|X_1) 
\]

(29)

where the second inequality above holds since $I_3$ is nonempty. It is easy to see that (29) implies (25). Therefore, we can find a pair $(R_1, R_2)$ satisfying

\[
\rho H(U \mid V) \leq R_1 \leq H(X_1) \\
\rho H(V \mid U) \leq R_2 \leq I(Y; X_2 \mid X_1) \\
\rho H(U, V) \leq R_1 + R_2 \leq I(Y; X_1, X_2) 
\]

(30)

(31)

(32)

In other words, the scaled (by $\rho$) Slepian-Wolf rate region and the capacity region of the MAC with causal cribbing intersect. We can now construct a source-channel code by concatenating a Slepian-Wolf source code and a channel code for the MAC with causal cribbing. The details are omitted.

We give now a proof of the direct part of Theorem 4 for the special case of $\rho = 1$, based on Theorem 3. We will use Shannon strategies, as in [4]. Consider all different strategies $t \in T \triangleq [X_1]^{\mid X_2}$ that map inputs $x_1 \in X_1$ into inputs $x_2 \in X_2$. A distribution on this set induces a random variable, which we denote by $Y$. For the DMMAC $(X_1, X_2, P_{Y|X_1,X_2,Y})$, the DM derived MAC is denoted by $(X_1, T, P_{Y|X_1,T,Y})$, where $P_{Y|X_1,T}(y \mid x_1,t) \triangleq P_{Y|X_1,X_2}(y \mid x_1,t(x_1))$.

Define a set of conditions as follows:

\[
H(U \mid V) \leq H(X_1|W,V) \\
H(V \mid U) \leq I(T; Y\mid X_1, W, U) \\
H(U, V) \leq I(X_1, T; Y \mid U) 
\]

for

\[
P_{W,U,V,X_1,T,Y}(w,u,v,x_1,t,y) = P_{W}(w)P_{U,V}(u,v)P_{X_1|W,U}(x_1 \mid w,u)P_{T|W,V}(t \mid w,v)P_{Y|X_1,T}(y \mid x_1,t) 
\]

(33)

By Theorem 3, a source $P_{U,V}(u,v)$ for which the conditions above hold, is transmissible by the derived MAC with strictly causal cribbing. If we now restrict the distribution in (33) to satisfy

\[
P_{W,U,V,X_1,T,Y}(w,u,v,x_1,t,y) = P_{W}(w)P_{U,V}(u,v)P_{X_1}(x_1)P_{T}(t)P_{Y|X_1,T}(y \mid x_1,t) 
\]

then

\[
H(X_1|W,V) = H(X_1) \\
I(T; Y\mid X_1, W, U) = I(T; Y\mid X_1) \\
= I(T; X_2; Y\mid X_1) \\
= I(X_2; Y\mid X_1, X_2) \\
= I(X_2; Y\mid X_1) \\
I(X_1, T; Y \mid U) = I(X_1, X_2; Y) 
\]

and

\[
P_{X_1,X_2,Y}(x_1,x_2,y) = P_{X_1}(x_1) \cdot \sum_{t(x_1)=x_2} P_{T}(t) 
\]

(34)

where for (34) we used the same method presented in [4, (44), (45)], expressing $P_{X_1,X_2}(x_1,x_2)$ as a function of $P_{T}(t)$:

\[
P_{X_1|X_2}(x_1 \mid x_2) = \sum_{t(x_1)=x_2} P_{T}(t) \\
P_{T}(t) = \prod_{x_1} \frac{P_{X_1,X_2}(x_1,x_2 = t(x_1))}{P_{X_1}(x_1)} 
\]

Note that any joint distribution $P_{X_1,X_2}$ can be expressed with strategies, as indicated in (10) above, and in [4, (44), (45)]. Therefore the joint distribution of $X_1$ and $X_2$ can be arbitrary. This completes the proof of achievability, based on Theorem 3. ■

References


The Source Coding Side of Secrecy
Paul Cuff – Princeton University

I. INTRODUCTION

Here we discuss achievability schemes and analysis techniques useful for source coding in adversarial settings. First we mention the equivalence between defining a “valid” joint distribution over all signals in a communication system and defining the behavior of the encoders and decoders. Then we show how to construct a joint distribution in reverse of the operation direction of the encoder, resulting in a communication system that is easy to analyze from the point of view of an optimal adversary. This relates to the work in [1] and [2].

II. CODING DEFINED BY A JOINT DISTRIBUTION

Questions of interest in information theory are usually defined in an operational context, involving encoders, decoders, messages, error probabilities, and distortions. All of these questions could be translated into statement and inquiries involving only probably distributions and their properties. For example, consider the definition of the rate-distortion function.

The standard definition of the rate-distortion function asks for the lowest communication rate such that there exists encoding functions and decoding functions that satisfy certain properties concerning the range of the encoding function and the resulting average distortion. We can alternatively state an equivalent definition for the rate-distortion function as a question about existence of probability distributions that satisfy certain conditions, as follows.

Rate-distortion Function: Given a source distribution $Q(x^n)$ and a distortion function $d(\cdot, \cdot)$, what is the minimum rate $R$ such that for all $\epsilon > 0$ and $n$ sufficiently large there exists a joint distribution $p(x^n, m, z^n)$ such that the cardinality of $M$ is less than $2^{nR}$, $X^n - M - X^n$ form a Markov chain, $p(x^n) = Q(x^n)$, and $E \frac{1}{n} \sum_{i=1}^{n} d(x_i, \hat{x}_i) < D + \epsilon$? Let this be the value of the rate-distortion function $R(D)$.

The above restatement of the rate-distortion function is trivial and not very helpful. However, in some problems, particularly those involving an adversary, we find this form of the problem statement to be revealing. For one thing, the operation of the encoders and decoders are implicitly specified in the joint distribution of the signals. For example, the encoder in the rate-distortion function statement above operates according to the induced conditional distribution $p(m|x^n)$. But by changing the emphasis from defining how the encoder and decoder behave to instead defining a joint distribution to satisfy the constraints of the problem, a reverse-encoding construction is easily conceived. That is, we might find it useful to construct the inverse of the encoder, $p(x^n|m)$, to have certain properties rather than design the actual working of the encoder explicitly.

III. REVERSE-CHANNEL ENCODER

In [1] we characterize the best lossless source coder that makes use of limited secret key to cause maximal distortion to an eavesdropper. An asymptotically optimal construction for the encoder is derived using two key concepts, discussed in the following two paragraphs. The communication is split into two parts, one message which has the secret key applied to it as a one-time pad, and the other non-secure message which is the crux of the analysis. The eavesdropper obtains the non-secure message, and we must be able to analyze the lowest distortion the eavesdropper can achieve given the received message.

The first key concept for constructing an optimal encoder is to design the encoder in reverse. Let $M$ be the non-secure message obtained by the eavesdropper, and let $X^n$ be the source sequence. The eavesdropper’s minimum average distortion when a particular message $m$ is observed depends on the distribution $p(x^n|m)$, which is the inverse of the encoder. Consider the following design. Using the standard technique of random codebook construction, let $U$ be an auxiliary random variable correlated with $X$ and construct a codebook of i.i.d. $U^n$ sequences indexed by $M$. Let $X^n$ be conditionally distributed as the output of a memoryless channel $\sim p(x|u)$ when the input to the channel is $U^n(M)$. The memoryless nature of this constructed conditional distribution $p(x^n|m)$ makes it trivial to characterize the minimum distortion incurred by the eavesdropper.

The last concept needed for the analysis is that of solvability. In the construction above, if $M$ is uniformly distributed over a set of size $2^{nR}$, with $R > I(X; U)$, then the resulting distribution $p(x^n)$ will be close to the i.i.d. source distribution $Q(x^n)$ in total variation. Consequently, the constructed joint distribution is close in total variation to a valid joint distribution. We close this gap with some lemmas about total variation distance.

REFERENCES

A Comparative Study of Cooperation for the Two-user Interference Channel

Daniela Tuninetti
University of Illinois at Chicago
Department of Electrical and Computer Engineering
851 S. Morgan St. (M/C 154)
Chicago, IL 60607, USA
Email: danielat@uic.edu

Abstract—The interference channel is a model for a wireless network where several source-destination pairs compete for the same resources. When the sources transmit simultaneously the destinations experience unwanted interference. Determining how to optimally manage the interference is a long standing open problem in network information theory. In this talk we review one emerging interference management technique: cooperation. Cooperation can occur among source nodes only (Source Cooperation or Generalized Feedback), or among destination nodes only (Destination Cooperation), or among all nodes (General Cooperation). For the special case of Gaussian noise channels, we compare the different forms of cooperation in terms of symmetric generalized degrees of freedom. When known, we also discuss capacity results to within a constant number of bits.

I. CHANNEL MODEL

A general full-duplex cooperative interference channel is a 2K-node network with inputs $X_0, \ldots, X_{2K-1}$, outputs $Y_0, \ldots, Y_{2K-1}$ and a memoryless channel with transition probability $P := P[Y_0, \ldots, Y_{2K-1} | X_0, \ldots, X_{2K-1}]$. Sources have index $0$ to $K-1$ and destinations $K$ to $2K-1$. Message $W_i$ is independent of everything else and uniformly distributed over $[1 : 2NR]$, with $N \in \mathbb{N}$ denoting the block-length and $R_i \in \mathbb{R}^+$ the rate in bits per channel use, for $i \in [0 : K-1]$. Encoding at node $i \in [0 : 2K-1]$ at channel use $t \in [1 : N]$ is a deterministic function $X_{i,t}(W_i, Y_{i,t}^{t-1})$, with the convention $W_{K} = \ldots = W_{2K-1} = \emptyset$. Decoding at node $i \in [K : 2K-1]$ after the $N$-th channel use is a deterministic function $W_{i,K}(Y_i^N)$. A rate vector $(R_0, \ldots, R_{K-1})$ is $\epsilon$-achievable if $\max_{i \in [0 : K-1]} P[W_i \neq W_i] \leq \epsilon$ for some $\epsilon \in (0, 1]$. The capacity region is the convex closure of the set of rate vectors that are $\epsilon$-achievable for all $\epsilon > 0 [1]$. In this work we consider the case $K = 2$ only, which is depicted in Fig. 1.

II. MODELS OF COOPERATION

Several cooperation models have been analyzed in literature such as: cooperation only occurs among sources (Source Cooperation, also known as Generalized Feedback), or only among destinations (Destination Cooperation), or among all nodes (General Cooperation). In each case, cooperation can be in-band or out-of-band. For out-of-band cooperation, the network is effectively composed of two parallel networks: the underlying interference channel (from the source inputs to the destination outputs) and the cooperation channel (which is usually assumed to be deterministic/noiseless).

In the following we list some recent journal papers that deal with cooperation for the two-user interference channel and that we will compare in this talk. The interested reader can find the technical details in these works and the list of related preceding publications in the references herein. Some extensions to networks with more than two source-destinations pairs can be found for example in [14], [15].

A. Source Cooperation/Generalized Feedback

The destinations do not have an input to the channel, i.e.,

$$X_K = \ldots = X_{2K-1} = \emptyset.$$  

A.1) Out-of-band. The channel input at source $i$, $i \in [0 : K-1]$, is a two-dimensional vector $X_i := [X_{i,d}, X_{i,s}]$, where $X_{i,d}$ affects the channel outputs at the destinations and $X_{i,s}$ the channel outputs at the sources. Effectively, there are two parallel channels: the underlying interference channel with transition probability $P[Y_K, \ldots, Y_{2K-1} | X_{0:d}, \ldots, X_{K-1:d}]$ and the cooperation channel with transition probability $P[Y_0, \ldots, Y_{K-1} | X_{0:s}, \ldots, X_{K-1:s}]$. 

![Fig. 1. The memoryless cooperative interference channel (channel inputs in green, channel outputs in pink, transmitted messages in black, and decoded messages in blue).](image-url)
Conferencing Encoders is a special case of out-of-band source cooperation where the cooperation channel is deterministic [2].

Cognition is a special case of conferencing encoders where the channel output at some sources is constant (these sources are known as “primary users”) and the channel output at the other sources is such that all messages can be conveyed in a single channel use (these sources are known as the “cognitive users”) [4], [5].

A.2) In-band. The same inputs affect both the underlying interference channel and the cooperation channel. The cooperation channel is noisy [6], [7], [8], [9].

Noisy Output Feedback is a special case of in-band source cooperation where the channel output at a source is a degraded version of the channel output at its intended destination, i.e., \( Y_i = g_i(Y_{i+K}, Z_i) \) for some deterministic function \( g_i \) and some random process \( Z_i \) representing the “extra noise”, for all \( i \in [0 : K - 1]\) [11]. If the “extra noise” process is deterministic then the channel is known simply as interference channel with feedback [12].

Ultimate Limit of Source Cooperation. By sharing all messages among the sources we obtain an equivalent memoryless broadcast channel with input \( X_0 = \ldots = X_{K-1} \) and outputs \( Y_K, \ldots, Y_{2K-1} \), whose capacity (which is not known in general) [1]) gives the ultimate gain that can be obtained with source cooperation.

B. Destination Cooperation

The sources do not have an output from the channel, i.e.,

\[
Y_0 = \ldots = Y_{K-1} = 0.
\]

B.1) Out-of-band. The channel output at destination \( i \), \( i \in [K : 2K - 1] \), is a two-dimensional vector \( Y_i := [Y_{i,d}, Y_{i,s}] \), where \( Y_{i,d} \) is affected by the channel inputs from the destinations and \( Y_{i,s} \) by the channel inputs from the sources. Effectively, there are two parallel channels: the underlying interference channel with transition probability \( P[Y_0, \ldots, Y_{K-1}, X_0, \ldots, X_{K-1}] \) and the cooperation channel with transition probability \( P[Y_0, \ldots, Y_{K-1}, X_K, \ldots, X_{2K-1}] \).

Conferencing Decoders is a special case of out-of-band destination cooperation where the cooperation channel is deterministic [3].

B.2) In-band. The channel outputs are affected by all channel inputs [6], [10].

Ultimate Limit of Destination Cooperation. By sharing all channel outputs at the destinations among the destinations we obtain an equivalent memoryless multiple access channel with inputs \( X_0, \ldots, X_{K-1} \) and output \( Y_{eq} := (Y_K, \ldots, Y_{2K-1}) \), whose capacity region [1] gives the ultimate gain that can be obtained with destination cooperation.

C. General Cooperation

This is the most general case where all nodes cooperate.

C.1) Out-of-band. Channel outputs at the destinations are affected by the channel inputs from the sources only and channel outputs at the sources are affected by the channel inputs from the destinations only. Effectively, there are two parallel channels: the underlying interference channel with transition probability \( P[Y_K, \ldots, Y_{2K-1}, X_0, \ldots, X_{K-1}] \) and a cooperation channel with transition probability \( P[Y_0, \ldots, Y_{K-1}, X_K, \ldots, X_{2K-1}] \).

Rate-limited Feedback is a special case of out-of-band general cooperation where the cooperation channel is deterministic [13].

C.2) In-band. All channel inputs affect all channel outputs.

To the best of the author’s knowledge the case of in-band general cooperation has not been studied so far.

Ultimate Limit of General Cooperation. By sharing all messages among the sources and all channel outputs at the destinations among the destinations we obtain an equivalent memoryless point-to-point channel with input \( X_{eq} := (X_0, \ldots, X_{K-1}) \) and output \( Y_{eq} := (Y_K, \ldots, Y_{2K-1}) \), whose capacity gives the following sum-rate upper bound

\[
R_0 + \ldots + R_{K-1} \leq C_{\text{perfect coop.}} := \max_{P[X_{eq}]} I(X_{eq}; Y_{eq}).
\]

which cannot be improved by feedback, i.e., \( C_{\text{perfect coop.}} \) does not depend on \( Y_0, \ldots, Y_{K-1} \).

ACKNOWLEDGMENT

The author’s work on the Interference Channel with Generalized Feedback [7], [8] is part of Dr. S. Yang’s doctoral dissertation, while that on the Cognitive Interference Channel [4], [5] is part of Dr. S. Rini’s doctoral dissertation and was done in collaboration with Dr. N. Devroye.

REFERENCES


Abstract—We provide an improved random coding bound for a class of discrete memoryless channels that improves the pre-factor in front of the exponent. Specifically, while the tightest known bounds have a constant pre-factor, the presented bound has a pre-factor of order $O(1/\sqrt{N})$, where $N$ is the blocklength.

I. INTRODUCTION

Characterizing the interplay between the data rate, error probability, and blocklength of the best codes for a given discrete memoryless channel (D.M.C.) is a central problem in information theory. Although this interplay has been investigated starting from the early days of the field [1], [2], [3], [4], [5], [6], [7], [8], [9], it is still an active research topic [10], [11], [12], [13], [14]. Due to the difficulty of the problem, it is customary to consider formulations that are asymptotic in the blocklength to characterize this interplay.

One of the best-known formulations is “error exponents,” in which the rate is held fixed below the channel capacity and one characterizes the rate of decay of the error probability, which is exponential in $N$ for most channels [3], [4], [5], [6]. Another asymptotic characterization is the “normal approximation” in which the error probability is a fixed at a positive constant in $(0,1/2)$ and one characterizes the speed with which the data rate converges to capacity [2], [13]. Between these two characterizations, one can consider the setup in which the error probability tends to zero and the rate simultaneously approaches capacity, with the goal of characterizing the speed of one convergence as a function of the other [14]. We call these three asymptotics the “small error probability,” “large error probability,” and “medium error probability” regimes, respectively. It should be noted that although there is an underlying relation between these three asymptotics the “small error probability,” “medium error probability” and “large error probability” regimes, respectively. For any $X$, $P(X)$ denotes the set of all probability measures on $X$. Similarly, for two finite sets $X$ and $Y$, $P(Y|X)$ denotes the set of all stochastic matrices from $X$ to $Y$. $\mathbb{R}$, $\mathbb{R}^+$ and $\mathbb{R}_+$ denote the set of real, positive real and non-negative real numbers, respectively. $\mathbb{Z}^+$ denotes the set of positive integers. Throughout the paper, all logarithms are base-2. For a finite set $X$, $P(X)$ denotes the set of all probability measures on $X$. Similarly, for two finite sets $X$ and $Y$, $P(Y|X)$ denotes the set of all stochastic matrices from $X$ to $Y$. $\mathbb{R}$, $\mathbb{R}^+$ and $\mathbb{R}_+$ denote the set of real, positive real and non-negative real numbers, respectively. $\mathbb{Z}^+$ denotes the set of positive integers. For any $W$ in $P(Y|X)$ and $Q$ in $P(X)$ the ensemble average error probability $\text{E}_{\log_2} (p(Q,W))$ and $\text{E}_{\log_2} (p(Q,W))$ respectively denote individual elements of vectors. Furthermore, capital letters represent random variables and lowercase letters denote individual realizations of the corresponding random variable. Throughout the paper, all logarithms are base-2. For a finite set $X$, $P(X)$ denotes the set of all probability measures on $X$. Similarly, for two finite sets $X$ and $Y$, $P(Y|X)$ denotes the set of all stochastic matrices from $X$ to $Y$.

B. Definitions

Throughout the paper, let $W$ be a D.M.C. from $X$ to $Y$. $E_{\rho}(R,W)$ and $E_{\rho}(\rho,Q,W)$ denotes the random coding exponent (cf. [7, eq. (5.6.16)]) and the Gallager’s function (cf. [7, eq. (5.6.14)]), respectively. For any $W$ $\in P(Y|X)$ and $Q$ $\in P(X)$ the ensemble average error probability (resp. ensemble average error probability conditioned on the

The authors are with the School of Electrical and Computer Engineering, Cornell University, Ithaca, NY 14853. E-mail: ya68@cornell.edu, wagner@ece.cornell.edu. This research was supported by the U.S. National Science Foundation under grants CCF-0830496 and CCF-1117128.
message \( m \) of a random code with codewords generated by using \( Q \) along with a maximum likelihood decoder\(^1\) is denoted by \( \tilde{P}_e(Q) \) (resp. \( \tilde{P}_e(m,Q) \)). \( \sigma^2(W) \) denotes the dispersion (cf. [2], [13]) of \( W \in \mathcal{P}(\mathcal{Y}|\mathcal{X}) \).

Further,

\[
S_{Q,W} := \{(x,y) \in \mathcal{X} \times \mathcal{Y} : Q(x)W(y|x) > 0 \},
\]

\[
\tilde{S}_{Q,W} := \{(x,y,z) : Q(x)W(y|x)Q(z)W(y|z) > 0 \},
\]

\[
\mathcal{X}_y(W) := \{ x \in \mathcal{X} : W(y|x) > 0 \},
\]

(1), (2), (3)

Given a \((Q,W) \in \mathcal{P}(\mathcal{X}) \times \mathcal{P}(\mathcal{Y}|\mathcal{X})\) pair, the following property amounts to saying that “feasibility decoding is optimal” (F.D.I.O.) when a random code with distribution \( Q \) is used for transmission over the D.M.C. \( W \).

**Property 1:** (F.D.I.O.) For all \((x,y,z) \in \tilde{S}_{Q,W}, W(y|x) = W(y|z).\)

**C. Statement of the result**

**Theorem 1:** Let \( W \in \mathcal{P}(\mathcal{Y}|\mathcal{X}) \) be arbitrary with \( \sigma^2(W) > 0 \) and \( R \in [R_{cr}(W), C(W)] \). If there exists \( Q \in \mathcal{P}(\mathcal{X}) \) achieving \( E_e(R,W) \) such that the F.D.I.O. property does not hold, then for all \( N \in \mathbb{Z}^+ \)

\[
\tilde{P}_e(Q) \leq \frac{K_1}{\sqrt{N}} e^{-NE_e(R,W)},
\]

where \( K_1 \) is a positive constant that only depends on \( W \) and \( R \).

**Remark 1:** Using the standard expurgation arguments, Theorem 1 ensures the existence of an \((N,R)\) code with maximal error probability upper bounded by the right side of (4), with a different constant.

**Remark 2:** The proof of Theorem 1 is based on Fano’s proof of the random coding bound [3, pp. 324–331] with a refinement to prove the smaller pre-factor. In the literature, Fano’s argument has been superceded by Gallager’s, which is simpler and gives the same exponent. Fano’s argument, however, lends itself more readily to obtaining improved pre-factors.

**Remark 3:** Note that the assumption related to the F.D.I.O. property in Theorem 1 holds for a reasonably large class of channels, such as the class of positive channels with positive dispersion. Yet this assumption does not exclude only degenerate cases; note that the binary erasure channel (B.E.C.) is excluded. Moreover, the assumption is not necessary in order to have an upper bound on the error probability with a pre-factor of \( O(1/\sqrt{N}) \). Indeed, Elias [15] proves such an upper bound for B.E.C.

**Remark 4:** The above theorem applies to the ensemble average error probability at rates above the critical rate. For rates below the critical rate, the order of the pre-factor turns out to hinge on the F.D.I.O property, a fact that was heretofore overlooked in the literature. The next result, Theorem 2, corrects a small oversight by Gallager [17], who claims that for any D.M.C. \( W \) and rate \( R < R_{cr}(W) \)

\[
\min_{Q \in \mathcal{P}(\mathcal{X})} \tilde{P}_e(Q) \sim g \frac{\log N}{\sqrt{N}} e^{-NE_e(R)},
\]

for some constant \( g \). In fact, his argument is valid only for those \( W \in \mathcal{P}(\mathcal{Y}|\mathcal{X}) \) such that there exists \( Q \in \mathcal{P}(\mathcal{X}) \) with \( E_e(1,Q,W) = \max_{P \in \mathcal{P}(\mathcal{X})} E_o(1,P,W) \) and the F.D.I.O. property is not true. For the remaining channels, we have the following result.

**Theorem 2:** Consider an arbitrary \( W \in \mathcal{P}(\mathcal{Y}|\mathcal{X}) \) with \( C(W) > 0 \) and \( R < R_{cr}(W) \). If the F.D.I.O. property holds for all \( Q \in \mathcal{P}(\mathcal{X}) \) with \( E_e(1,Q,W) = \max_{P \in \mathcal{P}(\mathcal{X})} E_o(1,P,W) \), then for all \( N \in \mathbb{Z}^+ \)

\[
K_2 e^{-NE_e(R,W)} \leq \tilde{P}_e(Q) \leq e^{-NE_e(R,W)}.
\]

for some \( 0 < K_2 < 1 \) that depends on \( W \) and \( R \).

**III. PROOF OF THEOREM 1**

Let \( W \in \mathcal{P}(\mathcal{Y}|\mathcal{X}) \) with \( \sigma^2(W) > 0 \) be arbitrary. Fix an arbitrary \( R \in [R_{cr}(W), C(W)] \). Consider an arbitrary \( Q \in \mathcal{P}(\mathcal{X}) \) with \( E_e(R,Q,W) = E_e(R,W) \), such that the F.D.I.O. property does not hold, whose existence is guaranteed by the assumption of the theorem. For the sake of notational convenience, let \( \tilde{S}_Q, \tilde{S}_{\tilde{Q}} \) and \( \mathcal{X}_y \) denote \( \tilde{S}_{Q,W}, \tilde{S}_{\tilde{Q}} \) and \( \mathcal{X}_y(W) \) as given in (1), (2) and (3), respectively. Define

\[
P_{X,Y,Z}(x, y, z) := Q(x)W(y|x)Q(z),
\]

for all \((x,y,z) \in \mathcal{X} \times \mathcal{Y} \times \mathcal{X} \). Also, let

\[
\tilde{P}_{X,Y,Z}(x, y, z) := \begin{cases} P_{X,Y,Z}(x, y, z) & \text{if } (x,y,z) \in \tilde{S}_Q \\ 0 & \text{else} \end{cases}
\]

Define \( P_{X,Y,Z}^N(x, y, z) := \prod_{n=1}^N P_{X,Y,Z}(x_n, y_n, z_n) \) and \( \tilde{S}_Q^N \) (resp. \( \tilde{S}_{\tilde{Q}}^N \)) denote the \( N \)-fold cartesian product of \( S_Q \) (resp. \( \tilde{S}_Q \)). Hence,

\[
P_{X,Y,Z}^N \left( x, y, z | \tilde{S}_Q^N \right) = \tilde{P}_{X,Y,Z}^N(x, y, z)
\]

\[
\begin{align*}
&:= \prod_{n=1}^N \tilde{P}_{X,Y,Z}(x_n, y_n, z_n). \\
&\text{One can show that}
\end{align*}
\]

\[
\exists \rho^* \in (0,1], \text{ s.t. } \frac{\partial E_e(\rho, Q,W)}{\partial \rho} \bigg|_{\rho=\rho^*(Q,W)} = R.
\]

Define

\[
D_0 := N \left( \frac{\rho^*}{1 + \rho^*} \right),
\]

\[
\Lambda_4(s,t) := \log \mathbb{E}_{\tilde{P}_{X,Y,Z}} \left[ e^{s \log \frac{P(1-Q)}{P(1-Q)}} + t \log \frac{W(y|x)}{W(y|x)} \right],
\]

for any \((s,t) \in \mathbb{R}^2 \). Observe that owing to the fact that \( \log \frac{P(1-Q)}{P(1-Q)} \), \( \log \frac{W(y|x)}{W(y|x)} \in \mathbb{R} \), for all \((x,y,z) \in \tilde{S}_Q, \Lambda_4(\cdot) \) is infinitely differentiable on \( \mathbb{R}^2 \).
Finally, for any $N \in \mathbb{Z}^+$, let

$$D_N := \left\{ \frac{1}{N} \sum_{n=1}^{N} \log \frac{f(Y_n)}{W(Y_n | X_n)} > D_0 \right\}.$$  

From the standard random coding arguments, one can show that

$$\tilde{P}_{e,1}(Q) \leq P_{X,Y,Z}^N \left\{ \frac{1}{N} \sum_{n=1}^{N} \log \frac{f(Y_n)}{W(Y_n | X_n)} \leq D_0, \right. \left. \frac{1}{N} \sum_{n=1}^{N} \log \frac{W(Y_n | X_n)}{W(Y_n | Z_n)} \leq 0 \right\}. \tag{12}$$

In order to conclude the proof, we need to upper bound the two terms on the right side of (12).

We begin with the second term. To this end, define

$$\Lambda^*(a) := \sup_{\lambda \in \mathbb{R}} \left\{ a\lambda - \Lambda(\lambda) \right\}, \tag{13}$$

for any $a \in \mathbb{R}$. By noting the convexity of $\Lambda(\cdot)$; (10), (13) and some algebra imply that

$$\Lambda^*(D_0) = E_r(R, W). \tag{14}$$

Owing to a result of Ney [19, eq. (2)], we deduce that

$$P_{X,Y}^N \{ D_N \} \leq \frac{k_1}{N} e^{-N\Lambda^*(D_0)} = \frac{k_1}{N} e^{-N\Lambda^*(D_0)}, \tag{15}$$

for some $k_1 \in \mathbb{R}^+$ and for all sufficiently large $N$, where the equality follows from (14).

Next, we upper bound the first term on the right side of (12). First, since for any $(x, y, z) \notin \mathcal{S}_Q$, we have

$$\log \frac{W(y | x)}{W(y | z)} = \infty, \quad Q \times W \times Q \text{ - a.s.}$$

we have

$$\alpha_N := P_{X,Y,Z}^N \left\{ \frac{1}{N} \sum_{n=1}^{N} \log \frac{f(Y_n)}{W(Y_n | X_n)} \leq D_0, \right. \left. \frac{1}{N} \sum_{n=1}^{N} \log \frac{W(Y_n | X_n)}{W(Y_n | Z_n)} \leq 0 \right\} \tag{16}$$

where, in (16) we define

$$\tilde{\alpha}_N := \tilde{P}_{X,Y,Z}^N \left\{ \frac{1}{N} \sum_{n=1}^{N} \log \frac{f(Y_n)}{W(Y_n | X_n)} \leq D_0, \right. \left. \frac{1}{N} \sum_{n=1}^{N} \log \frac{W(Y_n | X_n)}{W(Y_n | Z_n)} \leq 0 \right\}. \tag{17}$$

Define

$$t^* := -1/(1 + \rho^*) \quad \text{and} \quad \rho^* := 1 + 2t^*. \tag{18}$$

One can show that

$$\frac{\partial \Lambda_1(s, t)}{\partial s} \Big|_{s=s^*} = D_0, \quad \frac{\partial \Lambda_1(s, t)}{\partial t} \Big|_{t=t^*} = 0. \tag{19}$$

Before proceeding further, we define

$$B := (-\infty, D_0] \times (-\infty, 0], \quad \mathcal{A}_B := [D_0, 0]^T, \tag{20}$$

and

$$\Lambda_1^*(b) := \sup_{a \in \mathbb{R}^2} \{a(b) - \Lambda_1(a)\}, \tag{21}$$

for any $b \in \mathbb{R}^2$. Note that owing to the convexity of $\Lambda_1(\cdot)$, one can show that

$$\Lambda_1^*(\mathcal{A}_B) = s^* D_0 - \Lambda_1(s^*, t^*), \tag{22}$$

where $s^*$ and $t^*$ are as defined in (18). Moreover,

$$\Lambda_0(\lambda) := \log E_{P_{X,Y,Z}} \left[e^{\lambda \log \frac{W(Y | X)}{W(Y | Z)}} \right], \tag{23}$$

for all $\lambda \in \mathbb{R}$. Further, one can verify that

$$\Lambda_0^*(0) = E_{P_{X,Y,Z}} \left[ \log \frac{W(Y | X)}{W(Y | Z)} \right] > 0. \tag{24}$$

A result of Ney [19, Theorem] implies that there exists a unique dominating point (cf. [19, Definition]) $d_B \in \mathcal{B}$, which also satisfies (cf. [20, eq. (3.3)])

$$\Lambda_1^*(d_B) = \inf_{b \in \mathcal{B}} \sup_{a \in \mathbb{R}^2} \{b(a) - \Lambda_1(a)\}. \tag{25}$$

Moreover, [19, eq. (2)] implies that

$$\frac{c_1}{N} e^{-N\Lambda_1^*(d_n)} \geq \tilde{\alpha}_N \leq \frac{c_2}{\sqrt{N}} e^{-N\Lambda_1^*(d_n)}, \tag{26}$$

for some $c_1, c_2 \in \mathbb{R}^+$ and all sufficiently large $N$. Next, one can prove that

$$\Lambda_1^*(\mathcal{A}_B) = \Lambda_1^*(d_B). \tag{27}$$

Plugging (27) into (26) yields

$$\tilde{\alpha}_N \leq \frac{c_2}{\sqrt{N}} e^{-N\Lambda_1^*(d_n)}, \tag{28}$$

for some $c_2 \in \mathbb{R}^+$ and all sufficiently large $N$. Moreover, it is possible to check that

$$\Lambda_1(s^*, t^*) = -\log P_{X,Y,Z} \left\{ \mathcal{S}_Q \right\} + 2\Lambda \left( \frac{\rho^*}{1 + \rho^*} \right). \tag{29}$$

3Because of the fact that the random variables in $D_N$ are i.i.d., we might have used the stronger “exact asymptotics” result [18] by considering lattice and non-lattice cases separately. However, the application of such a result has little effect on the ultimate bound since the second term of (12) cannot be handled by an analogous theorem.

4To justify the application of the aforementioned result, one can check that $\Lambda(\cdot)$ satisfies the regularity conditions stated in [19, Theorem]. Moreover, one can verify that $\Lambda \left( \frac{\partial \Lambda_1(s, t)}{\partial s} \right) > \Lambda^*(0) = E_{P_{X,Y}} \left[ \log \frac{W(Y | X)}{W(Y | Z)} \right]$. This guarantees the “mean does not belong to the set” regularity condition that $D_N$ must satisfy. The remaining regularity conditions on $D_N$ are easy to check. Therefore the existence of a unique “dominating point” (cf. [19, Definition]) is guaranteed owing to [19, Theorem]. However, one can check that this dominating point is $D_0$ (e.g. [20, pg. 159]). Lastly, [20, eq. (3.3)] gives the exponential factor in (15).

5Similar to the previous footnote, (24) ensures the fulfillment of the “mean does not belong to the set” condition of the theorem. The remaining conditions are easy to check.
Finally, plugging (18), (22) and (29) into (28) along with (10), (14) and some algebra yields

\[ \tilde{\alpha}_N \leq \frac{P_{X,Y,Z} \left\{ \tilde{S}_Q \right\}^{-N} c_2 e^{-N[E_e(R,W)+R]} \right.}{\sqrt{N}}. \]  

(30)

By plugging (30) into (16) and noting \( P_{X,Y,Z}^{N} \left\{ \tilde{S}_Q \right\} = P_{X,Y,Z} \left\{ \tilde{S}_Q \right\}^N \), we deduce that

\[ \alpha_N \leq \frac{c_2}{\sqrt{N}} e^{-N[E_e(R,W)+R]} \left(1 \right). \]  

(31)

Lastly, (12), (15) and (31) imply that

\[ \tilde{P}_{e,1}(Q) \leq \frac{K_1}{e^{N[E_e(R,W)]}} \]  

(32)

for some \( K_1 \in \mathbb{R}^+ \) and all sufficiently large \( N \).

IV. PROOF OF THEOREM 2

Let \( W \in \mathcal{P}(\mathcal{Y}|\mathcal{X}) \) with \( C(W) > 0 \) and \( R < R_{ca}(W) \) be arbitrary. Assume that for all \( Q \in \mathcal{P}(\mathcal{X}) \) with \( E_0(1,Q,W) = \max_{P \in \mathcal{P}(\mathcal{X})} E_0(1,P,W) \), the F.D.I.O. property holds. Consider any such \( Q \in \mathcal{P}(\mathcal{X}) \). For this \((Q,W)\) pair, let \( P_{X,Y,Z} \) and \( \tilde{P}_{X,Y,Z} \) be as given in (7) and (8), respectively. For the sake of notational convenience, let \( \tilde{S}_Q \) and \( \lambda_y \) denote \( \tilde{S}_{Q,W} \) and \( \lambda_y(W) \) as given in (2) and (3), respectively.

Owing to the fact that the F.D.I.O. property holds, one can show that

\[ \log P_{X,Y,Z} \left\{ \tilde{S}_Q \right\} = -E_0(1,Q,W). \]  

(33)

By using the standard random coding arguments, we have

\[ \tilde{P}_{e,1}(Q) \leq e^{N[R_{ca}(W) - E_0(1,Q,W)]} \]  

(34)

\[ = e^{-N[E_e(R,W)]} \]  

(35)

where (34) follows from the fact that for any \((x,y,z) \notin \tilde{S}_Q\), \( \log \frac{W(y|x)}{P(y|x)} \) is nearly \( Q \times W \times Q - (a.s.) \), and the F.D.I.O. property is satisfied. (35) follows from (33) and (36) is true owing to the choice of \( Q \in \mathcal{P}(\mathcal{X}) \) and the fact that \( R < R_{ca}(W) \) (e.g. [17, pg. 245]). Hence, the upper bound of (6) follows.

In order to establish the lower bound of (6), one can use Gallager’s arguments [17, pp. 245-246] by noting

\[ P_{X,Y,Z}^{N} \left\{ \frac{1}{N} \sum_{n=1}^{N} \log \frac{W(Y_n|X_n)}{W(Y_n|Z_n)} \leq 0 \right\} = e^{-NE_0(1,Q,W)}. \]  

V. COMPARISON WITH THE SPHERE-PACKING BOUND

Our main result is an improvement of the random coding bound for rates greater than the critical rate, obtained by improving the pre-factor from \( O(1) \) to \( O(1/\sqrt{N}) \) for a broad class of channels.

Even for the symmetric channels, however, this pre-factor does not match its lower bound counterpart [22], namely \( O(N^{-\frac{1}{2}}(1 + |E_0(R)|)) \), where \( |E_0(R)| \) is the slope of \( E_0(R) \). It is worth noting, however, that for rates close to capacity, \( |E_0(R)| \) is nearly zero, so the order of the pre-factor is nearly determined in this regime.

REFERENCES


Source Coding with Side-Information at the Receivers and an Application

Michèle Wigger
Telecom ParisTech, Paris, France
Email: michele.wigger@telecom-paristech.fr

Abstract—We review results on the source-coding problem in Figure 1, i.e., on the simple network proposed by Gray and Wyner where additionally the receivers have side-information about the source. We also describe how this problem is relevant for coding over broadcast channels (BC) with feedback.

I. THE SOURCE CODING PROBLEM

We consider the source-coding problem in Figure 1, where a transmitter describes the source sequence $X^n=(X_1,\ldots,X_n)$ to Receivers 1 and 2, who observe the side-information $Y_1^n=(Y_{1,1},\ldots,Y_{1,n})$ and $Y_2^n=(Y_{2,1},\ldots,Y_{2,n})$, respectively. Here, $(X_t,Y_{1,t},Y_{2,t})^{n}_{t=1}$ is a sequence of independent and identically distributed (IID) triples of joint law $P_{X,Y_1,Y_2}$. The transmitter can send a common message $M_0$ of rate $R_0$ to both receivers and private messages $M_1$ and $M_2$ of rates $R_1$ and $R_2$ to Receivers 1 and 2, respectively. The goal is that Receiver $i$, for $i \in \{1,2\}$, produces a reconstruction sequence $\hat{X}_i^n=(\hat{X}_{1,i},\ldots,\hat{X}_{n,i})$ that satisfies

$$\sum_{i=1}^n d_i(\hat{X}_i,t) \leq D_i,$$

where $d_i$ is the symbol-wise distortion function and $D_i \geq 0$ the distortion constraint. The described setup includes the case where $X^n=(X_1^n,X_2^n)$ and Receiver $i$ only wishes to reconstruct a lossy version of $X_i^n$.

Theorem 1 ([5]): A triple $(R_0,R_1,R_2)$ is achievable if

$$R_0 + R_1 \geq I(X;X_1|V_0), \quad R_0 + R_1 + R_2 \geq I(X;X_1|Y_1,V_0) + I(X;X_2|Y_2,V_0) + \max_{i \in \{1,2\}} I(X;X_i|Y_i)V_0),$$

for some $\hat{X}_1,\hat{X}_2, V_0$ such that $\hat{X}_1,\hat{X}_2, V_0$ and $X_1^n, X_2^n, V_0$ form a Markov chain and $\mathbb{E}[d(X,X_i)] \leq D_i$, for $i \in \{1,2\}$.

Though the region is not known to be optimal in general, it is optimal for all special cases where the rates-distortions region is known. In the following we review these special cases. Gray and Wyner characterized the rates-distortions region when there is no side-information [1]. Heegard and Berger [2] proposed inner and outer bounds on the rates-distortions region when the transmitter can send only a common message, but no private messages, i.e., when $R_1 = R_2 = 0$. The bounds coincide when $X \rightarrow Y_1 \rightarrow X_1$ or $X \rightarrow Y_2 \rightarrow X_2$, Steinberg and Merhav [3], and Tian and Diggavi [4] considered the case when the transmitter can send a common message and a private message to Receiver 2 but not to Receiver 1, i.e., when $R_1 = 0$. More specifically, [3] characterizes the rates-distortions region for the successive Wyner-Ziv refinement problem where Receiver 2 (who receives the additional private message has the better side-information, i.e., $X \rightarrow Y_2 \rightarrow Y_1$, and [4] proposes inner and outer bounds on the rates-distortions region for the scalable source-coding problem where Receiver 1 has the better side-information, i.e., $X \rightarrow Y_1 \rightarrow Y_2$. The bounds in [4] are tight when either $D_1 = 0$ or $D_2 = 0$ or when the two distortion measures $d_1$ and $d_2$ are deterministic and degraded.

II. APPLICATION TO THE BC WITH FEEDBACK

Our lossy source-coding problem has application to coding over BCs with feedback, see especially [5] but also [6], [7]. The core idea of these schemes is the following. In a first stage the transmitter sends the desired messages at rates that do not allow for decoding at the receivers. Then, using the feedback, it identifies resolution information which it sends during the second stage. To this end, it first compresses the resolution information using a good lossy source-code for the setup in Figure 1, where the side-information at the receivers is given by their channel outputs in the first stage. It then sends the compression indices over the BC so that the receivers can decode them. With the lossy reconstructions of the resolution information learned in the second stage and the outputs from the first stage the receivers then decode the desired messages.

REFERENCES

On Gaussian Channels with MMSE Interference

Ronit Bustin and Shlomo Shamai (Shitz)
Department of Electrical Engineering, Technion-Israel Institute of Technology.
Technion City, Haifa 32000, Israel; Email: bustin@tx.technion.ac.il, sshlomo@ee.technion.ac.il

Abstract—We examine codes, over the additive Gaussian noise channel, designed for for reliable communication at some specific signal-to-noise ratio (snr) and constrained by the permitted MMSE at some lower snr. We show that the maximum possible rate is the one attained by superposition codebooks. Moreover, the MMSE function of codes attaining this maximum rate under the MMSE constraint is completely defined for all snrs. The problem is also extended to the maximization of the rate under two MMSE constraints. The optimal rate is again achieved by three-layers superposition codes.

I. INTRODUCTION

Capacity and capacity achieving codes have been the main concern of Information Theory from the very beginning. Trying to design capacity achieving codes is a central goal of many researchers in this field. Recently some emphasis has been given to the research of non-capacity achieving point-to-point codes [1], [2]. These codes, referred to as “bad” point-to-point codes [2], are heavily used in many multi-terminal wireless networks. In [3] it was shown that the mutual information and thus also the minimum mean square error (MMSE) of “good” (capacity achieving) point-to-point codes is known exactly, no matter the specific structure of the code. Furthermore, it is known that “bad” codes can obtain lower MMSE at low signal-to-noise ratios (snrs) [2]. This advantage is meaningless in point-to-point communication, where all that matters is the performance at the receiver. However, in multi-terminal wireless networks, such as a cellular network, the case is different. In such networks there are two fundamental phenomena: interference from one node to another (an interference channel), and the potential cooperation between nodes (a relay channel). In the interference channel, where a message sent to an intended receiver acts as interference to other receivers in the network, a lower MMSE implies better interference cancelation, and thus improved rates for the interfered user. The performance of optimal point-to-point codes in the interference setting was the investigation in [4].

The best known achievable region for the two-user interference channel is given by the Han and Kobayashi (HK) scheme [5]. This scheme uses partial decoding of the interfering message at the receiver. Rate splitting (that is, superposition coding) is a special case of the HK scheme, and is also point-to-point “bad” (see [1, Appendix VIII-C]). It was shown in [6] that these codes are close to optimal for the Gaussian interference channel, and in fact are within one bit from capacity. In this work we show that these codes are in fact optimal MMSE-wise.

Although it is known that we can obtain an advantage, MMSE-wise, when using “bad” codes, the question “how much better can we do, given a looser requirement on the rate?” is still open. In this work we answer this question for the additive Gaussian noise channel showing that superposition codebooks, optimal for a specific Gaussian broadcast channel (BC) are optimal in this sense. We further extend the question to the case of two MMSE constraints in lower snrs, and show that three-layers superposition codebooks attain the maximum possible rate. This result can also be extended to the general K receiver case.

A similar question has been raised in the work of Bandemer and El Gamal [7], where they provide the rate-disturbance region: for any given rate that can be transmitted reliably to the intended receiver, what is the minimum possible disturbance that can be attained at some interfered user. In [7] the authors measure the disturbance using the mutual information between the codeword and the output at the interfered user, rather than the minimum possible MMSE, as done here. We further discuss and compare the two measures in our concluding remarks (section IV).

II. PROBLEM FORMULATION AND PRELIMINARY RESULTS

In this work we are looking at the transmission of code-words, of length \( n \), through a discrete memoryless standard Gaussian channel:

\[
Y = \sqrt{\gamma} X + N \tag{1}
\]

where \( N \) is standard additive Gaussian noise. The codewords are constrained by the standard average power constraint: \( \forall x \in C_n \quad \frac{1}{n} \sum_{i=1}^{n} x_i^2 \leq 1 \), where \( C_n \) stands for a code of \( n \)-dimensional codewords. We examine codebooks designed for reliable transmission at \( \gamma = \text{snr}_2 \) (reliable decoding of the codeword from \( Y(\gamma = \text{snr}_2) \)). Our main interest will be in examining non-optimal codes, alternatively known as “bad” codes [2], defined using code-sequences, as follows:

**Definition 1:** A non-optimal code-sequence \( C = \{C_n\}_{n=1}^{\infty} \), for a channel with capacity \( C \), is a code-sequence with vanishing error probability and rate satisfying \( \lim_{n \to \infty} \frac{1}{n} \log M_n < C \) where \( M_n \) is the size of code \( C_n \).

Their associated MMSE defined as:

\[
\text{MMSE}^C(\gamma) = \lim_{n \to \infty} \text{MMSE}_{C_0} (\gamma) = \lim_{n \to \infty} \frac{1}{n} \text{Tr}(E_X(\gamma)) \tag{2}
\]

where \( E_X(\gamma) \) is the MMSE matrix when estimating the codeword \( X \) from the output of the channel \( Y = \sqrt{\gamma} X + N \). We further define the following for abbreviation:

\[
I(\gamma) = \lim_{n \to \infty} I_n(\gamma) = \lim_{n \to \infty} \frac{1}{n} I(X; Y(\gamma)) \tag{3}
\]
Surely, for any such codes, the error probability for any \( \gamma > \text{snr}_2 \) is zero, when \( n \to \infty \), since reliable transmission is guaranteed at \( \text{snr}_2 \). As a result \( \text{MMSE}^e(\gamma) \) for these \( \text{snr}_s \) is also zero. On the other hand, for \( \gamma < \text{snr}_2 \) the value of the error probability is not guaranteed to be any specific value. For an optimal code, it was shown in [3], that for Gaussian i.i.d. input and thus \( \text{MMSE}^e(\gamma) \) is also known exactly and descends gradually according to \( \frac{1}{1+\gamma} \).

Our goal is to find a code-sequence which both attains a minimum required rate at \( \text{snr}_2 \), denoted as \( I(\text{snr}_2) \geq \frac{1}{2}\log (1 + \alpha^2 \text{snr}_2) \), for some predetermined \( \alpha \in (0, 1] \), and secondly, obtains the minimum possible \( \text{MMSE} \) at some \( \text{snr}_1 < \text{snr}_2 \). Clearly, if \( \alpha = 1 \) we have the maximum rate at \( \text{snr}_2 \), attainable only by an optimal code-sequence. As mentioned above, this is a well understood case [3]. For \( \alpha \leq \frac{\text{snr}_1}{\text{snr}_2} \) we also have an obvious solution, since for these low rates we can obtain zero \( \text{MMSE}^e(\text{snr}_1) \) by simply choosing an optimal code-sequence of rate \( \frac{1}{2}\log (1 + \alpha^2 \text{snr}_1) \). Thus, the interesting range of parameters is \( \frac{\text{snr}_1}{\text{snr}_2} < \alpha < 1 \), for which the minimum attainable \( \text{MMSE}^e(\text{snr}_1) \) is unknown. This problem is equivalent to maximizing the rate at \( \text{snr}_2 \), given some constraint on the maximum allowed \( \text{MMSE} \) at \( \text{snr}_1 \). In this formulation the obvious extension, motivated by multi-user interference channels, is to maximize the rate at \( \text{snr}_2 \), given two \( \text{MMSE} \) constraints. In this work we proceed with this view of the problem.

A. The I-MMSE Approach

The approach used in order to provide insight into the above mentioned problem is the I-MMSE approach, this to say that we make use of the fundamental relationship between the mutual information and the \( \text{MMSE} \) in the Gaussian channel and its generalizations [8], [9]. Even though we are examining a scalar Gaussian channel, the \( n \)-dimensional version of this relationship is required since we are looking at the transmission of \( n \)-dimensional codewords through the channel. In our setting the relationship is as follows:

\[
I_n(\text{snr}) = \frac{1}{2} \int_0^{\text{snr}} \text{MMSE}^e(\gamma) \, d\gamma.
\]

Taking the limit of \( n \to \infty \) on both sides results with:

\[
I(\text{snr}) = \frac{1}{2} \int_0^{\text{snr}} \text{MMSE}^e(\gamma) \, d\gamma.
\]

The main property of the I-MMSE used for these proofs is an \( n \)-dimensional “single crossing point” property derived in [10] given here for completeness. This property is an extension of the scalar “single crossing point” property shown in [11]. In [10] the following function is defined as an arbitrary random vector \( X \):

\[
q_A(\mathbf{X}, \sigma^2, \gamma) = \frac{\sigma^2}{1 + \sigma^2 \gamma} \text{Tr}(A) - \text{Tr}(AE\mathbf{X}(\gamma))
\]

where \( A \) is some \( n \times n \) general weighting matrix. The following theorem is proved in [10].

Theorem 1 ([10]): Let \( A \in \mathbb{S}^n_+ \) be a positive semidefinite matrix. Then, the function \( \gamma \mapsto q_A(\mathbf{X}, \sigma^2, \gamma) \), defined in (6), has no nonnegative-to-negative zero crossings and, at most, a single negative-to-nonnegative zero crossing in the range \( \gamma \in [0, \infty) \). Moreover, let \( \text{snr}_0 \in [0, \infty) \) be that negative-to-nonnegative crossing point. Then,

1. \( q_A(\mathbf{X}, \sigma^2, 0) < 0 \).
2. \( q_A(\mathbf{X}, \sigma^2, \gamma) \) is a strictly increasing function in the range \( \gamma \in [0, \text{snr}_0) \).
3. \( q_A(\mathbf{X}, \sigma^2, \gamma) > 0 \) for all \( \gamma \in [\text{snr}_0, \infty) \).
4. \( \lim_{\gamma \to \infty} q_A(\mathbf{X}, \sigma^2, \gamma) = 0 \).

In this work, the matrix \( A \) can be set to the identity matrix. The above property is valid for all natural \( n \), thus we may also take \( n \to \infty \).

B. Superposition Coding

An important family of non-optimal codes, that is, a family of codes that do not attain the point-to-point capacity at \( \text{snr}_2 \), is that of Gaussian superposition codes which are optimal for a degraded Gaussian BC [12]. As will be shown in the sequel these codes are optimal MMSE-wise. The analysis of this family was done by Merhav et. al. in [13, section 5.3] from a statistical physics perspective. As noted in [13], the MMSE of this family of codebooks undergoes phase transitions, that is, it is a discontinuous function of \( \gamma \). The mutual information, \( I(\gamma) \), and \( \text{MMSE}^e(\gamma) \) of this family of codebooks is known exactly and given in the next theorem. An example is depicted in Figure 1.

Theorem 2 ([13] section 5.3): A superposition codebook designed for \( (\text{snr}_0, \text{snr}_1, \cdots, \text{snr}_K) \) with the rate-splitting coefficients \( (\beta_0, \cdots, \beta_{K-1}) \) has the following \( I(\gamma) \):

\[
\begin{align*}
\frac{1}{2} \log (1 + \gamma), & \quad 0 \leq \gamma < \text{snr}_0, \\
\frac{1}{2} \log \left( \frac{1}{1 + \text{snr}_0} \prod_{j=1}^K (1 + \frac{\beta_0 + \cdots + \beta_{j-1}}{\beta_j + \cdots + \beta_{K-1}} \text{snr}_j) \right) + \frac{1}{2} \log (1 + \beta_0 \gamma), & \quad \text{snr}_0 \leq \gamma < \text{snr}_1, \\
\frac{1}{2} \log \left( \frac{1}{1 + \text{snr}_1} \prod_{j=1}^{K-1} (1 + \frac{\beta_0 + \cdots + \beta_{j-1}}{\beta_j + \cdots + \beta_{K-1}} \text{snr}_j) \right) + \frac{1}{2} \log (1 + \beta_{K-1} \text{snr}_{K-1}), & \quad \text{snr}_K < \gamma
\end{align*}
\]

and the following \( \text{MMSE}^e(\gamma) \):

\[
\text{MMSE}^e(\gamma) = \begin{cases} \\
\frac{1}{1 + \beta_j \gamma}, & 0 \leq \gamma < \text{snr}_0, \\
\frac{\text{snr}_j}{\beta_j + \cdots + \beta_{K-1}}, & \text{snr}_j \leq \gamma < \text{snr}_{j+1}, \\
0, & \text{snr}_{j+1} < \gamma \end{cases}
\]

III. Main Results

The main result is given in the next theorem.

Theorem 3: Assuming \( \text{snr}_1 < \text{snr}_2 \) the solution of the following optimization problem,

\[
\max \ I(\text{snr}_2) \\
\text{s.t. } \text{MMSE}^e(\text{snr}_1) \leq \frac{\beta}{1 + \beta \text{snr}_1}
\]

for some \( \beta \in [0, 1] \), is the following

\[
I(\text{snr}_2) = \frac{1}{2} \log (1 + \beta \text{snr}_2) + \frac{1}{2} \log \left(1 + \frac{\text{snr}_1}{1 + \beta \text{snr}_1}\right)
\]
and is attainable when using the optimal Gaussian superposition codebook designed for \((\text{snr}_1, \text{snr}_2)\) with rate-splitting coefficient \(\beta\).

**Proof:** It is simple to verify that the optimal Gaussian superposition codebook complies with the above MMSE constraint and attains the maximum rate. Thus, the focus of the remainder of the proof is on deriving a tight upper bound on the rate. We prove an equivalent claim, by assuming a code of rate \(R_c = \frac{1}{2} \log (1 + \alpha \text{snr}_2)\), designed for reliable transmission at \(\text{snr}_2\), and deriving a lower bound on \(\text{MMSE}^c(\text{snr}_1)\).

If \(\alpha \text{snr}_2 \leq \gamma \leq 1\) the lower bound is trivially zero using the optimal Gaussian codebook designed for \(\alpha \text{snr}_2\). This is equivalent to setting \(\beta = 0\) in which case we obtain the rate \(I(\text{snr}_2) = \frac{1}{2} \log (1 + \text{snr}_1)\) using an optimal Gaussian codebook (no superposition). Thus, we assume \(\gamma \leq \alpha \text{snr}_2\).

Using the trivial upper bound on \(I(\gamma) \leq \frac{1}{2} \log (1 + \gamma)\) (due to maximum entropy), we can lower bound the following difference, for any \(\gamma < \alpha \text{snr}_2\):

\[
I(\text{snr}_2) - I(\gamma) \geq I(\text{snr}_2) - \frac{1}{2} \log (1 + \gamma). \tag{10}
\]

Using the I-MMSE relationship (5), the above translates to the following inequality:

\[
\frac{1}{2} \int_{\gamma}^{\text{snr}_2} \text{MMSE}^c(\tau) \, d\tau \geq R_c - \frac{1}{2} \log (1 + \gamma) \tag{11}
\]

\[
= \frac{1}{2} \log (1 + \alpha \text{snr}_2) - \frac{1}{2} \log (1 + \gamma).
\]

Defining \(d\) through the following equality:

\[
\frac{1}{2} \log (1 + \alpha \text{snr}_2) - \frac{1}{2} \log (1 + \gamma) = \frac{1}{2} \log (1 + d \text{snr}_2) - \frac{1}{2} \log (1 + d \gamma). \tag{12}
\]

it is simple to check that for \(\gamma < \alpha \text{snr}_2\), \(d\) is in the range of \((0, 1)\). Now we can continue with equation (11):

\[
\frac{1}{2} \int_{\gamma}^{\text{snr}_2} \text{MMSE}^c(\tau) \, d\tau \geq \frac{1}{2} \log (1 + d \text{snr}_2) - \frac{1}{2} \log (1 + d \gamma)
\]

\[
= \frac{1}{2} \int_{\gamma}^{\text{snr}_2} \text{MMSE}_G(\tau) \, d\tau. \tag{13}
\]

where \(\text{MMSE}_G(\tau)\) is the MMSE assuming a Gaussian random variable with variance \(d\) through the additive Gaussian channel at \(\text{snr} = \tau\). The single crossing point property (Theorem 1, with \(A = I\)) tells us that \(\text{MMSE}^c(\tau)\) and \(\text{MMSE}_G(\tau)\) cross each other at most once, and after that crossing point \(\text{MMSE}_G(\tau)\) remains an upper bound. From the inequality in (13) we can thus conclude that the single crossing point, if exists, will occur in the region \((\gamma, \infty)\). Thus, for \(\gamma\) we have the following lower bound:

\[
\text{MMSE}^c(\gamma) \geq \frac{d(\gamma)}{1 + d(\gamma) \gamma} = \frac{\alpha \text{snr}_2 - \gamma}{\text{snr}_2 - \gamma} \frac{1}{1 + \gamma}.
\]

A similar derivation can be done for any \(\gamma < \alpha \text{snr}_2\), and will result with a different \(d(\gamma)\). Specifically for \(\gamma = \text{snr}_1\) we obtain

\[
\text{MMSE}^c(\text{snr}_1) \geq \frac{\alpha \text{snr}_2 - \text{snr}_1}{\text{snr}_2 - \text{snr}_1} \frac{1}{1 + \text{snr}_1}.
\]

Deriving \(\alpha\) as a function of the constraining \(\beta\), and substituting in \(R_c = \frac{1}{2} \log (1 + \alpha \text{snr}_2)\) results with the superposition rate given in (9).

An interesting question to ask is whether there could be a different code that can attain maximum rate under the MMSE constraint at \(\text{snr}_1\) and also provide better MMSE for other values of \(\text{snr}\). The answer is to the negative, and is given in the next theorem, proof of which is omitted and can be found in [14].

**Theorem 4:** From the set of reliable codes of rate \(R_c = \frac{1}{2} \log (1 + \beta \text{snr}_2)\) + \(\frac{1}{2} \log (\frac{1 + \text{snr}_1}{1 + \text{snr}_2})\), complying with the MMSE constraint at \(\text{snr}_1\), the superposition codebook provides the minimum MMSE for all \(\text{snr}\).

Two MMSE Constraints: We now wish to extend the result of Theorem 3 to the case of two constraints:

**Theorem 5:** Assuming \(\text{snr}_0 < \text{snr}_1 < \text{snr}_2\) the solution of the following optimization problem,

\[
\max \quad I(\text{snr}_2)
\]

\[\text{s.t.} \quad \text{MMSE}^c(\text{snr}_0) \leq \frac{\beta_1}{1 + \beta_1 \text{snr}_1} \]

\[
\quad \text{MMSE}^c(\text{snr}_0) \leq \frac{\beta_0}{1 + \beta_0 \text{snr}_0} \tag{14}
\]

for some positive \(\beta_1, \beta_0\) such that \(\beta_1 + \beta_0 \leq 1\) and \(\beta_1 < \beta_0\), is the following

\[
I(\text{snr}_2) = \frac{1}{2} \log \left( \frac{1 + \beta_1 \text{snr}_2}{1 + \beta_1 \text{snr}_1} \right) \frac{1 + \beta_0 \text{snr}_0}{1 + \beta_0 \text{snr}_0}.
\]

and is attainable when using the optimal three-layers Gaussian superposition codebook designed for \((\text{snr}_0, \text{snr}_1, \text{snr}_2)\) with rate-splitting coefficients \((\beta_0, \beta_1)\).
When $\beta_0 < \beta_1$ the first constraint can be removed and we return to the case of a single constraint given in Theorem 3.

**Proof:** It is simple to verify that the optimal Gaussian three-layers superposition codebook complies with the above MMSE constraints and attains the maximum rate. Thus, we need to derive a tight upper bound on the rate. Deriving the upper bound begins with the usage of Theorem 3 on $I(snr_1)$, when we take into consideration only the constraint on $\text{MMSE}^c(snr_0)$. This provides the following upper bound:

$$I(snr_1) \leq \frac{1}{2} \log \left(1 + \frac{\beta_1}{\beta_1 + \beta_2} snr_1 \right) + \frac{1}{2} \log \left(1 + \frac{\beta_1 \beta_2}{\beta_1 + \beta_2} \right)$$

(15)

On the other hand, using the I-MMSE approach we have:

$$I(snr_2) - I(snr_1) = \frac{1}{2} \int_{snr_1}^{snr_2} \text{MMSE}^c(\tau) d\tau \leq \frac{1}{2} \int_{snr_1}^{snr_2} \text{mmse}_{G}(\tau) d\tau$$

where $\text{mmse}_{G}(\tau)$ is the MMSE assuming a Gaussian random variable with variance $\beta_1$. This inequality is valid since according to the first constraint we have

$$\text{MMSE}^c(snr_1) \leq \frac{\beta_1}{1 + \beta_1 snr_1} = \text{mmse}_{G}(snr_1)$$

(16)

thus, according to the single crossing point property

$$\text{MMSE}^c(\tau) \leq \text{mmse}_{G}(\tau), \forall \tau \geq snr_1$$

(17)

leading to the inequality in equation (16). Putting together (15) and (16) we obtain the desired upper bound.

**IV. DISCUSSION AND CONCLUSIONS**

These results provide the engineering insight to the good performance of the HK superposition scheme on the two-user interference channel, as shown in [6]. From our results, that show that the HK superposition scheme, is optimal MMSE-wise, we can conclude that one cannot construct better codes of the type defined in [1], [2] that will beat HK, through the use of estimation. Note that, as mentioned in [1, section V], the codes constructed there have an important complexity advantage over HK codes. Furthermore, keep in mind that the HK scheme is efficient in the two-user interference channel and a simple approach in the general $K$-user interference channel. Finally, we expect that the I-MMSE approach to shed further light on the capacity region of the two-user interference channel itself.

As mentioned in the introduction, Corollary 2 in [7] can also be derived directly from the I-MMSE formulation. Using our notation, we begin with the MMSE rate. Since, $0 \leq I(snr_1) \leq \frac{1}{2} \log \left(1 + \alpha^* snr_1 \right)$ there exists an $\alpha^* \in [0, 1]$ such that $R_d = \frac{1}{2} \log \left(1 + \alpha^* snr_1 \right)$. Thus, the averaged MMSE of the code crosses the MMSE of a scalar Gaussian input with power $\alpha^*$ in the range $[0, snr_1]$. Now, using the I-MMSE,

$$I(snr_2) = \frac{1}{2} \log \left(1 + \alpha^* snr_1 \right) + \frac{1}{2} \int_{snr_1}^{snr_2} \text{MMSE}^c(\gamma) d\gamma$$

$$\leq \frac{1}{2} \log \left(1 + \alpha^* snr_2 \right)$$

(18)

where the last transition is due to the “single crossing point” property which ensures that the MMSE of the scalar Gaussian input with power $\alpha^*$ will remain an upper bound on $\text{MMSE}^c(\gamma)$ in the range $[snr_1, \infty)$. Moreover, the above derivation does not indicate a superposition coding scheme, but rather a Gaussian code with reduced power of $\alpha^*$. Such a scheme, which attains the required minimum rate at $snr_2$, does not attain the minimum MMSE at $snr_1$. Extending to two mutual information disturbance constraint is trivial, as only the most constraining one determines the result. Thus, the different measurement of “disturbance” suggested here is conceptually different than the one suggested in [7].

Finally, the two MMSE constraints solution, presented here, can be directly extended to the $K$-MMSE constraint, as shown in [15].

**ACKNOWLEDGMENT**

This work has been supported by the Israel Science Foundation (ISF) and the CORNET Consortium. Ronit Bustin is supported by the Adams Fellowship Program of the Israel Academy of Sciences and Humanities.

**REFERENCES**


On the Gaussian Listening-Helper Source-Coding Problem

Shraga I. Bross∗, and Haim Permuter†
∗ Engineering Department , Bar-Ilan University, Ramat Gan, 52900, Israel
Email: brosss@biu.ac.il
† Department of Electrical and Computer Engineering, Ben-Gurion University of the Negev, Beer-Sheva
Email: haimp@bgu.ac.il

Abstract— In the Gaussian listening-helper source-coding problem Encoder 1 and Decoder 1 observe respectively a pair of i.i.d. correlated Gaussian sources and both wish to communicate the first source to Decoder 2 subject to a distortion constraint. Encoder 1 sends a message to both decoders and then Decoder 1 — the listening-helper — sends a message just to Decoder 2.

We derive an inner bound on the rate region of this problem by proposing a Gaussian achievable scheme. This inner bound coincides with the solution to the Gaussian optimization problem associated with a single-letter outer bound corresponding to this problem.

Index Terms—multi-terminal source coding, listening-helper problem.

I. INTRODUCTION

The Gaussian listening-helper source-coding problem that we consider is depicted in Fig. 1. Encoder 1 observes a scalar i.i.d. Gaussian source $X$ that is correlated with a scalar i.i.d. source $Y$ observed by Decoder 1. Encoder 1 wishes to communicate the source $X$ to within certain distortion constraint to Decoder 2 by sending a message at rate $R$ to both decoders. Decoder 1 (the listening-helper) is allowed to communicate to Decoder 2 by sending a message at rate $R_1$.

Decoder 2 uses both messages to form its estimate of the source $X$. The goal is to determine the set of all rate pairs $(R,R_1)$ that satisfy the distortion constraint.

We derive an inner bound on the rate region for this source-coding problem by proposing a Gaussian scheme in which Encoder 1 quantizes its observation using a Gaussian test channel and then compresses the quantized values using proper binning. Decoder 1 quantizes its observation using another test channel and finally, both Encoder 1 and Decoder 1 cooperate to provide Decoder 2 with the enumeration information it needs in order to resolve its ambiguity regarding the compressed information Encoder 1 had generated. Furthermore, we show that the Gaussian solution associated with an upper bound for our problem coincides with the proposed Gaussian achievable scheme.

The paper is organized as follows. In Section II we provide a formal definition of the Gaussian listening-helper source-coding model. In Section III we present our main result, while Section IV is devoted to the description of the main steps of the proof.

The work of S. Bross was supported by the Israel Science Foundation under Grant 497/09.

II. PROBLEM FORMULATION

The core problem we consider, the listening-helper source-coding problem, is described as follows. Let $\{(X_i,Y_i)\}_{i=1}^n$ be a pair of zero-mean Gaussian random vectors generated by i.i.d drawings of a pair of jointly Gaussian random variables with variance $\sigma_X^2$ and $\sigma_Y^2 = a_i^2 \sigma_X^2 + \sigma_{W_i}^2$, respectively. With no loss of generality, we can write

$$Y_i = a_X X_i + N_{i(y)}^y,$$

where $N_{i(y)}^y \sim \mathcal{N}(0,\sigma^2_{W_i})$ is independent of $X_i$.

Encoder 1 which observes $X^n$ sends a message to both decoders using an encoding function

$$f^{(n)}: X^n \to \{1,2,\ldots,M^{(n)}\},$$

where $X^n$ denotes the set of $n$-vectors over $X$. Based on $f^{(n)}(X^n)$ and its observation $Y^n$, Decoder 1 sends a message to Decoder 2 using an encoding function

$$f_1^{(n)}: \{1,2,\ldots,M^{(n)}\} \times Y^n \to \{1,2,\ldots,M_1^{(n)}\}.$$

Decoder 2 then uses both received messages to estimate $X^n$ using a reproduction function

$$g^{(n)}: \{1,2,\ldots,M^{(n)}\} \times \{1,2,\ldots,M_1^{(n)}\} \to \hat{X}_2^n.$$

Definition 1: A rate-distortion triple $(R,R_1,D_2)$ is achievable for the Gaussian listening-helper source-coding problem if there exists a block length $n$, encoders $f^{(n)}$ and $f_1^{(n)}$, and a decoder $g^{(n)}$ such that,

$$R \geq \frac{1}{n} \log M^{(n)}$$

$$R_1 \geq \frac{1}{n} \log M_1^{(n)}$$

$$D_2 \geq \frac{1}{n} \sum_{i=1}^n \mathbb{E}[(X_i - \hat{X}_{2,i})^2].$$

Let $\mathcal{R}(D_2)$ be the closure of the set of achievable rate-distortion triples. The rate region $\mathcal{R}(D_2)$ for the Gaussian listening-helper source-coding problem is defined by

$$\mathcal{R}(D_2) = \left\{(R,R_1): (R,R_1,D_2) \in \mathcal{R}(D_2) \right\}.$$
Since we are interested in the Mean-Square-Error (MSE) distortion constraint we can restrict the reproduction function to be the MMSE estimate of $X^n$ given $f^{(n)}(X^n)$ and $f_1^{(n)}(f^{(n)}(X^n), Y^n)$, that is

$$
X^n = \mathbb{E}\left[X^n|f^{(n)}(X^n), f_1^{(n)}(f^{(n)}(X^n), Y^n)\right].
$$

III. MAIN RESULTS

Our main result is a characterization of an inner bound on the rate-region for the Gaussian listening-helper source-coding problem.

\textbf{Proposition 1:} For a positive number $D_2 \leq \sigma_X^2$ the rate-region $\mathcal{R}(D_2)$ contains the rate region $\mathcal{R}_C(D_2)$ defined by

$$
\mathcal{R}_C(D_2) = \bigcup_{\sigma_{W_u}^2, \sigma_{W_v}^2} (R, R_1, R_2),
$$

\begin{align*}
R &\geq \frac{1}{2} \log \left[1 + \sigma_X^2 \sigma_{W_u}^2 \sigma_{W_v}^2 \left(\frac{1}{\sigma_W^2} + \frac{1}{\sigma_{W_v}^2} + \frac{1}{\sigma_{W_u}^2}\right)\right], \\
R_1 &\geq \frac{1}{2} \log \left[1 + \frac{\sigma_X^2 \sigma_{W_u}^2 \sigma_{W_v}^2}{\sigma_W^2} \left(\frac{1}{\sigma_{W_u}^2} + \frac{1}{\sigma_{W_v}^2} + \frac{1}{\sigma_{W_u}^2}\right)\right], \\
R + R_1 &\geq \frac{1}{2} \log \left[1 + \frac{\sigma_X^2 \sigma_{W_v}^2}{\sigma_{W_u}^2} \left(\frac{1}{\sigma_{W_v}^2} + \frac{1}{\sigma_{W_u}^2}\right)\right], \\
D_2 &= \frac{1}{2} \log \left[1 + \frac{\sigma_X^2}{\sigma_{W_u}^2} \left(\frac{1}{\sigma_{W_v}^2} + \frac{1}{\sigma_{W_u}^2}\right)\right].
\end{align*}

A. A Gaussian achievable scheme

A natural Gaussian achievable scheme for the listening-helper problem is described as follows. Let $S(U, V)$ be the set of zero-mean jointly Gaussian random variables $U$ and $V$ such that

1) $U \circ X \circ Y$ and $X \circ UY \circ V$ are Markov chains.
2) $\sigma_X^2(\mathbb{E}|U, V) \leq D_2$.

For any $(U, V) \in S(U, V)$ and a large block-length $n$:

- Generate $e^{n[I(X;U)+\epsilon]}$, $\epsilon > 0$ independent codewords $u_1, \ldots, u_{e^{n[I(X;U)+\epsilon]}}$ randomly according to $p_U$. Assign these codewords uniformly into $e^{nR}$ bins. Label them $u(j, l), j \in \{1, \ldots, e^{n[R+\epsilon]}\}, l \in \{1, \ldots, e^{nR}\}$. Share the codebook and its partition between Encoder 1 and both decoders.
- For each $u(j, l)$ generate $e^{n[R_1+\epsilon]}$, $\epsilon > 0$ independent codewords randomly according to $p_{V|U}$. Label the codewords by $v(j, l, k), k \in \{1, \ldots, e^{n[R_1+\epsilon]}\}$ and share this codebook between Decoder 1 and Decoder 2.

Given a source and a side-information sequence pair $(x, y)$:

1) Encoder 1 looks for the codeword $u(j, l)$ that is jointly typical with $x$ and sends its index $l$ to both decoders.
2) Encoder 1 and Decoder 1 send together the enumeration index $j$ to Decoder 2.
3) Decoder 1 looks for the codeword $v(j, l, k)$ that is jointly typical with $(u(j, l), y)$, and sends the index $k$ of that codeword to Decoder 2.

Decoder 1 can recover $u$ with high probability provided that

$$
R \geq I(X; U| Y).
$$

Decoder 1 can compute $v$ with high probability provided that

$$
R_1 \geq I(Y; V| U),
$$

and taking into account that Encoder 1 and Decoder 1 join efforts in sending the index $j$ to Decoder 2 we obtain

$$
R + R_1 \geq I(X; U) + I(Y; V| U).
$$

Decoder 2 computes the MMSE estimate of the source sequence $X^n$ given $(U^n, V^n)$ and condition 2 above guarantees that the estimate meets the desired distortion.

The following lemma characterizes an achievable rate-region based on this scheme.

\textbf{Lemma 1:} A Gaussian achievable scheme as above which satisfies the long Markov chain $U \circ X \circ Y \circ V$ achieves $\mathcal{R}_C(D_2)$. Moreover, the Gaussian solution associated with an upper bound for our problem coincides with $\mathcal{R}_C(D_2)$.

In Section IV.B we show that for Gaussian $(U, V) \in S(U, V)$ such that $U \circ X \circ Y \circ V$ the rate region associated with (7)-(9) equals $\mathcal{R}_C(D_2)$.

IV. PROOFS

The source-coding problem considered next will be used to show that the Gaussian solution associated with an upper bound for our main problem equals $\mathcal{R}_C(D_2)$.

A. A source-coding sub-problem

Let $\{(X_i, Y_i, Z_i)\}_{i=1}^n$ be a sequence of independent drawings of a triplet of zero-mean jointly Gaussian random variables with covariance $K_{(X,Y,Z)}$. An encoder observes $Y^n$ while both the encoder and the decoder have access to the side-information $Z^n$. The encoder sends a message to the decoder using an encoding function

$$
f^{(n)}_E: Y^n \times Z^n \rightarrow \{1, 2, \ldots, M^{(n)}\}.
$$

Based on $f^{(n)}_E(Y^n, Z^n)$ and its side-information $Z^n$ the decoder forms an estimate for $X^n$ using a reproduction function

$$
g^{(n)}_D: \{1, 2, \ldots, M^{(n)}\} \times Z^n \rightarrow X^n.
$$
This system is shown in Fig. 2. For a given distortion

\[ D \geq 1 \frac{1}{n} \sum_{i=1}^{n} E \left[ (X_i - \hat{X}_i)^2 \right]. \]  

(12)

Here also since we are interested in the MSE distortion constraint we can restrict the reproduction function to be the MMSE estimate of \( X^n \) given \( f_E^{(n)}(Y^n, Z^n) \) and \( Z^n \), that is

\[ \hat{X}^n = E \left[ X^n | f_E^{(n)}(Y^n, Z^n), Z^n \right]. \]

For a given distortion \( D > 0 \), define \( P_0(D) \) as the set of laws \( p_{XYZV}(x, y, z, v) \), \( x, y, z, v \in \mathbb{R} \), such that the marginal law \( f \) \( p_{XYZV} \) identifies with \( p_{XYZ} \), and

\[ E \left[ (X - E(X|V, Z))^2 \right] \leq D. \]

Then, by a modification of \([4, \text{sec. 6.1.1}]\), we have that

\[ R_E \geq R_{Y|Z}(D) = \min_{p_{XYZV} \in P_0(D)} I(Y; V|Z). \]  

(13)

Consequently, define an optimization problem \( P \) as follows

\[ \max \ h(Y|VZ) \]

subject to

\[ D \geq \sigma_{Y|VZ}^2, \]

(14)

then let \( \hat{P}_G[D, (X, Y, Z), \sigma_{Y|VZ}^2] \) be the corresponding optimization problem assuming \( V \) is Gaussian and denote by \( \varphi \left( \hat{P}_G[D, (X, Y, Z), \sigma_{Y|VZ}^2] \right) \) the conditional variance \( \sigma_{Y|VZ}^2 \) associated with the optimal value of \( \hat{P}_G \).

Consequently, \( \hat{P}_G \) may be expressed as

\[ R_{Y|Z}(D) = \min_{p_{XYZV} \in P_0(D)} 2 \frac{\log \sigma_{Y|VZ}^2}{\sigma_{Y|VZ}^2}. \]  

(15)

On the other hand, when \( Z^n \) is available just at the decoder, - i.e. \( \hat{f}_E^{(n)} = f_E^{(n)}(Y^n) \), by a modification of \([2]\), we have that

\[ R_E \geq R_{Y|Z}^{(n)}(D) = \min I(Y; V|Z), \]

(16)

where the minimization is over the set of laws \( \mathcal{P}(D) \) defined by

\[ p_{XYZV}(x, y, z, v) = p_{XYZ}(x, y, z) p_{V|Y}(v|y). \]

Consequently,

\[ R_{Y|Z}^{(n)}(D) = \min_{p_{XYZV} : \varphi(D) \geq D} 2 \frac{\log \sigma_{Y|VZ}^2}{\sigma_{Y|VZ}^2}. \]  

(17)

In \([3, \text{Section 3}]\) the author shows that, when the encoder observes the source sequence \( X^n \) i.e. \( Y = X \), both optimization problems (15) and (18) have the same solution and, in fact, the additional Markov relation \( Z \circ X \circ V^2 \) in (18) characterizes the optimal solution of (15). The following lemma asserts that the same is true when the encoder observes a correlated random variable \( Y \) which satisfies a Markov relation.

**Lemma 2:** For jointly Gaussian random variables \( (X, Y, Z) \) satisfying \( Z \circ X \circ Y \), both optimization problems (15) and (18) have the same solution and, in fact, the additional Markov relation in (18) characterizes the optimal solution of (15).

**Proof:** Omitted.

**B. The Gaussian solution associated with an outer bound**

**Lemma 3:** (Single-letter outer bound) If the rate-distortion triple \( (R, R_1, D_2) \) is achievable then there exist random variables \( (U, V) \) satisfying the Markov relation \( U \circ X \circ Y \), such that

\[ R + R_1 \geq I(X; U) + I(Y; V|U) \]

\[ R \geq I(X; U|Y) \]

\[ R_1 \geq I(Y; V|U) \]

\[ D_2 \geq \sigma_{X|Y,V}^2. \]

(19)

**Proof:** Assume that \( (R, R_1, D_2) \) is achievable. Let \( T = f^{(n)}(X^n) \) and \( T_1 = f_1^{(n)}(f^{(n)}(X^n), Y^n) \), then the rate \( R \) can be lower bounded as follows

\[ nR \geq \log M(n) \geq H(T) \geq H(T|Y^n) \]

\[ = I(X^n; T|Y^n) = \sum_{k=1}^{n} I(X_k; T|Y^{n-1}, X^{k-1}) \]

\[ \geq \sum_{k=1}^{n} I(X_k; U_k|Y_k) \]

\[ \geq \sum_{k=1}^{n} I(X_k; U_k), \]

(20)

where \( X^{k-1} \triangleq (X_1, \ldots, X_{k-1}) \), \( U_k \triangleq (T, Y^{k-1}), Y^{n-k} \triangleq (Y_1, \ldots, Y_{k-1}, Y_{k+1}, \ldots, Y_n) \), and the equality (a) follows by the Markov relation \( X_k \circ U_k \circ Y^n \circ X^{k-1} \).

Let \( V_k \triangleq T_1 \), then the rate \( R_1 \) can be lower bounded as follows

\[ nR_1 \geq \log M_1(n) \geq H(T_1) \geq H(T_1|T) \]

\[ = I(Y^n; T_1|T) = \sum_{k=1}^{n} I(Y_k; T_1|T, Y^{k-1}) \]

\[ = \sum_{k=1}^{n} I(Y_k; V_k|U_k) . \]

(21)
The sum-rate can be lower bounded as follows
\[
\begin{align*}
n(R + R_t) & \geq \log M(n) + \log M_1(n) \\
& \geq H(T) + H(T_t) \geq H(T ; T_t) \\
& = H(T) + H(T_t | T) \\
& = H(T | X^n) + I(T ; Y^n) + H(T_t | T) \\
& = H(T | X^n) + H(T_t | T) + \sum_{k=1}^{n} I(Y_k ; T | Y^{k-1}) \\
& \geq \sum_{k=1}^{n} [I(X_k ; Y_k) + I(Y_k ; V_k | U_k) + I(Y_k ; U_k)] \\
& = \sum_{k=1}^{n} [I(X_k ; Y_k ; U_k) + I(Y_k ; V_k | U_k)] \\
& \geq \sum_{k=1}^{n} [I(X_k ; Y_k ; U_k) + I(Y_k ; V_k | U_k)].
\end{align*}
\]

(22)

Here

(b) follows since \( Y^n \) is a memoryless sequence; and

(c) follows since \( Y_k \), \( X_k \), \( U_k \) is a Markov chain.

By (2) and the memoryless property of the sequence \((X_k, Y_k), k = 1, \ldots, n\) one can verify the Markov relation \( U_k \circ X_k \circ U_k \) which implies the Markov relation \( U \circ X \circ Y \). The combination of (20), (21) and (22) together with the latter Markov relation establishes the desired single-letter lower bound.

Define next an optimization problem \( P_G \) over the conditional variance \( \sigma^2_{X | U \circ V} \) and \( V^G \) as follows

\[
\begin{align*}
\min_{V^G, \sigma^2_{X | U \circ V}} & \quad \frac{1}{2} \log \frac{\sigma^2_X}{\sigma^2_{X | U \circ V} + \sigma^2_{Y | V} + \sigma^2_{V}} \\
\text{subject to} & \quad R \geq \frac{1}{2} \log \frac{\sigma^2_Y}{\sigma^2_{X | U \circ V}}, \quad R_t \geq \frac{1}{2} \log \frac{\sigma^2_{Y | V} + \sigma^2_{U}}{\sigma^2_{V}}, \quad D_2 \geq \sigma^2_{X | U \circ V} \quad \text{and} \quad U^G \circ X \circ Y.
\end{align*}
\]

\( P_G \) is the restriction of the outer bound (19) to a Gaussian law and on account of the Markov relation \( U^G \circ X \circ Y \) and (1) it may be expressed as

\[
\begin{align*}
\min_{V^G, \sigma^2_{X | U \circ V}} & \quad \frac{1}{2} \log \frac{\sigma^2_X}{\sigma^2_{X | U \circ V} + \sigma^2_{Y | V} + \sigma^2_{V}} \\
\text{subject to} & \quad R \geq \frac{1}{2} \log \frac{\sigma^2_Y}{\sigma^2_{X | U \circ V}}, \quad R_t \geq \frac{1}{2} \log \frac{\sigma^2_{Y | V} + \sigma^2_{U}}{\sigma^2_{V}}, \quad D_2 \geq \sigma^2_{X | U \circ V} \quad \text{and} \quad U^G \circ X \circ Y.
\end{align*}
\]

Lemma 4: In the optimization problem \( P_G \) the conditional variance \( \sigma^2_{X | U \circ V} \) is monotonically increasing with \( \sigma^2_{X | U \circ V} \).

**Proof:** By the Markov relation \( U^G \circ X \circ Y \) and (1) we may assume that
\[
U^G = X + N^{(u)},
\]
where \( N^{(u)} \sim \mathcal{N}(0, \sigma^2_{W_u}) \) is independent of \( X \). Then a straightforward computation yields the relation
\[
\sigma^2_{X | U \circ V} = \sigma^2_{W_u} \left( \frac{\sigma^2_{W_u}}{\sigma^2_{X | U}} + \sigma^2_Y \right)^{-1}.
\]

We may express \( P_G \) as a double optimization problem
\[
\begin{align*}
\min_{\sigma^2_{X | U \circ V}, \sigma^2_{Y | V}, \sigma^2_{V}} & \quad \frac{1}{2} \log \left[ 2 \pi e \sigma^2_X \left( \sigma^2_Y + \sigma^2_{W_u} \right) \right] \\
\text{subject to} & \quad R \geq \frac{1}{2} \log \frac{\sigma^2_Y}{\sigma^2_{X | U \circ V}}, \\
& \quad R_t \geq \frac{1}{2} \log \frac{\sigma^2_{Y | V} + \sigma^2_{U}}{\sigma^2_{V}}, \quad D_2 \geq \sigma^2_{X | U \circ V} \quad \text{and} \quad U^G \circ X \circ Y + V^G.
\end{align*}
\]

Let \((X, Y, U^G)\) be jointly Gaussian as per (1) and (23) then the choice of \( V^G = Y + N^{(v)} \) where \( N^{(v)} \sim \mathcal{N}(0, \sigma^2_{W_v}) \) is independent of \((X, N^{(u)}), N^{(u)}\) establishes that the optimal solution to \( P_G \) achieves \( R_G(D_2) \).

**References**


Upper-Bounding Rate Distortion Functions based on the Minimum Mean-Square Error

Meik Dörpinghaus*, Matthias Rüngeler**, and Rudolf Mathar*

*Institute for Theoretical Information Technology, RWTH Aachen University, 52056 Aachen, Germany, {doerpinghaus, mathar}@ti.rwth-aachen.de
**Institute for Communication Systems and Data Processing, RWTH Aachen University, 52056 Aachen, Germany, ruengeler@ind.rwth-aachen.de

Abstract—We derive a new upper bound on the rate distortion function for arbitrary memoryless sources, which is based on the relation between mutual information and minimum mean-square error discovered by Guo et al. This upper bound is in general tighter than the well known upper bound given by the rate distortion function of a Gaussian source with an equal variance found by Shannon and becomes tight for Gaussian sources. We evaluate the new upper bound for various source distributions and compare it to the Shannon lower and upper bound and to the rate distortion function calculated with the Blahut-Arimoto algorithm. This shows that the new upper bound is quite tight.

I. INTRODUCTION AND SETUP

It is well known that the rate distortion function states which rates are in general at least required to describe a source $X$, such that it can be reconstructed up to a given distortion $D$ for a specific distortion measure.

Let $X$ be a random source that generates independent identically distributed (i.i.d.) symbols with respect to the probability distribution function (PDF) $p(x)$, i.e., $X \sim p(x)$. When encoding, source sequences $X^n$ consisting of $n$ source symbols are mapped onto indices

$$f_n : X^n \rightarrow \{1, 2, \ldots, 2^{nR}\}. \quad (1)$$

Here, $R$ is the rate of the encoded sequence. By this mapping the source sequences are represented by $nR$ bits. Based on this index representation the decoder is able to generate an estimate $\hat{X}^n$ of the source sequence $X^n$, i.e., the decoding function is

$$g_n : \{1, 2, \ldots, 2^{nR}\} \rightarrow \hat{X}^n. \quad (2)$$

The encoding and decoding given by the functions $f_n$ and $g_n$ is often referred to as a $(2^{nR}, n)$-rate distortion code.

The question is: How close can the source sequences $X^n$ be reconstructed when they are encoded with rate $R$? I.e., how large is the expected distortion $D$ between the source sequences $X^n$ and their reconstruction $\hat{X}^n$ with

$$D = E[d(X^n, g_n(f_n(X^n)))]$$

where

$$d(x^n, \hat{x}^n) = d(x^n, g_n(f_n(x^n))) = \frac{1}{n} \sum_{i=1}^{n} d(x_i, \hat{x}_i) \quad (3)$$

is the distortion between the source sequence $x^n$ and its reconstruction $\hat{x}^n$. In addition, $d(x_i, \hat{x}_i)$ is the distortion between the individual source symbols $x_i$ and their estimates $\hat{x}_i$.

The distortion $D$ and the rate $R$ form a rate distortion pair $(R, D)$. A rate distortion pair is achievable if a sequence of $(2^{nR}, n)$-rate distortion codes $(f_n, g_n)$ exists such that

$$\lim_{n \rightarrow \infty} E[d(X^n, g_n(f_n(X^n)))] \leq D. \quad (4)$$

The rate distortion function $R(D)$ is defined as the minimum rate $R$ that is required to encode the source $X$ for a given distortion $D$. In [1], [2] Shannon has shown that for an i.i.d. source $X$ with distribution $p(x)$ and bounded distortion function $d(x^n, \hat{x}^n)$ the rate distortion function is given by

$$R(D) = \min_{p(x) \in S} I(X; \hat{X}) \quad (5)$$

where $I(X; \hat{X})$ is the mutual information of $X$ and $\hat{X}$ and

$$S = \left\{ p(\hat{x}|x) \left| \int \int p(\hat{x}|x)p(x)d(x, \hat{x})dxd\hat{x} \leq D \right. \right\} \quad (6)$$

see also [3, Th. 10.2.1]. Minimization in (5) is hence over all $p(\hat{x}|x)$ for which $p(x, \hat{x})$ fulfills the distortion constraint $D$.

For certain distortion measures $d(x, \hat{x})$ and source distributions $p(x)$, $R(D)$ is known. E.g., it is a well known result that for a Gaussian source $X \sim N(0, \sigma^2_X)$ and the mean-square error as distortion measure, i.e., $E[|X - \hat{X}|^2] \leq D$, the rate distortion function is given by

$$R(D) = \left\{ \frac{1}{2} \log \left( \frac{\sigma^2_X}{D} \right) \quad \text{for } 0 \leq D \leq \sigma^2_X, \right. \quad (7)\\ \left. 0 \quad \text{for } D > \sigma^2_X \right\}$$

While for a few combinations of distortion and source distributions the rate distortion functions are known, they are in general unknown. Existing bounds like the Shannon lower bound [2] and the upper bound given by the fact that the rate distortion function for a Gaussian source in (7) is an upper bound to the rate distortion function of arbitrarily distributed sources $X$ with the same variance $\sigma^2_X$, see [1], are in general not tight. This is the motivation for the present work. We derive a new upper bound on the rate distortion function for the mean-square error as distortion measure and arbitrary source distributions. This upper bound is based on the relation between the minimum mean-square error (MMSE) and the mutual information given in [4]. Recently, in [5] this relation has already been applied in the context of rate distortion theory. However, in contrast to the present work [5] does not consider minimization over the reproduction distribution for the study of $R(D)$.

1All logarithms are to the base $e$ and, thus, all rates are in nats.
II. NEW UPPER BOUND ON $R(D)$

**Theorem 1.** Let $X$ be a random source that generates i.i.d. symbols according to $X \sim p(x)$ with $\text{var}(X) = \sigma_X^2$. The minimal required rate $R$ such that $\text{E}[(X - \hat{X})^2] \leq D$ is upper-bounded by

$$R(D) \leq \frac{1}{2} \log \left( 1 + \frac{\sigma_X^2}{\sigma_N^2} \right) - \frac{1}{2} \int_0^\infty \left( \frac{\sigma_X^2}{1 + \sigma_X^2 \gamma} - \text{mmse}(\gamma) \right) d\gamma$$

(8)

where $\text{mmse}(\gamma)$ is the minimum mean-squared error when estimating $X$ disturbed by additive Gaussian noise, i.e.,

$$\text{mmse}(\gamma) = \mathbb{E} \left[ (X - \mathbb{E}[X|X+N])^2 \right]$$

(10)

and where $\gamma$ is the normalized SNR, i.e., $\gamma = \frac{\sigma_X^2}{\sigma_N^2}$. Furthermore, $\sigma_Y^2$ is related to the distortion $D$ by

$$D = \text{mmse}(1/\sigma_Y^2)$$

(11)

$$= \frac{\sigma_X^2 \sigma_Y^2}{\sigma_X^2 + \sigma_Y^2} - 2 \frac{d}{d(\sigma_Y^2)} D(p_X+N\parallel p_{X+N}).$$

(12)

Here $D(p_X+N\parallel p_{X+N})$ is the Kullback-Leibler divergence between the PDF of $X+N$ and of $X+N$ where $X$ is a Gaussian random variable with the same mean and variance as $X$.

Theorem 1 has also the following interpretation. The rate distortion function $R(D)$ for an arbitrarily distributed source $X$ with variance $\sigma_X^2$ is upper-bounded by the mutual information of an AWGN channel with the input $X-E[X]$ and a noise variance $\sigma_N^2$, which is chosen such that the distortion is equal to $D = \text{mmse}(1/\sigma_N^2)$. As $\gamma$, i.e., the upper bound on $R(D)$, corresponds to the mutual information of an AWGN channel, mmse$(1/\sigma_N^2)$ and hence $D$ is given by two times the derivative of (9) with respect to $1/\sigma_N^2$ yielding (12), see [4] for the relation between mutual information and MMSE.

The representations in (9) and (12) using the Kullback-Leibler divergence allow an easy numerical evaluation of the upper bound on the rate distortion function. To calculate $D(p_X+N\parallel p_{X+N})$ the PDF $p_{X+N}$ is required. As $X$ and the additive noise $N$ are independent, $p_{X+N}$ is given by the convolution of $p_X$ and $p_N = \mathcal{N}(0, \sigma_N^2)$. In case $p_{X+N}$ cannot be obtained in closed-form, a numerical convolution is required to calculate the upper bound on $R(D)$. Thus, evaluation of (9) gives an upper bound on the rate $R$ for a given $\sigma_N^2$. The corresponding distortion $D$ can be calculated from (12). Hence, to evaluate the upper bound on the rate distortion function pairs of the upper bound on $R$ given by (9) and $D$ given by (12) have to be calculated by varying the parameter $\sigma_N^2$.

III. PROOF OF THEOREM 1

As the rate distortion function is independent of the mean $\mathbb{E}[X]$ of the source, i.e., the rate distortion functions $R(D)$ for the sources $X$ and $X - \mathbb{E}[X]$ are equal, in the following proof we assume that $\mathbb{E}[X] = 0$ without loss of generality.

With (5) the rate distortion function is given by

$$R(D) = \min_{p(\hat{x}|x)\in S} \mathcal{I}(X; \hat{X})$$

(13)

where the minimization is over all $p(\hat{x}|x)$ such that

$$\mathbb{E}[(X - \hat{X})^2] \leq D$$

(14)

i.e., all $p(\hat{x}|x)$ in the set $S$ in (6) with $d(x, \hat{x}) = (x - \hat{x})^2$.

As $R(D)$ is monotonically decreasing in $D$, all $p(\hat{x}|x)$ being solutions of (13) fulfill (14) with equality. Obviously, any choice $p(\hat{x}|x) \in S$ different from the optimal $p(\hat{x}|x)$ which minimizes $\mathcal{I}(X; \hat{X})$ yields an upper bound on $R(D)$:

$$R(D) \leq \mathcal{I}(X; \hat{X}).$$

(15)

Thus, we construct an upper bound on the rate distortion function $R(D)$ by choosing some $p(\hat{x}|x)$ satisfying

$$\mathbb{E}[(X - \hat{X})^2] = D$$

(16)

for which $\mathcal{I}(X; \hat{X})$ can be easily evaluated and at the same time is a sufficiently tight upper bound. Therefor, we define

$$Y = X + N$$

(17)

where $N$ is zero-mean additive white Gaussian noise with variance $\sigma_N^2$. Furthermore, let

$$\hat{X} = \mathbb{E}[X|Y]$$

(18)

be the MMSE estimate of $X$ from $Y$. Now, the variance $\sigma_N^2$ has to be chosen such that (16) is fulfilled. As the MMSE estimate $\hat{X}$ is a sufficient statistic of $Y$, see [6], it does not change the mutual information [3, Sect. 2.9] and it holds that

$$\mathcal{I}(X; \hat{X}) = \mathcal{I}(X; Y).$$

(19)

Thus, an upper bound on $R(D)$ is given by the mutual information of an AWGN channel with the source $X$ at its input and the variance of the additive Gaussian noise $\sigma_N^2$ depending on the distortion $D$ and implicitly given by (10) and (11).

Hence, to prove Theorem 1 it remains to show that (9) is equal to $\mathcal{I}(X; Y)$, i.e., the mutual information of the AWGN channel in (17) with the source $X$ at its input and noise variance $\sigma_N^2$. Therefor, we rewrite $\mathcal{I}(X; Y)$ as follows, see [7]²:

$$\mathcal{I}(Y; X) = h(Y) - h(Y|X) = h(Y) - h(N)$$

$$= - \int p_Y(y) \log \left( \frac{p_Y(y)}{p_{Y|X}(y)} \right) dy - h(N)$$

$$= - \int p_Y(y) \log \left( \frac{p_{Y|X}(y)}{p_Y(y)} \right) dy - \int p_Y(y) \log \left( \frac{p_{Y|X}(y)}{p_Y(y)} \right) dy$$

$$= - \int p_{Y|X}(y) \log \left( \frac{p_Y(y)}{p_{Y|X}(y)} \right) dy - \int p_Y(y) \log \left( \frac{p_{Y|X}(y)}{p_Y(y)} \right) dy$$

$$= - h(N)$$

(20)

$$= h(Y) - D(p_Y \parallel p_{Y|X}) - h(N)$$

(21)

²Note that [7] states that inequality (8) in Theorem 1 holds with equality. However, this statement is wrong in general. The erroneous assumption in [7] is that the information rate of a system with optimal source and channel coding is equal to the information rate of an AWGN channel where the source symbols are transmitted without coding. It can be shown that this statement does not hold in general and, therefore, (8) does not hold with equality in general.
where \( h(\cdot) \) denotes the differential entropy, \( p_Y(y) \) is the PDF of \( Y \), and \( p_Y^*(y) \) is the PDF of a corresponding zero-mean Gaussian variable with the same variance

\[
\sigma_Y^2 = \sigma_X^2 + \sigma_N^2. \tag{22}
\]

Moreover, \( D(p_Y \| p_Y^*) \) is the Kullback-Leibler divergence between \( p_Y(y) \) and \( p_Y^*(y) \). Furthermore, (20) holds because

\[
-\int p_Y(y) \log(p_Y(y)) \, dy = -\int p_Y(y) \log \left( \frac{\exp \left( \frac{-y^2}{2\sigma_Y^2} \right)}{\sqrt{2\pi\sigma_Y^2}} \right) \, dy = \frac{1}{2} \log (2\pi e \sigma_Y^2) = -\int p_Y^*(y) \log(p_Y^*(y)) \, dy. \tag{23}
\]

As \( Y \) and \( N \) are Gaussian, (21) is given by

\[
\mathcal{I}(Y; X) = \frac{1}{2} \log (2\pi e \sigma_X^2) - \frac{1}{2} \log (2\pi e \sigma_N^2) - D(p_Y \| p_Y^*) = \frac{1}{2} \log \left( 1 + \frac{\sigma_N^2}{\sigma_X^2} \right) - D(p_{X+N} \| p_{X+N}^*) \tag{24}
\]

where for (24) we have used (22). This shows that (9) is the mutual information of an AWGN channel with noise variance \( \sigma_N^2 \) and an arbitrarily distributed source \( X \) with zero-mean and variance \( \sigma_X^2 \) at its input.

The alternative representation of the upper bound on \( R(D) \) in (8) holds, as \( D(p_Y \| p_Y^*) \) in (24) is given by

\[
D(p_Y \| p_Y^*) = h(Y^*) - h(Y) \tag{25}
\]

where \( Y^* \) is a zero-mean Gaussian random variable with variance \( \sigma_Y^2 \). If \( Y^* \) is the input to the AWGN channel in (17), this results in the zero-mean Gaussian output \( Y^* \), yielding (26).

Moreover, (25) and (27) follow from the results given in [8].

## IV. Properties of the Upper Bound

### A. Gaussian Sources

For a Gaussian source \( X \), \( \text{mmse}(\gamma) \) in the upper bound (8) becomes \( \sigma_X^2 / (1 + \sigma_X^2 \gamma) \) and, thus, the integral in (8) is zero. Hence, the upper bound of the AWGN channel. However, for a Gaussian source the capacity of the AWGN channel and the rate distortion function \( R(D) \) in (7) are equal, as (11) becomes equal to

\[
D = \frac{\sigma_X^2 \sigma_N^2}{\sigma_X^2 + \sigma_N^2}. \tag{28}
\]

which follows from (12) as the Kullback-Leibler divergence in (12) is zero for Gaussian inputs. Thus, for a Gaussian source the upper bound on \( R(D) \) in (8) and (9) is tight.

This discussion also shows another well known fact. In case we estimate the Gaussian source \( X \) after transmission over an AWGN channel based on \( Y \) using an MMSE estimator, the MMSE is given by \( D \) in (28), see (10) to (12). To achieve this distortion no code at all is required. On the other hand, we can source encode the source \( X \) using a rate-distortion code, then use a channel code to transmit it reliably over the AWGN channel. Following Shannon’s source channel coding separation theorem [1], this separation of source and channel coding is optimal. At the receiver the signal can be channel and source decoded. To achieve a maximum distortion \( D \), the source encoder has to encode the source with rate \( R(D) \) given in (7). For reliable transmission over the AWGN channel its capacity has to correspond to \( R(D) \), i.e., for \( 0 \leq D \leq \sigma_X^2 \)

\[
\frac{1}{2} \log \left( 1 + \frac{P}{\sigma_N^2} \right) \leq R(D) \leq \frac{1}{2} \log \left( 1 + \frac{\sigma_X^2}{\sigma_N^2} \right) \tag{29}
\]

where \( P \) is the required transmit power. Obviously \( P = \sigma_X^2 \).

However, this means that for a given transmit power, there is no advantage of the use of source and channel coding when a Gaussian source has to be transmitted over an AWGN channel. Directly transmitting uncoded source symbols over the AWGN channel yields the same distortion \( D \) as perfect source and channel coding. In addition, the latter one implies an infinite delay. This is a well known result, see e.g. [9], [10].

### B. Gap to Shannon’s Lower Bound

Shannon gave a lower bound on \( R(D) \), which for the mean-square error distortion measure becomes [2]

\[
R(D) \geq h(X) - \frac{1}{2} \log (2\pi e D) = \text{LB}_{\text{Sha}}. \tag{30}
\]

The gap \( \Delta \) between the new upper bound on \( R(D) \) given in Theorem 1 and Shannon’s lower bound in (30) is given by

\[
\Delta = \text{UB}_{\text{new}} - \text{LB}_{\text{Sha}} = -h(Y) + \frac{1}{2} \log \left( 2\pi e \text{mmse} \left( \frac{1}{\sigma_N^2} \right) \right). \tag{31}
\]

where we have used (9), (30), (11), and (24). The variance of the MMSE estimate \( E[X|Y] \) is equal to \( \text{mmse}(1/\sigma_X^2) \). Furthermore, for a given variance Gaussian random variables are entropy maximizers and the second term on the RHS of (31) corresponds to the differential entropy of a Gaussian random variable with variance \( \text{mmse}(1/\sigma_X^2) \). In general, the estimation error of the MMSE estimate \( E[X|Y] \) is non-Gaussian. Thus, \( h(X|Y) \) in (31) is upper-bounded by the second term on the RHS of (31). \( \Delta \) corresponds to the negative difference of the entropy of \( X \) conditioned on \( Y \) and the corresponding entropy in case \( X \) is Gaussian with the same variance. Hence, \( \Delta \) becomes zero for \( X \) being Gaussian.

### C. Comparison of the New Upper Bound on \( R(D) \) with Shannon’s Upper Bound on the Rate Distortion Function

Shannon has shown that for an arbitrary distributed source \( X \) with variance \( \sigma_X^2 \), the rate distortion function is upper-bounded by the rate distortion function of a Gaussian source with the same variance, which is given in (7). I.e., Gaussian sources are hardest to encode, cf. [11].

The difference between this upper bound in (7) given by Shannon and the new upper bound on \( R(D) \) stated in
Theorem 1 is for $D \leq \sigma_X^2$ given by

$$\text{UB}_{\text{Sh}} - \text{UB}_{\text{new}} = \frac{1}{2} \log \left( \frac{\sigma_X^2}{\text{mmse}(\frac{\gamma}{\sigma_X^2})} \right) - \frac{1}{2} \int_0^{\infty} \text{mmse}(\gamma) d\gamma$$

(32)

where we have used (7), (11), and (8). The difference on the RHS of (32) depends on \( \text{mmse}(\gamma) \), which is bounded by $0 \leq \text{mmse}(\gamma) \leq \frac{\sigma_X^2}{1 + \frac{1}{\gamma}}$, where the RHS is the MMSE in case $X$ is Gaussian. The upper bound on \( \text{mmse}(\gamma) \) holds as Gaussian random variables are hardest to estimate [12, Prop. 15].

\( \text{UB}_{\text{new}} \) is in general tighter than \( \text{UB}_{\text{Sh}} \), as, by using \( \text{mmse}(\gamma) \leq \frac{\sigma_X^2}{1 + \frac{1}{\gamma}} \), and the relation between the MMSE and the mutual information given in [4], (32) is lower-bounded by

$$\text{UB}_{\text{new}} \geq \frac{1}{2} \log \left( 1 + \frac{\sigma_X^2}{\sigma_N^2} \right) - I(X + N; X) \geq 0$$

(33)

where the RHS of (33) follows from the fact that $I(X + N; X)$ is maximized if $X$ is Gaussian. For \( \text{mmse}(\gamma) = \frac{\sigma_X^2}{1 + \frac{1}{\gamma}} \), (32) is equal to zero.

Finally, for an arbitrary distribution of the source $X$ and $D \to \sigma_X^2$, which by (11) corresponds to $\sigma_X^2 \to \infty$, the MMSE converges to the MMSE in case the source is Gaussian:

$$\lim_{1/\sigma_X^2 \to 0} \left\{ \text{mmse}(\gamma) - \frac{\sigma_X^2}{1 + \frac{1}{\gamma}} \right\} = 0.$$

(34)

Thus, \( \text{UB}_{\text{Sh}} - \text{UB}_{\text{new}} \) converges to zero for $D \to \sigma_X^2$.

### D. Evaluation of the Upper Bound in Theorem 1

In Fig. 1 we have evaluated the new upper bound on the rate distortion function given by Theorem 1 for a uniform source distribution (Fig. 1(a)), a source with Laplace distribution and a bipolar input distribution (both Fig. 1(b)) all with zero-mean and variance $\sigma_X^2 = 1$, i.e.,

$$P_{X, \text{uniform}}(x) = \begin{cases} \frac{1}{\sqrt{2}} & \text{for } |x| \leq \sqrt{3}, \\ 0 & \text{otherwise}, \end{cases}$$

(35)

$$P_{X, \text{Laplace}}(x) = \frac{1}{\sqrt{2}} \exp \left( -\sqrt{2}|x| \right),$$

(36)

$$P_{X, \text{bipolar}}(x) = \begin{cases} \frac{1}{2} & \text{for } x = \pm 1, \\ 0 & \text{otherwise}. \end{cases}$$

(37)

For comparison the Shannon upper bound in (7) corresponding to the rate distortion function for a Gaussian source, the Shannon lower bound in (30), and the actual rate distortion function calculated numerically based on the Blahut-Arimoto algorithm [13], [14] are shown. The Shannon lower bound (30) is not shown for the bipolar source as $h(X)$ does not exist in this case.

Fig. 1 shows that the new upper bound and the Shannon lower bound on the rate distortion function become tight for $D \to 0$. On the other hand, for $D \to \sigma_X^2$ the new upper bound converges to the Shannon upper bound. The comparison of the new upper bound with the numerical evaluation of $R(D)$ based on the Blahut-Arimoto shows that the new upper bound is quite tight for the displayed source distributions.

The MATLAB source code is available on our websites.
On the Information Loss in Memoryless Systems: The Multivariate Case

Bernhard C. Geiger*, Gernot Kubin*
*Signal Processing and Speech Communication Laboratory, Graz University of Technology, Austria
{geiger.gernot.kubin}@tugraz.at

Abstract—In this work we give a concise definition of information loss from a system-theoretic point of view. Based on this definition, we analyze the information loss in memoryless input-output systems subject to a continuous-valued input. For a certain class of multiple-input, multiple-output systems the information loss is quantified. An interpretation of this loss is accompanied by upper bounds which are simple to evaluate.

Finally, a class of systems is identified for which the information loss is necessarily infinite. Quantizers and limiters are shown to belong to this class.

I. INTRODUCTION

In the XXXI. Shannon lecture Han argued that information theory links information-theoretic quantities, such as entropy and mutual information, to operational quantities such as source, channel, capacity, and error probability [1]. In this work we try to make a new link to an operational quantity not mentioned by Han: information loss. Information can be lost, on the one hand, in erasures or due to superposition of noise as it is known from communication theory. Dating back to Shannon [2] this loss is linked to the conditional entropy of the input given the output, at least in discrete-amplitude, memoryless settings. On the other hand, as stated by the data processing inequality (DPI, [3]), information can be lost in deterministic, noiseless systems. It is this kind of loss that we will treat in this work, and we will show that it makes sense to link it to the same information-theoretic quantity.

The information loss in input-output systems is very sparsely covered in the literature. Aside from the DPI for discrete random variables (RV) and static systems, some results are available for jointly stationary stochastic processes [4]. Yet, all these results just state that information is lost, without quantifying this loss. Only in [5] the information lost by collapsing states of a discrete-valued stochastic process is quantified as the difference between the entropy rates at the input and the output of the memoryless system.

Conversely, energy loss in input-output systems has been deeply analyzed, leading to meaningful definitions of transfer functions and notions of passivity, stability, and losslessness. Essentially, it is our aim to develop a system theory not from an energetic, but from an information-theoretic point of view. So far we analyzed the information loss of discrete-valued stationary stochastic processes in finite-dimensional dynamical input-output systems [6], where we proposed an upper bound on the information loss and identified a class of information-preserving systems (the information-theoretic counterpart to lossless systems). In [7] the information loss of continuous RVs in memoryless systems was quantified and bounded in a preliminary way. In this work, extending [7], we analyze the information loss for static multiple-input, multiple-output systems which are subject to a continuous input RV.

Unlike in our previous work, we permit functions which lose an infinite amount of information and present the according conditions. Aside from that we provide a link between information loss and differential entropy, a quantity which is not invariant under changes of variables. The next steps towards an information-centered system theory are the analysis of discrete-time dynamical systems with continuous-valued stationary input processes and a treatment of information loss in multirate systems.

In the remainder of this paper we give a mathematically concise definition of information loss (Section II). After restricting the class of systems in Section III, in Section IV we provide exact results for information loss together with simple bounds, and establish a link to differential entropies. Finally, in Section V we show under which conditions the information loss becomes infinite. An extended version of this paper, accompanied by several examples illustrating the theoretical results, is available in [8].

II. A DEFINITION OF INFORMATION LOSS

When talking about the information loss induced by processing of signals, it is of prime importance to accompany this discussion by a well-based definition of information loss going beyond, but without lacking, intuition. We try to meet this objective with the following

Definition 1. Let $X$ be an RV\(^1\) on the sample space $\mathcal{X}$, and let $Y$ be obtained by transforming $X$. We define the information loss induced by this transform as

$$L(X \rightarrow Y) = \sup_{\mathcal{P}} \left( I(\hat{X};X) - I(\hat{X};Y) \right)$$

where the supremum is over all partitions $\mathcal{P}$ of $\mathcal{X}$, and where $\hat{X}$ is obtained by quantizing $X$ according to the partition $\mathcal{P}$ (see Fig. 1).

This Definition is motivated by the data processing inequality (cf. [3]), which states that the expression under the supremum is always non-negative: Information loss is the worst-case reduction of information about $X$ induced by

\(^1\)Note that $X$ and all other involved RVs need not be scalar-valued.
transforming $X$. We now try to shed a little more light on Definition 1 in the following

Theorem 1. The information loss of Definition 1 is given by the conditional entropy of the input given the output, i.e.,

$$L(X \rightarrow Y) = H(X|Y).$$

(2)

Proof: We start by noticing that

$$I(X;Y) - I(\hat{X};Y) = H(\hat{X}|Y) \leq H(X|Y)$$

(3)

by the definition of mutual information and since both $\hat{X}$ and $Y$ are functions of $X$. The inequality in (3) is due to data processing ($\hat{X}$ is a function of $X$). We now show that in the supremum over all partitions equality can be achieved.

To this end, observe that among all partitions of the sample space of $X$ there is a sequence $\{\mathcal{P}_n\}$ of increasingly fine partitions\(^2\) such that

$$\lim_{n \to \infty} \hat{X}_n = X$$

(4)

where $\hat{X}_n$ is the quantization of $X$ induced by partition $\mathcal{P}_n$. By the axioms of entropy (e.g., [9, Ch. 14]), $H(\hat{X}_n|Y)$ is an increasing sequence in $n$ with limit $H(X|Y)$. Thus, equality in (3) is achieved, which completes the proof.

This Theorem shows that the supremum in Definition 1 is achieved for $\hat{X} \equiv X$, i.e., when we compute the difference between the self-information of the input and the information output of the system contains about its input. In addition to that, the Theorem suggests a natural way to measure the information loss via measuring mutual informations, as it is depicted in Fig. 1. As we will see later (cf. Theorem 3), the considered partition does not have to be infinitely fine.

III. PROBLEM STATEMENT

Let $X = [X_1, X_2, \ldots, X_N]$ be an $N$-dimensional RV with a probability measure $P_X$ absolutely continuous w.r.t. the Lebesgue measure $\mu$ ($P_X \ll \mu$). We require $P_X$ to be concentrated on $X \subseteq \mathbb{R}^N$. This RV, which possesses a unique probability density function (PDF) $f_X$, is the input to the following multivariate, vector-valued function:

Definition 2. Let $g: \mathcal{X} \rightarrow \mathcal{Y}$, $\mathcal{X}, \mathcal{Y} \subseteq \mathbb{R}^N$, be a surjective, Borel-measurable function defined in a piecewise manner:

$$g(x) = \begin{cases} g_1(x), & \text{if } x \in \mathcal{X}_1 \\ g_2(x), & \text{if } x \in \mathcal{X}_2 \\ \vdots & \end{cases}$$

where $x = [x_1, x_2, \ldots, x_N]$ and $g_i: \mathcal{X}_i \rightarrow \mathcal{Y}_i$ bijectively. Furthermore, let the Jacobian matrix $J_{g_i}(\cdot)$ exist on the closures of $\mathcal{X}_i$. In addition to that, we require the Jacobian determinant, $|\det J_{g_i}(\cdot)|$, to be non-zero $P_X$-almost everywhere.

In accordance with previous work [7] the $\mathcal{X}_i$ are disjoint sets of positive $P_X$-measure which unite to $\mathcal{X}$, i.e., $\bigcup_i \mathcal{X}_i = \mathcal{X}$ and $\mathcal{X}_i \cap \mathcal{X}_j = \emptyset$ if $i \neq j$. Clearly, also the $\mathcal{Y}_i$ unite to $\mathcal{Y}$, but need not be disjoint. This definition ensures that the preimage $g^{-1}[y]$ of each element $y \in \mathcal{Y}$ is a countable set.

Using the method of transformation [9, pp. 244] one obtains the PDF of the $N$-dimensional output RV $Y = [Y_1, Y_2, \ldots, Y_N]$ as

$$f_Y(y) = \sum_{x \in g^{-1}[y]} \frac{f_X(x)}{|\det J_{g}(x)|}$$

(6)

where the sum is over all elements of the preimage. Note that since $Y$ possesses a density, the corresponding probability measure $P_Y$ is also absolutely continuous w.r.t. the Lebesgue measure.

IV. MAIN RESULTS

We now state our main results:

Theorem 2. The information loss induced by a function $g$ satisfying Definition 2 is given as

$$H(X|Y) = \int_X f_X(x) \log \left( \frac{\sum_{y \in g^{-1}[g(x)]: g(x) = y} f_X(x)}{|\det J_{g}(x)|} \right) dx.$$  

(7)

The proof of this Theorem can be found in the Appendix of [8] and, in a modified version for univariate functions, in [7]. Note that for univariate functions the Jacobian determinant is replaced by the derivative of the function.

Corollary 1. The information loss induced by a function $g$ satisfying Definition 2 is given as

$$H(X|Y) = h(X) - h(Y) + E \{ \log |\det J_{g}(X)| \}$$

(8)

Proof: The proof is obtained by recognizing the PDF of $Y$ inside the logarithm in (7) and by splitting the logarithm.

This result is particularly interesting because it provides a link between information loss and differential entropies already anticipated in [9, pp. 660]. There, it was claimed that

$$h(Y) \leq h(X) + E \{ \log |\det J_{g}(X)| \}$$

(9)

where equality holds iff $g$ is bijective. While (9) is actually another version of the DPI, Corollary 1 quantifies how much information is lost by processing. In addition to that, a very similar expression denoted as folding entropy has been presented in [10], although in a completely different setting analyzing the entropy production of autonomous dynamical systems.

We now introduce a discrete RV $W$ which depends on the set $\mathcal{X}_i$ from which $X$ was taken. In other words, we have $W =$

\[\text{choose the set } \mathcal{X}_i \text{ for each } x \in \mathcal{X} \text{ such that } g(x) = y_i \text{ for some } y_i \in \mathcal{Y}_i.\]
i iff \( x \in X_i \). One can interpret this RV as being generated by a vector quantization of \( X \) with a partition \( \mathcal{P} = \{X_i\} \). With this new RV we can state

**Theorem 3.** The information loss is identical to the uncertainty about the set \( X_i \) from which the input was taken, i.e.,

\[
H(X|Y) = H(W|Y).
\]

The proof closely follows the proof provided in [7] and thus is omitted. However, this equivalence suggests a way of measuring information loss by means of proper quantization: Since \( H(W|Y) = I(W;X) - I(W;Y) \) the loss can be determined by measuring mutual informations, which in this case are always finite (or, at least, bounded by \( H(W) \)).

The interpretation derived from Theorem 3 allows us now to provide upper bounds on the information loss:

**Theorem 4.** The information loss is upper bounded by

\[
H(X|Y) \leq \int_y P_Y(y) \log \text{card}(g^{-1}[y]) dy
\]

(11)

\[
\leq \log \left( \sum_i \int_{y_i} f_X(y) dy \right)
\]

(12)

\[
\leq \max_y \log \text{card}(g^{-1}[y])
\]

(13)

where \( \text{card}(B) \) is the cardinality of the set \( B \).

**Proof:** We give here only a sketch of the proof: The first inequality results from bounding \( H(W|Y = y) \) by the entropy of a uniform distribution on the preimage of \( y \). Jensen’s inequality yields the second line of the Theorem. The coarsest bound is obtained by replacing the cardinality of the preimage by its maximal value.

In this Theorem, we bounded the information loss given a certain output by the cardinality of the preimage. While the first bound considers the fact that the cardinality may actually depend on the output itself, the last bound incorporates the maximum cardinality only. In cases where the function from Definition 2 is defined not on a countable but on a finite number of subdomains, this finite number can act as an upper bound (cf. [7]). Another straightforward upper bound, which is independent from the bounds in Theorem 4 is obtained from Theorem 3 by removing conditioning:

\[
H(X|Y) \leq H(W) = -\sum_i p_i \log p_i
\]

(14)

where \( p_i = P_X(X_i) = \int_{X_i} f_X(x) dx \).

A further implication of introducing this discrete RV \( W \) is that it allows us to perform investigations about reconstructing the input from the output. Currently, a Fano-type inequality bounding the reconstruction error by the information loss is under development. In addition to that, new upper bounds on the information loss related to the reconstruction error of optimal (in the maximum a posteriori sense) and of simpler, sub-optimal estimators are analyzed.

**V. FUNCTIONS WITH INFINITE INFORMATION LOSS**

We now drop the requirement in Definition 2 that the \( g \) possesses partial inverses to analyze a wider class of Borel-measurable functions \( g: X \to Y \). We keep the requirement that \( P_X \ll \mu \) and thus \( X \) possesses a density \( f_X \) (positive on \( X \) and zero elsewhere). We maintain

**Theorem 5.** Let \( g: X \to Y \) be a Borel-measurable function and let the continuous RV \( X \) be the input to this function. If there exists a set \( B \subseteq Y \) of positive \( P_Y \)-measure such that the preimage \( g^{-1}[y] \) is uncountable for every \( y \in B \), then the information loss is infinite.

**Proof:** With \( B \subseteq Y \) we notice that

\[
H(X|Y) \geq \int_B H(X|Y = y) dP_Y(y)
\]

(15)

where the integral is now written as Lebesgue integral, since \( P_Y \) now not necessarily possesses a density.

Since on \( B \) the preimage of every element is uncountable, we obtain with [4] and the references therein \( H(X|Y = y) = \infty \) for all \( y \in B \), and, thus, \( H(X|Y) = \infty \).

Note that the requirement of \( B \) being a set of positive \( P_Y \)-measure cannot be dropped, as one of the examples provided in [8] illustrates. We immediately obtain the following

**Corollary 2.** Let \( g: X \to Y \) be a Borel-measurable function and let the continuous RV \( X \) be the input to this function. If the probability measure of the output, \( P_X \), possesses a non-vanishing discrete component, the information loss is infinite.

**Proof:** According to the Lebesgue-Radon-Nikodym theorem [11, pp. 121] every measure can be decomposed in a component absolutely continuous w.r.t. \( \mu \) and a component singular to \( \mu \). The latter part can further be decomposed into a singular continuous and a discrete part, where the latter places positive \( P_Y \)-mass on points. Let \( y^* \) be such a point, i.e., \( P_Y(y^*) > 0 \). As an immediate consequence, \( P_X(g^{-1}[y^*]) > 0 \), which is only possible if \( g^{-1}[y^*] \) is uncountable (\( P_X \ll \mu \)).

This result is also in accordance with intuition, as the analysis of a simple quantizer shows: While the entropy of the input RV is infinite \((I(X;X) \to \infty \text{ for } X \to X)\); cf. [9, pp. 654]), the quantized output can contain only a finite amount of information \((I(X;Y) \to H(Y) < \infty)\). In addition to that, the preimage of each possible output value \( y \) is a set of positive \( P_Y \)-measure. The loss, as a consequence, is infinite.

While for the quantizer the preimage of each possible output value is a set of positive measure, there certainly are functions for which some outputs have a countable preimage and some whose preimage is a non-null set. An example of such a system is the limiter [9, Ex. 5-4]. For such systems it can be shown that both the information loss \( I(X \to Y) = H(X|Y) \) and the information transfer \( I(X;Y) \) are infinite.

Finally, there exist functions \( g \) for which the preimages of all output values \( y \) are null sets, but which still fulfill the conditions of Theorem 5. Functions which project \( X \) on a lower-dimensional subspace of \( \mathbb{R}^N \) fall into that category.
VI. EXAMPLE: A TWO-DIMENSIONAL TRANSFORM WITH FINITE INFORMATION LOSS

In this Section we illustrate our theoretical results with the help of an example. The logarithm is taken to base 2. Let \( X \) be uniformly distributed on the square \( \mathcal{X} = [-a, a] \times [-a, a] \), or equivalently, the two constituting RVs \( X_1 \) and \( X_2 \) are independent and uniformly distributed on \([-a, a]\). In other words, if \( f_X(x) = 1/4a^2 \) for all \( x \in \mathcal{X} \), we have \( f_X(x_i) = 1/2a \) for \( x_i \in [-a,a] \) and \( i = 1,2 \).

We consider a function \( g \) performing the mapping:
\[
Y_1 = X_1 \quad (16)
\]
\[
Y_2 = |X_1 - X_2| \quad (17)
\]

The corresponding Jacobian matrix is a triangular matrix
\[
J_g(x) = \begin{bmatrix}
1 & 0 \\
\text{sgn}(x_1 - x_2) & \text{sgn}(x_2 - x_1)
\end{bmatrix}
\] (18)
where \( \text{sgn}(\cdot) \) is the sign-function. From this immediately follows that the magnitude of the determinant of the Jacobian matrix is unity for all possible values of \( X \), i.e., \( |\det J_g(x)| = 1 \) for all \( x \in \mathcal{X} \). The subsets of \( \mathcal{X} \) on which the partitioned functions \( g_i \) are bijective are no intervals in this case; they are the triangular halves of the square induced by \( x_1 = x_2 \) (see Fig. 2)
\[
\mathcal{X}_1 = \{x_1, x_2 \in \mathcal{X} : x_1 > x_2\} \quad (19)
\]
\[
\mathcal{X}_2 = \{x_1, x_2 \in \mathcal{X} : x_1 \leq x_2\} \quad (20)
\]

The preimage of \( g(x) \) is, in any case,
\[
\{[x_1, x_2], [x_1, 2x_1 - x_2] \} \cap \mathcal{X} \quad (21)
\]
The transform \( g \) is bijective whenever \( [x_1, 2x_1 - x_2] \notin \mathcal{X} \), i.e., if \( 2|x_1 - x_2| > a \).

With the PDF of \( X \) and of its components we obtain for the information loss
\[
H(X|Y) = \int_{-a}^{a} \int_{-a}^{a} \frac{1}{4a^2} \log\left(\frac{1}{2a} + \frac{f_X(2x_1 - x_2)}{2a}\right) dx_1 dx_2 \quad (22)
\]
which is non-zero only if \(-a \leq 2x_1 - x_2 \leq a\) (numerator and denominator cancel otherwise; no loss occurs in the bijective domain of the function). As a consequence,
\[
H(X|Y) = \int_{-a}^{a} \int_{-a}^{a} \frac{\log 2}{4a^2} dx_1 dx_2 = \int_{-a}^{a} \frac{1}{4a} dx_2 = \frac{1}{2} \quad (23)
\]
The information loss is identical to a half bit. This is intuitive by looking at Fig. 2, where it can be seen that any information loss occurs only on one half of the domain \( \mathcal{X} \) (shaded in stronger colors). By destroying the sign information, in this area the information loss is equal to one bit.

VII. CONCLUSION

In this work, we proposed a mathematically concise definition of information loss for the purpose of establishing a system theory from an information-theoretic point of view. For a certain class of multivariate, vector-valued functions and continuous input variables this information loss was quantified, and the result is accompanied by convenient upper bounds. We further showed a connection between information loss and the differential entropies of the input and output variables.

Finally, a class of systems has been identified for which the information loss is infinite. Vector-quantizers and limiters belong to that class, but also functions which project the input space onto a space of lower dimensionality.

REFERENCES

One-Bit Quantizers for Fading Channels

Tobias Koch  
University of Cambridge  
Cambridge, CB2 1PZ, UK  
Email: tobi.koch@eng.cam.ac.uk

Amos Lapidoth  
ETH Zurich  
CH-8092 Zurich, Switzerland  
Email: lapidoth@ist.ee.ethz.ch

Abstract—We study channel capacity when a one-bit quantizer is employed at the output of the discrete-time average-power-limited Rayleigh-fading channel. We focus on the low signal-to-noise ratio regime, where communication at very low spectral efficiencies takes place, as in Spread Spectrum and Ultra-Wideband communications. We demonstrate that, in this regime, the best one-bit quantizer does not reduce the asymptotic capacity of the coherent channel, but it does reduce that of the noncoherent channel.

I. INTRODUCTION

We study the effect on channel capacity of quantizing the output of the discrete-time average-power-limited Rayleigh-fading channel using a one-bit quantizer. This problem arises in communication systems where the receiver uses digital signal processing techniques, which require the analog received signal to be quantized using an analog-to-digital converter (ADC). The effects of quantization are particularly pronounced when high-resolution ADCs are not practical and low-resolution ADCs must be used [1].

We focus on the low signal-to-noise ratio (SNR) regime, where communication at very low spectral efficiencies takes place (as in Spread-Spectrum and Ultra-Wideband communications). For the average-power-limited real-valued Gaussian channel, it is well-known that, in this regime, a symmetric one-bit quantizer (which produces 1 if the channel output is nonnegative and 0 otherwise) reduces the capacity by a factor of $2/\pi$, corresponding to a 2dB power loss [2]. It was recently shown that, by allowing for asymmetric one-bit quantizers with corresponding asymmetric signal constellations, these two decibels can be recovered in full [3]. A similar result was shown for the average-power-limited complex-valued Gaussian channel [4]: using binary on-off keying and a radial quantizer (which produces 1 if the magnitude of the channel output is above some threshold and 0 otherwise), one can achieve the low-SNR asymptotic capacity of the unquantized channel by judiciously choosing the threshold and the on-level as functions of the SNR. Here we extend [3], [4] to Rayleigh-fading channels. Specifically, we study the capacity per unit-energy [5] of such channels when the channel output is quantized using a one-bit quantizer.

For coherent fading channels, where the receiver has perfect channel knowledge, we show that quantizing the channel output with a one-bit quantizer causes no loss in the capacity per unit-energy. As in [4], the capacity per unit-energy can be achieved using binary on-off keying and a radial quantizer by choosing the threshold as a function of the SNR and the fading, with the threshold and the on-level both tending to infinity as the SNR tends to zero. This result might mislead one to think that quantizing the channel output with a one-bit quantizer causes no loss in the capacity per unit-energy also for noncoherent fading channels, where the receiver does not have perfect channel knowledge. Indeed, in the absence of a quantizer the capacity per unit-energy does not depend on whether the receiver has perfect channel knowledge or not [6], [7]. Since this capacity per unit-energy can be achieved using binary on-off keying with diverging on-level, it might therefore seem plausible that also in the presence of a quantizer the capacity per unit-energy would not depend on whether the receiver has perfect channel knowledge or not. But this is not the case: in contrast to the coherent case, quantizing the output of the noncoherent Rayleigh-fading channel with a one-bit quantizer reduces the capacity per unit-energy.

The rest of the paper is organized as follows. Section II describes the channel model and introduces the capacity per unit-energy. Section III presents the main results. Section IV discusses the capacity per unit-energy when the real and the imaginary part of the channel output are quantized separately with one-bit quantizers. And Section V presents the proofs of the main results.

II. CHANNEL MODEL AND CAPACITY PER UNIT-ENERGY

We consider a discrete-time Rayleigh-fading channel whose complex-valued output $\hat{Y}_k$ at time $k \in \mathbb{Z}$ corresponding to the channel input $x_k \in \mathbb{C}$ (where $\mathbb{C}$ and $\mathbb{Z}$ denote the set of complex numbers and the set of integers) is given by

$$\hat{Y}_k = H_k x_k + Z_k, \quad k \in \mathbb{Z}. \quad (1)$$

Here $\{Z_k, k \in \mathbb{Z}\}$ and $\{H_k, k \in \mathbb{Z}\}$ are independent sequences of independent and identically distributed (i.i.d.), zero-mean, circularly-symmetric, complex Gaussian random variables, the former with unit variance and the latter with variance $\sigma^2$. We say that the channel is coherent if the receiver is cognizant of the realization of $\{H_k, k \in \mathbb{Z}\}$ and that it is noncoherent if the receiver is cognizant only of the statistics of $\{H_k, k \in \mathbb{Z}\}$.

The receiver does not have access to the channel outputs $\{\hat{Y}_k, k \in \mathbb{Z}\}$ but only to a quantized version thereof. Specifically, the complex channel output $\hat{Y}_k$ is fed to a one-bit
quantizer which produces $Y_k = 1$ if $\hat{Y}_k$ is in the quantization region $D$ and $Y_k = 0$ otherwise, for some Borel set $D \subset \mathbb{C}$. In the coherent case, $D$ may depend on the fading $\{ H_k, k \in \mathbb{Z} \}$.

We assume that the average power of the channel inputs is limited by $P$. The capacity of the above channel is [8], [9]

$$C(P) = \sup_{P > 0} I(X; Y|H), \text{ coherent case}$$

$$C(P) = \sup_{P > 0} I(X; Y), \text{ noncoherent case}$$

where the suprema on the right-hand side (RHS) of (2) and (3) are over all distributions on $X$ satisfying $E[|X|^2] \leq P$ and over all quantization regions $D$. (Since the above channel is memoryless, we omit the time indices.)

The capacity per unit-energy is given by [5, Th. 2]

$$\hat{C}(0) = \frac{C(P)}{P}$$

It can be shown that

$$\hat{C}(0) = \lim_{P \to 0} \frac{C(P)}{P}$$

Thus, the capacity per unit-energy is equal to the slope at zero of the capacity-vs-power curve. It can be further shown that [5, Th. 3] (see also [6])

$$\hat{C}(0) = \sup_{\xi \neq 0, D} \frac{D(P|X \sim D|X = \xi) \| P_Y|X = \xi \| P_H)}{\| \xi \|^2}$$

in the coherent case and

$$\hat{C}(0) = \sup_{\xi \neq 0, D} \frac{D(P|X \sim D|X = \xi) \| P_Y|X = \xi \| P_H)}{\| \xi \|^2}$$

in the noncoherent case. Here $D(\| \cdot \|)$ denotes relative entropy

$$D(P\|Q) = \begin{cases} \int \log \left( \frac{dP}{dQ} \right) dP, & \text{if } P \ll Q \\ \infty, & \text{otherwise} \end{cases}$$

(where $P \ll Q$ indicates that $P$ is absolutely continuous with respect to $Q$); $D(\| \cdot \|)$ denotes conditional relative entropy

$$D(P_Y|X = \xi) \| P_Y|X = \xi \| P_Y|X = \xi \| P_H) = \int D(P_Y|H = h, X = \xi) \| P_Y|H = h, X = \xi \| P_H) \, dP_H(h);$$

$P_H$ denotes the distribution of the fading $H$; $P_Y|X = x$ denotes the output distribution given that the input is $x$; and $P_Y|H = h, X = \xi$ denotes the output distribution conditioned on $(H, X) = (h, x)$.

By the Data Processing Inequality [10, Th. 2.8.1], the capacity per unit-energy of the quantized channel is upper-bounded by that of the unquantized channel [7], [6]

$$\hat{C}(0) \leq \frac{1}{\sigma^2}.$$  
(8)

We show that in the coherent case this upper bound holds with equality, while in the noncoherent case it is strict.

### III. Main Result

We restrict ourselves to radial quantizers, for which

$$D = \{ \hat{y} \in \mathbb{C} : |\hat{y}| \geq T \}, \text{ for some } T > 0.$$  
(9)

In the noncoherent case—as we show in Section V-B—such quantizers are optimal in the sense that they maximize the relative entropy on the RHS of (7) for every $\xi \neq 0$. In the coherent case such quantizers need not be optimal in the above sense. However, they suffice to achieve the capacity per unit-energy. And such quantizers have the practical advantage of not requiring knowledge of the phase of $\hat{y}$.

**Theorem 1:** Consider the above channel model, and assume that the channel output is quantized using a one-bit quantizer.

1) In the coherent case,

$$\hat{C}(0) = \frac{1}{\sigma^2}$$

which can be achieved by some radial quantizer (9) with $T$ depending on $H$ and $\xi^2$.

2) In the noncoherent case,

$$\hat{C}(0) < \frac{1}{\sigma^2}$$

with the inequality being strict.

**Proof:** See Section V.

### IV. Quantizing the Real and Imaginary Part

Instead of quantizing $\hat{Y}$ using a one-bit quantizer, often the real and imaginary parts of $\hat{Y}$ are quantized separately using a one-bit quantizer for each; see, e.g., [11]-[14], [6]. Thus, the first quantizer produces $Y_{k,1} = 1$ if $\text{Re}(Y_k) \in D_R$ and $Y_{k,1} = 0$ otherwise, and the second quantizer produces $Y_{k,2} = 1$ if $\text{Im}(Y_k) \in D_I$ and $Y_{k,2} = 0$ otherwise, for some Borel sets $D_R, D_I \subset \mathbb{R}$. (Here $\mathbb{R}$ denotes the set of real numbers, $\text{Re}(\cdot)$ denotes the real part, and $\text{Im}(\cdot)$ denotes the imaginary part.) In the coherent case, $D_R$ and $D_I$ may depend on the fading $\{ H_k, k \in \mathbb{Z} \}$.

The capacity per unit-energy of this channel is given by (6) or (7), but with $Y$ replaced by $(Y_R, Y_I)$, and with $D \subset \mathbb{C}$ replaced by $(D_R, D_I) \subset \mathbb{R} \times \mathbb{R}$.

For symmetric quantizers, i.e., for

$$D_R = D_I = \{ u \in \mathbb{R} : u \geq 0 \}.$$  
(12)

it follows from [11] and [15, Th. 2] that, in the coherent case,

$$\hat{C}_{\text{sym}}(0) = \frac{2}{\pi \sigma^2}.$$  
(13)

In the noncoherent case, symmetric quantizers result in zero capacity and hence, by (4), in zero capacity per unit-energy. Indeed, for (12)

$$\text{Pr}(Y_R = 1 \mid X = x) = \text{Pr}(Y_I = 1 \mid X = x) = \frac{1}{2}, \quad x \in \mathbb{C}.$$  

Since, conditioned on $X$, the random variables $Y_R$ and $Y_I$ are independent, this implies that the capacity is zero. Thus, quantizing the real and imaginary parts of the Rayleigh-fading

\[\text{Here and throughout this paper, } \xi \text{ refers to the parameter in (6) or (7).}\]
channel using symmetric one-bit quantizers reduces the capacity per unit-energy by a factor of \(2/\pi\) in the coherent case, and it reduces it to zero in the noncoherent case. In the following, we show that if we allow for asymmetric quantizers, then we can fully recover the loss of \(2/\pi\) incurred on the coherent Rayleigh-fading channel. For the noncoherent channel, we show that asymmetric quantizers achieve a positive capacity per unit-energy, albeit strictly smaller than \(1/\sigma^2\).

**Theorem 2:** Consider the above channel model, and assume that the real and imaginary parts of \(Y\) are quantized separately using a one-bit quantizer for each.

1) In the coherent case,

\[
\hat{C}(0) = \frac{1}{\sigma^2}
\]

which can be achieved by some quantization regions

\[
D' = \{ u \in \mathbb{R} : u \geq T_k \}
\]

(15)

where \(T_k\) and \(T_l\) depend on \(\text{Re}(H\xi)\) and \(\text{Im}(H\xi)\), respectively.

2) In the noncoherent case,

\[
\frac{2Q(1)}{\sigma^2} \leq \hat{C}(0) < \frac{1}{\sigma^2}
\]


with the upper bound being strict. Here \(Q(\cdot)\) denotes the Gaussian Q-function [16, Eq. (1.3)]. The lower bound can be achieved by the quantization regions (15) and (16) with \(T_k = T_l = (|\xi|^2 + \sigma^2)/2\).

**Proof:** Omitted.

V. PROOF OF THEOREM 1

A. Part 1)

We show that a radial quantizer (9) achieves the rate per unit-energy \(1/\sigma^2\). Together with (8), this proves Theorem 1.

To end this, we first note that, conditioned on \((H, X) = (h, x)\), the squared magnitude of \(\hat{\mathbf{Y}}\) is a noncentral \(\chi^2\) distribution with degree 2 and noncentrality parameter \(\frac{2}{\sigma^2}|h|^2|x|^2\) [16, p. 8]. Consequently, a radial quantizer yields [16, Sec. 2-E]

\[
\text{Pr}(Y = 1 \mid H = h, X = x) = Q_1\left(\sqrt{\frac{2}{\sigma^2}|h|^2|x|^2}, \sqrt{\frac{2}{\sigma^2}1}\right)
\]

where \(Q_1(\cdot, \cdot)\) denotes the first-order Marcum Q-function [16, Eq. (2.20)]. Furthermore, for \(x = 0\) this becomes

\[
\text{Pr}(Y = 1 \mid H = h, X = 0) = e^{-\frac{h^2}{\sigma^2}}.
\]

We thus obtain

\[
D(P_{Y|H,X=\xi} \mid P_{Y|H,X=0}) = E\left[ Q_1\left(\sqrt{\frac{2}{\sigma^2}|H|\xi, \sqrt{\frac{2}{\sigma^2}}1\right), \log \frac{1}{1 - e^{-\frac{h^2}{\sigma^2}}} \right]
\]

\[
+ E\left[ H_b\left(1 - Q_1\left(\sqrt{\frac{2}{\sigma^2}|H|\xi, \sqrt{\frac{2}{\sigma^2}}1\right)\right) \right] - E\left[ Q_1\left(\sqrt{\frac{2}{\sigma^2}|H|\xi, \sqrt{\frac{2}{\sigma^2}}1\right) \right]
\]

\[
\geq E\left[ Q_1\left(\sqrt{\frac{2}{\sigma^2}|H|\xi, \sqrt{\frac{2}{\sigma^2}}1\right) \right]\frac{\xi^2}{2} - \log 2 \quad (18)
\]

where \(H_b(\cdot)\) denotes the binary entropy function, i.e.,

\[
H_b(p) \triangleq \begin{cases} p \log \frac{1}{p} + (1-p) \log \frac{1}{1-p}, & \text{for } 0 < p < 1 \\ 0, & \text{for } p = 0 \text{ or } p = 1. \end{cases}
\]

Here the inequality follows because the second term in the first step is nonnegative, and because the binary entropy function is upper-bounded by \(\log 2\).

We choose \(T = \mu|H|\xi\) for some fixed \(\mu \in (0, 1)\) and lower-bound the RHS of (18) using the general lower bound on the first-order Marcum Q-function [16, Sec. C-2, Eq. (C.24)]

\[
Q_1(\alpha, \beta) \geq 1 - \frac{1}{2}e^{-\frac{(\alpha - \beta)^2}{4}} - e^{-\frac{(\alpha + \beta)^2}{4}}, \quad \alpha > \beta \geq 0.
\]

We thus obtain for the first term on the RHS of (18)

\[
E\left[ Q_1\left(\sqrt{\frac{2}{\sigma^2}|H|\xi, \sqrt{\frac{2}{\sigma^2}|H|\xi\right) \right]\frac{\mu^2|H|^2|\xi|^2}{\sigma^2}
\]

\[
\geq \frac{\mu^2E[|H|^2]|\xi|^2}{\sigma^2} - \frac{1}{2} E\left[ \exp\left(-\frac{1}{\sigma^2}|H|^2|\xi|^2(1-\mu)^2\right) \right]
\]

\[
+ \frac{1}{2} E\left[ \exp\left(-\frac{1}{\sigma^2}|H|^2|\xi|^2(1+\mu)^2\right) \right]
\]

\[
\geq \frac{\mu^2E[|H|^2]|\xi|^2}{\sigma^2} - \frac{2}{\sigma^2}(1-\mu)^2 \quad (19)
\]

where the last step follows because 0 \(\leq xe^{-ax} \leq 1/(ea)\) for every \(a > 0\). Combining (19) with (18), and computing its ratio to \(|\xi|^2\) in the limit as \(|\xi|^2\) tends to infinity, yields

\[
\hat{C}(0) \geq \frac{\mu^2E[|H|^2]}{\sigma^2} = \frac{\mu^2}{\sigma^2} \quad (20)
\]

Theorem 1 follows then by letting \(\mu\) tend to one.

B. Part 2)

We first note that, by the Data Processing Inequality for relative entropy [10, Sec. 2.9], the relative entropy on the RHS of (7) is upper-bounded by the relative entropy corresponding to the unquantized channel, i.e., [6, Eq. (64)]

\[
\frac{D(P_{Y|X=x} \mid P_{Y|X=0})}{|\xi|^2} \leq \frac{1}{\sigma^2} \log \left(1 + \frac{|\xi|^2}{\sigma^2}\right) \quad (21)
\]
Consequently, the capacity per unit-cost (7) is strictly smaller than $1/\sigma^2$ unless $|\xi|$ tends to infinity. It thus remains to show that

$$
\limsup_{|\xi| \to \infty} \sup_D D(P_{Y|X=\xi} \parallel P_{Y|X=0}) \leq \frac{1}{\sigma^2}.
$$

To this end, we first note that, for every $\xi \neq 0$, the supremum in (22) over all quantization regions $D$ can be replaced with the supremum over all radial quantizers (9). Indeed, for every quantization region satisfying

$$
\Pr(Y = 1 \mid X = \xi) = \beta, \quad 0 < \beta < 1
$$

the relative entropy

$$
\begin{align*}
D(P_{Y|X=\xi} \parallel P_{Y|X=0}) &= \beta \log \frac{1}{\Pr(Y = 1 \mid X = 0)} + (1 - \beta) \log \frac{1}{1 - \Pr(Y = 1 \mid X = 0)} - H_b(\beta) \\
&= (1 + \beta) \log \frac{1}{1 - \Pr(Y = 1 \mid X = 0)} - H_b(\beta) - H_b(\beta) - \frac{1}{\sigma^2} \log \frac{1}{\beta},
\end{align*}
$$

is a convex function of $\Pr(Y = 1 \mid X = 0)$. Thus, for every $0 < \beta < 1$, the RHS of (23) is maximized for the quantization region that minimizes (or maximizes) $\Pr(Y = 1 \mid X = 0)$ while holding $\Pr(Y = 1 \mid X = \xi) = \beta$ fixed. By the Neyman-Pearson lemma [17], such a quantization region has the form

$$
D_\lambda = \left\{ \tilde{y} \in \mathbb{C} : \frac{f(\tilde{y}|0)}{f(\tilde{y}|\xi)} \leq \Lambda, \quad \Lambda > 0 \right\}
$$

(or the complement thereof), where $f(\tilde{y}|x)$ denotes the conditional density of $Y$, conditioned on $X = x$, and $\Lambda$ is such that $\Pr(\tilde{Y} \in D_\lambda \mid X = \xi) = \beta$. (Note that for every $0 < \beta < 1$ there exists such a $\Lambda$ since, for the above channel model (1), $\Pr(\tilde{Y} \in D_\lambda \mid X = \xi)$ is a continuous, strictly increasing function of $\Lambda > 0$.) The likelihood ratio on the RHS of (24) is readily evaluated as

$$
f(\tilde{y}|0) = \frac{(1 + |\xi|^2/\sigma^2)^{1/2}}{(1 + \Lambda^2/\sigma^2)^{1/2}}, \quad \tilde{y} \in \mathbb{C}.
$$

Consequently, $D_\lambda$ is the same as (9) with

$$
T = \sigma \sqrt{1 + \frac{\sigma^2}{|\xi|^2} \log \frac{1 + \Lambda^2/\sigma^2}{1 + \Lambda^2/\sigma^2}}.
$$

We thus obtain that, for every $\xi \neq 0$, the relative entropy $D(P_{Y|X=\xi} \parallel P_{Y|X=0})$ is maximized by a radial quantizer (9).

For such a quantizer, we have

$$
\Pr(Y = 1 \mid X = x) = \exp\left(-\frac{T^2}{|x|^2 + \sigma^2}\right),
$$

which yields

$$
\begin{align*}
D(P_{Y|X=\xi} \parallel P_{Y|X=0}) &= e^{-|\xi|^2/2\sigma^2} \log \frac{1}{e^{-|\xi|^2/2\sigma^2}} + \left[1 - e^{-|\xi|^2/2\sigma^2}\right] \log \frac{1}{e^{-|\xi|^2/2\sigma^2}} - H_b\left(e^{-|\xi|^2/2\sigma^2}\right) \\
&\leq \frac{T^2}{\sigma^2} e^{-|\xi|^2/2\sigma^2} + \left[1 - e^{-|\xi|^2/2\sigma^2}\right] \log \left(1 - e^{-|\xi|^2/2\sigma^2}\right) \\
&\leq \frac{T^2}{\sigma^2} e^{-|\xi|^2/2\sigma^2} + 1 - e^{-|\xi|^2/2\sigma^2}
\end{align*}
$$

where the second step follows because $H_b(e^{-\cdot}) \geq 0$ and $\exp(-T^2/(|\xi|^2 + \sigma^2)) \geq \exp(-T^2/\sigma^2)$, and the third step follows because $-x \log x < 1, 0 < x < 1$.

The first term on the RHS of (25) is maximized for $T^2 = |\xi|^2 + \sigma^2$. The RHS of (25) is thus upper-bounded by

$$
D(P_{Y|X=\xi} \parallel P_{Y|X=0}) \leq \frac{|\xi|^2}{\sigma^2} + \frac{2}{e}.
$$

Dividing the RHS of (26) by $|\xi|^2$, and computing the limit as $|\xi|$ tends to infinity, yields

$$
\limsup_{|\xi| \to \infty} \sup_D D(P_{Y|X=\xi} \parallel P_{Y|X=0}) \leq \frac{1}{e \sigma^2} + \frac{1}{|\xi|^2}.
$$

This proves Theorem 2.

Acknowledgment

Enlightening discussions with A. Martinez and comments from S. Verdú are gratefully acknowledged.

References

Model Switching and other Unconventional Fun with Experts

Steven de Rooij
Centrum Wiskunde & Informatica (CWI)
Science Park 123, Amsterdam, Netherlands
Email: s.de.rooij@cwi.nl

I. Universal Coding and Regret

Universal codes combine a number of codes into one that achieves code lengths close to those of the best of the bunch. We consider the strongest notion of universality, where we compete with the best code for any data sequence, not just in expectation. When this is the goal, a natural performance measure is regret: the difference between the universal code length and the length of the best original code. Given a fixed finite set of $K$ codes, a simple universal combination can be obtained with a two-part scheme, where the first $\lceil \log_2 K \rceil$ bits are used to identify the original codes to be used for the data, and the second part is the actual encoding of the data using that code. The regret of this code is bounded by the length of the first part of the code. (From here on, all logarithms are binary and we ignore the rounding of code lengths to integer numbers of bits.)

This idea can be taken a step further. Consider the case where a good code is available for any reasonably small segment of the input sequence, but either the data or the codes themselves are so changeable that none of the $K$ original codes perform very well on the entire data sequence. In such cases, a stronger regret guarantee is desirable. For simplicity, fix the number of source symbols at $n$. Then, starting from $K$ codes, first construct a new set of all “tracking” codes that split the input sequence into $m$ blocks, and use one of the $K$ original codes for each block. The goal is now to minimise the regret with respect to this extended set of codes. Counting how many such codes there are is a simple combinatorial exercise; we can subsequently use a two-part code as before to obtain a regret $R(x^n, m)$ satisfying

$$R(x^n, m) \leq \log \left( \frac{n - 1}{m - 1} \right) + m \log K. \quad (1)$$

This solution is not quite satisfactory. First, it requires finding the best tracking code; while this can be done using dynamic programming, we will see that it is possible to obtain similar regret guarantees with much faster algorithms. Second, the number of segments $m$ is a parameter of the algorithm, but $m$ is typically unknown so we would like to have a regret guarantee that is valid for all $m$ simultaneously. Third, the code is not sequential, making it useless in an online setting.

A number of very simple and elegant algorithms have been developed that avoid these issues. Some derive from the information theory literature [Wil07], [VW98], [SM99], but there are also important, and strongly related results in online learning that deserve more exposure [HW98], [Vov99], [BW02], [CBL06], [GLL08]. This text is based on our paper [KdR08], which outlines the common structure to these algorithms.

II. Expert Sequence Priors

Universal codes of the kind described above are most conveniently defined and analysed in the Bayesian framework. As a first step, we switch to probability theory and replace the length functions $L_1, \ldots, L_K$ of the $K$ original codes by probabilistic sources $P_k$, such that $-\log P_k(x^n = x^n) = L_k(x^n)$ for all $k$ and all data sequences $x^n = x_1, \ldots, x_n \in X^*$ (for simplicity assume the alphabet to be discrete). Such probabilistic sources can now be used in a sequential prediction setting; the accumulated logarithmic loss exactly corresponds to the code length:

$$\sum_{t=1}^{n} -\log P_k(x_t = x_t|x^{t-1}) = -\log P_k(x^n = x^n) = L(x^n).$$

In the online learning literature, the prediction strategies $P_k$ are called “experts” because, unless we have additional knowledge about the data generating process, which we do not wish to assume, we have to use their predictions.

We now extend the model class as follows. Let $k^n \in \{1, \ldots, K\}^n$ denote a sequence of expert identifiers. Define $P_{k^n}(x^n) = P_{k_1}(X_1) \cdot P_{k_2}(X_2|X_1) \cdot \ldots \cdot P_{k_n}(X_n|X_{n-1}).$

We do not know which sequence of experts will yield the best predictions, but we can represent our uncertainty about the data generating process, which we do not wish to assume, we have to use their predictions.

We can use this prior to make predictions by conditioning the Bayesian marginal distribution:

$$P(X_{n+1}|x^n) = \frac{P(x^{n+1})}{P(x^n)} = \frac{\sum_{k^n+1} P_{k^n+1}(x^{n+1}; X_{n+1})}{\sum_{k^n} P_{k^n}(x^n)}.$$  \quad (2)

It is now also very easy to obtain a reasonable regret bound, by dropping every term from the marginal likelihood except the one we are interested in. Choose any reference expert sequence $\hat{k}^n$, and let $m$ be the number of blocks it has. Then

$$R(x^n, k^n) = -\log P(x^n) - (-\log P_{\hat{k}^n})$$

$$= -\log \sum_{k^n} P_{k^n}(x^n)\pi(k^n) + \log P_{\hat{k}^n}(x^n)$$

$$\leq -\log \left( P_{\hat{k}^n}(x^n)\pi(\hat{k}^n) \right) + \log P_{\hat{k}^n}(x^n)$$

$$= -\log \pi(\hat{k}^n). \quad (3)$$
A. Example

In general, the best sequence of experts may have a very low prior probability, so it will be hard to compete with. However, we can construct the prior such that expert sequences with relatively few blocks receive a high prior probability. For example, we may set

$$\pi(k^n) = K^{-m} \alpha^{n-1} \left( 1 - \frac{\alpha}{\alpha} \right)^{m-1}, \quad (4)$$

where $m$ is the number of blocks in $k^n$, and $\alpha \in [0, 1]$ is a hyperparameter that can be interpreted as the “switching rate”: it is the probability of a new block starting at any given time. It may be verified that this prior sums to one.

An algorithm to efficiently compute the predictions of this distribution, called Fixed Share, was first published in COLT 1995; see [HW98] for the journal version. For Fixed Share, the regret bound (3) reduces to

$$R(x^n, k^n) \leq m \log K - n \log \alpha - (m - 1) \log \left( 1 - \frac{\alpha}{\alpha} \right).$$

The bound is optimised by setting the hyperparameter to $\alpha^* = (n - m + 1)/(n - 1)$, which yields

$$R(x^n, k^n) \leq m \log K + (n - 1)H(\alpha^*), \quad (5)$$

where $H$ denotes the binary entropy function. Note that this bound is very close to (1); the slack is necessary because this new regret bound is valid for all $m$, whereas (1) is tight for a single fixed $m$.

B. Second Example: Hyperpriors

In case the expert sequence prior is burdened by an unknown parameter, we can “integrate it out” using a hyperprior. Let $\pi^{(\alpha)}$ denote an expert sequence prior $\pi$ with hyperparameter $\alpha$, and let $P^{(\alpha)}$ denote the tracking distribution with expert sequence prior $\pi^{(\alpha)}$. Now impose a hyperprior $\rho$ on $\alpha$. We then obtain the following parameterless distribution:

$$P(X^n) = \int P^{(\rho)}(X^n)^{\rho(\alpha)} \pi^{(\alpha)}(X^n) \rho(\alpha) \, d\alpha$$

$$= \sum_k P_{K^n}(X^n) \int P^{(\rho)}(k^n)^{\rho(\alpha)} \pi^{(\alpha)}(k^n) \rho(\alpha) \, d\alpha.$$

Note that the final integral itself defines an expert sequence prior. We will call it $\sigma$. Thus, to obtain a parameterless tracking distribution we do not have to look at the data; it suffices to mix the expert sequence prior using $\rho$.

In case of the example of the previous section, with $\pi^{(\alpha)}$ given as in (4) and hyperprior $\rho(\alpha) = \text{Beta}(\frac{1}{2}, \frac{1}{2})$, we find

$$\sigma(k^n) = K^{-m} \frac{\Gamma(n - m + \frac{1}{2}) \Gamma(m + \frac{1}{2})}{\pi \Gamma(n + 1)}.$$

Around the time that Fixed Share was published, but completely independently, Paul Volf and Frans Willems developed an algorithm dubbed the “Switching Method”, that efficiently predicts according to this distribution [Wii07], [VW98]. It can be shown that its regret exceeds (5) by at most $\frac{1}{2} \log n + 1$ bits, a modest price to be paid for a completely parameterless strategy.

In the next section we proceed to show how Fixed Share and the Switching Method can be implemented efficiently.

III. COMPUTATION USING HMMS

In general, the predictions of an expert distribution based on an expert sequence prior (2) may require summing an exponential number of terms, but the complexity can be reduced dramatically if the expert sequence prior admits a simple sufficient statistic. This is the case for the two example priors of the previous section: in Fixed Share, the marginal prior distribution on the next expert $\pi(k_{n+1} | k^n)$ can be expressed as a function of only the current expert $k_n$. Namely,

$$\pi(k_{n+1} = k | k^n) = \frac{\alpha}{K} + 1 \{ k = k_n \} (1 - \alpha).$$

Such expert distributions can be represented by a Hidden Markov Model (HMM), where the hidden state is such a sufficient statistic. The value of the hidden variable determines the distribution on experts; the experts’ predictions are weighted according to this distribution. It is convenient to represent the prior in the form of a state transition diagram for the hidden states. For the Fixed Share algorithm with four experts, the diagram looks as follows:

All straight transitions have probability $1 - \alpha$; they represent that no new block is started at that sample size. The transitions into the centre nodes have probability $\alpha$; they represent a switch to a new block. The centre nodes are “silent states” where no prediction has to be produced; such states redistribute some of the probability mass over the experts. The arcs out of the silent states all have probability $1/K$.

Using the Forward algorithm with these state transitions, the distribution on the hidden state can be updated in $O(n K)$, so that the entire data set can be processed in $O(n K)$. The switching method is only slightly more complicated. In this case, the currently used expert is not sufficient to determine the probability of starting a new block: we also need to know how many blocks there were previously. The following state transition diagram visualises the state transition diagram required to calculate $\sigma(k_{n+1} | k^n)$. For simplicity it is for two experts, and we also assume that the first expert always predicts first. Then the current expert is determined by the number of switches modulo 2.
Much of current online learning research is related to prediction with expert advice, but it may not be instantly recognisable as such, as over time the problem has been generalised substantially. Rather than that the learner uses a set of experts who make predictions in the form of probability distributions, is subsequently penalized with logarithmic loss, before finally observing the actual outcome, in the more general setting both experts and outcomes are abstracted away altogether: the learner chooses an action from some space of allowed actions, and receives an arbitrary loss. This more general setup allows the theory to encompass online linear optimisation and prediction problems with loss functions other than logarithmic loss. It also makes the problem harder, and perhaps less directly applicable to information theory. As a starting point, see [CBL06].

IV. THERE IS MORE

The power of expert tracking algorithms is twofold. First, they are black box: any online prediction strategy can be used as an expert. As such they can be applied very generally. One example is in [vEGdR11], where the estimators associated with each a series of model classes are used as “experts”. The paper subsequently uses an algorithm similar to Fixed Share to improve the performance of Bayesian Model Averaging under many circumstances. Second, very attractive computational complexity can sometimes be achieved. For example, the Fixed Share algorithm runs exactly as fast as Bayesian Model Averaging itself.

Based on our paper [KdR08], we have seen two expert tracking algorithms as examples of how you can do more with a bunch of prediction strategies than what everyone always seems to be doing, which is to just take the Bayesian mixture. The preprint of the full paper discusses several other expert sequence priors for tracking, as well as more sophisticated methods to analyse the resulting performance.

Note that the time complexity of the forward algorithm on all symbols has increased to $O(n^2 \cdot K)$.

REFERENCES


Here the upward arcs represent the starting of a new block, and the straight arcs represent staying in the same block. For the $ith$ node from the left, the $ith$ row from the bottom, the probability of the upward arc is $(s + 1/2)/(n + 1)$ and the probability of the straight arc is one minus that; in other words the Krichevsky-Trofimov estimator is used to predict whether or not a switch occurs.
Some Old and New Relations between Information and Estimation

Kartik Venkat*, Tsachy Weissman*

Elegant relationships between classical quantities in information and estimation arise in the presence of additive Gaussian noise. In this talk, we review and present these relationships as expectations of random quantities, and subsequently present some of our recent findings pertaining to their ‘pointwise’ analogues.

Duncan, in [1], showed that for the continuous-time additive white Gaussian noise channel, the minimum mean squared filtering (causal estimation) error is twice the input-output mutual information for any underlying signal distribution. Another discovery was made by Guo et al. in [2], where the derivative of the mutual information was found to equal half the minimum mean squared error in non-causal estimation. By combining these two intriguing results, the authors of [2] also establish the remarkable equality of the causal mean squared error (at some ‘signal to noise’ level snr) and the non-causal error averaged over ‘signal to noise’ ratio uniformly distributed between 0 and snr. There have been extensions of these results to the presence of mismatch. In this case, the relative entropy and the difference of the mismatched and matched mean squared errors are bridged together: Mismatched estimation in the scalar Gaussian channel was considered by Verdú in [3]. In [4], a generalization of Duncan’s result to incorporate mismatch for the full generality of continuous time processes is provided. In [5], Kadota et al. generalize Duncan’s theorem to the presence of feedback.

In [6], the pointwise analogues of these relationships are obtained, giving considerable insight into the above results. As an illustration, consider Duncan’s 1970 result, which can equivalently be expressed saying that the difference between the input-output information density and half the causal estimation error is a zero mean random variable (regardless of the distribution of the channel input). We characterize this random variable explicitly, rather than merely its expectation. Classical estimation and information theoretic quantities emerge with new and surprising roles. For example, the variance of this random variable turns out to be given by the causal MMSE (which, in turn, is equal to twice the mutual information by Duncan’s result).

REFERENCES


* Stanford University. Email: kvenkat@stanford.edu, tsachy@stanford.edu
Polar martingales of maximal spread

Emmanuel Abbe
Faculté Informatique et Communications
Ecole Polytechnique Fédérale de Lausanne
Email: emmanuel.abbe@epfl.ch

Abstract—This paper investigates polar codes for $q$-ary input channels using other kernels than $[1, 1]$ to construct the generator matrix. The kernel is optimized by maximizing the spread of the polar martingale and it is shown that in certain cases, the resulting construction has a significantly improved error probability (even at small block length like $n = 1024$).

I. INTRODUCTION

The generator matrix of a polar code [1] of block length $n$ is obtained by deleting some rows of the matrix $G_n = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} ^{\otimes \log_2 n}$. Which rows to delete depends on the channel and on the targeted error probability (or rate). For a symmetric discrete memoryless channel $W$, the rows to be deleted are indexed by

$$B_{\epsilon,n} := \{i \in [n] : I(U_i; Y^n U_{i-1}) \leq 1 - \epsilon\}, \quad (1)$$

where $\epsilon$ is a parameter governing the error probability, $U^n$ has i.i.d. components which are uniform on the input alphabet, $X^n = U^n G_n$ and $Y^n$ is the output of $n$ independent uses of $W$ when $X^n$ is the input. The key observation at the root of this construction can be explain by considering $n = 2$. Let $u_1, u_2 \in \mathbb{F}_2 = \{0,1\}$,

$$x_1 = u_1 + u_2 \quad (2)$$

$$x_2 = u_2 \quad (3)$$

and let $Y_1, Y_2$ be the output of two independent uses of a binary input channel $W$ when $x_1, x_2$ are the inputs. Note that the binary input channels

$$W^- : u_1 \rightarrow Y_1, Y_2 \quad (4)$$

$$W^+ : u_2 \rightarrow Y_1, Y_2, u_1 \quad (5)$$

satisfy the relations

$$I(W^-) \leq I(W) \leq I(W^+) \quad (6)$$

$$I(W^+) + I(W^-) = 2I(W) \quad (7)$$

where $I(W)$ denotes the mutual information of the channel $W$ when the input distribution is uniform over $\mathbb{F}_2$. Therefore, we have transformed two independent uses of the channel $W$ into two uses of the channels $W^-$ and $W^+$, with overall the same amount of mutual information. If one had to transmit only one bit uniformly drawn, using $W^+$ rather than $W$ would lead to a lower error probability. One can then iterate this argument, after $\log_2(n)$ iterations, one obtains the channels $u_i \mapsto Y^n u_{i-1}$. For a given number of information bits to be transmitted (rate), selecting the channels having largest mutual informations leads to the least error probability. As explained in the next section, polarization happens in the sense that as $n$ tends to infinity, these synthesized channels have mutual information tending to either 0 or 1. Hence, sending information bits on the high mutual information channels (equivalently, deleting rows of $G_n$ corresponding to low mutual information channels) allows to achieve communication rates as large as the mutual information of the original binary input channel. The construction extends to $q$-ary input alphabets when $q$ is prime, using the same matrix $G_n = \begin{bmatrix} 1 & 0 \end{bmatrix} ^{\otimes \log_2 n}$, while carrying the operations over $\mathbb{F}_q$.

It is tempting to investigate what happens if one keeps the Kronecker structure for the generator matrix but modifies the kernel $[1, 1]$. For binary input alphabets, there might not be another interesting choice. One can consider kernel matrices which are not $2 \times 2$ but $k \times k$. In this case, [3] shows that a significant improvement in the error probability rate can be achieved, however, to the cost of suffering from a complexity increase and a much larger block length requirement. Not as much has been studied concerning modifying the kernel matrix over $\mathbb{F}_q$. In [4], the error probability of non-binary polar codes constructed on the basis of Reed-Solomon matrices is calculated using numerical simulations on $q$-ary erasure channels. It is confirmed that 4-ary polar codes can have significantly better performance than binary polar codes. In this paper, our goal is to investigate potential improvements at finite block length using modified kernels over $\mathbb{F}_q$. We propose to pick kernels not by optimizing the polar code exponent as in [4] but by maximizing the polar martingale spread. The resulting improvement is illustrated with numerical simulations. Preliminary theoretical results are provided and it is shown how the proposed criteria connects to new entropy maximization problems.

A. Polar martingale

In order to show that polarization happens, namely that

$$\left|\{i \in [n] : I(U_i; Y^n U_{i-1}) \in (\epsilon, 1 - \epsilon)\}\right| \rightarrow 0, \quad (8)$$

it is helpful to rely on a random process having a uniform measure on the possible realizations of $I(U_i; Y^n U_{i-1})$, so that counting the number of such mutual informations in $(\epsilon, 1 - \epsilon)$ is obtained by evaluating the probability that the process lies in this interval. The process is defined by taking $\{B_n\}_{n \geq 1}$ to be
i.i.d. uniform random variables valued in \{-, +\} and defining the binary (or \(q\)-ary with \(q\) prime) random input channels \(\{W_n, n \geq 0\}\) by

\[
W_0 := W, \\
W_n := W_{B_n}, \quad \forall n \geq 1.
\]  

(9)

The polarization result is then expressed as

\[
P\{I(W_n) \in (\varepsilon, 1 - \varepsilon)\} \to 0.
\]  

(10)

The process \(I(W_n)\) is particularly handy as it is a bounded martingale with respect to the filtration \(B_n\). Therefore, \(I(W_n)\) converges almost surely, which means that almost surely, for any \(\varepsilon > 0\) and \(n\) large enough, \(|I(W_{n+1}) - I(W_n)| = I(W_n^+) - I(W_n) < \varepsilon\). Since for \(q\)-ary input channels (\(q\) prime), the only channels for which \(I(W^+) - I(W)\) is arbitrarily small is when \(I(W)\) is arbitrarily close to 0 or 1, the conclusion of polarization follows. Hence, the key point is that the martingale \(I(W_n)\) is a random walk in \([0, 1]\) which is 'unstable' at any points \(I(W) \in (0, 1)\) as it must move from at least \(I(W^+) - I(W) > 0\) in this range. The plot of \(I(W^+) - I(W) > 0\) for different values of \(I(W)\) is provided in Figure 1. This paper is motivated by the following observation: the larger the spread \(I(W^+) - I(W)\), the more unstable the martingale is at non-extremal points and hence the faster it should converge to the extreme (i.e., polarized channels).

When restricting the channels to be 'additive noise', one can equivalently work with the 'source' setting, in which case the corresponding martingale spread is at least \(H(X + X') - H(X)\) where \(X, X'\) are i.i.d. under the noise distribution. In [2], the rate of convergence of the polar martingale is studied as a function of the block length. We will investigate in this paper the performance at finite block length.

II. PROBLEM: KERNELS WITH MAXIMAL SPREAD

Being interested in the performance of polar codes at finite block length, we start in this paper with the optimization of the kernel matrix over \(\mathbb{F}_q\) for a block length of 2. Namely, we investigate the following optimization:

\[
K^*(W) = \arg \max_{K \in M(\mathbb{F}_q)} I(W^+(W, K))
\]  

(11)

where \(W^+(W, K)\) is the channel \(u_2 \mapsto Y_2 Y_2 u_1\), \((Y_1, Y_2)\) are the output of two independent uses of \(W\) when \((x_1, x_2) = (u_1, u_2)K\) are the inputs. We call \(K^*\) the 2-optimal kernel for \(W\).

We consider in particular channels which are 'additive noise', in which case one can equivalently study the 'source' version of this problem as follows:

\[
\lambda^*(\mu) = \arg \max_{\lambda \in \mathbb{F}_q^*} H(X + \lambda X')
\]  

(12)

where \(X, X'\) are i.i.d. under \(\mu\). As discussed next, the connection with previous problem is obtained by choosing

\[
K^*(W) = \begin{bmatrix} 1 & 0 \\ \lambda^*(\mu) & 1 \end{bmatrix},
\]  

where \(\mu\) is the distribution of the noise of the channel \(W\).

III. EQUIVALENT PROBLEMS AND DEFINITIONS

A general kernel is a matrix over \(\mathbb{F}_q\) which is invertible. For \(2 \times 2\) matrices, let \(K = [a b \ c d]\) be such a matrix and consider \((X_1, X_2)\) to be i.i.d. under \(\mu\) over \(\mathbb{F}_q\) and \((U_1, U_2) = (X_1, X_2)K\). Then, since \(K\) is invertible, we have

\[
2H(\mu) = H(X_1, X_2) = H(U_1, U_2) = H(U_1) + H(U_2 | U_1)
\]  

(13)

and

\[
H(U_1) - H(\mu) = H(\mu) - H(U_2 | U_1)
\]  

(14)

is the entropy spread gained by using the transformation \(K\). To maximize the spread, one may maximize \(H(U_1) = H(aX_1 + cX_2)\) over the choice of \(a\) and \(c\), or simply \(H(X_1 + cX_2)\) over the choice of \(c\) (this leads to the definition of \(\lambda^*\)). Hence, the maximization problem depends on the variable \(c\), \(a\) can be set to 1, and \(b\) and \(d\) need to ensure that \(K\) is invertible, which leads w.l.o.g. to a kernel of the form \(K = \begin{bmatrix} 1 & \alpha \alpha & \beta \end{bmatrix}\). Note that to maximize the spread, one may alternatively minimize \(H(U_2 | U_1) = H(X_2 | X_1 + cX_2)\).

IV. RESULTS FOR \(\mathbb{F}_3\)

**Lemma 1.** Let \(X, X'\) be i.i.d. random variables valued in \(\mathbb{F}_3\), then

\[
H(X + X') \leq H(X - X').
\]  

(15)

(The arithmetic is over \(\mathbb{F}_3\).)

**Proof outline:** Let \(p\) denote the distribution of \(X + X'\) and \(\tilde{p}\) denote the distribution of \(X - X'\). Note that

\[
\|F(p)\|_2 = \|F(\tilde{p})\|_2
\]

where \(F\) is the Fourier transform and \(\|\cdot\|_2\) the \(l_2\)-norm. Hence,

\[
\|p\|_2 = \|\tilde{p}\|_2.
\]

This implies that \(p\) and \(\tilde{p}\) lie on an Euclidean ball (and on the simplex). Moreover, note that \(\tilde{p}\) is such that \(\tilde{p}(1) = \tilde{p}(2)\) and
\[ \hat{p}(0) \geq \hat{p}(1). \] Finally, because of the triangular shape of the entropy ball, one can show that the entropy ball passing by \( \hat{p} \) is contained in the Euclidean ball, implying the desired result.

**Corollary 1.** For a probability distribution \( \mu \) over \( \mathbb{F}_3 \),

\[ \lambda^{*}(\mu) = 2 \]

if \( \mu(1) \neq \mu(2), \) and \( \lambda^{*}(\mu) = \{1, 2\} \) if \( \mu(1) = \mu(2). \)

The gap between \( H(X + X') \) and \( H(X - X') - H(X) \) is illustrated in Figure 2. Figure 3 illustrates the improvements of the error probability of a polar code using the kernel \( \left[ \begin{array}{c} 1 & 0 \\ 0 & 1 \end{array} \right] \) instead of \( \left[ \begin{array}{c} 1 & 1 \\ 0 & 1 \end{array} \right] \) for a block length \( n = 1024 \) when the channel is additive noise channel over \( \mathbb{F}_3 \) with noise distribution \( \{0.7, 0.3, 0\} \).

\[ \text{V. RESULTS FOR } \mathbb{F}_q \]

When \( \mu \) is over \( \mathbb{F}_q \) with \( q \geq 5 \), \( \lambda^{*}(\mu) \) varies with \( \mu \). One can check numerically that for the distribution \( \{0.8, 0.1, 0.1, 0.0\} \) we have \( \gamma^{*} = 4 \) whereas for the distribution \( \{0.7, 0.2, 0.1, 0.0\} \) we have \( \gamma^{*} = \{2, 3\} \).

**Lemma 2.** Let \( \mu \) be a probability distribution over \( \mathbb{F}_q \) with support \( S_{\mu} \). If there exists \( \gamma \in \mathbb{F}_q \) such that

\[ |S_{\mu} + \gamma S_{\mu}| = |S_{\mu}|^{2} \quad \text{(16)} \]

then

\[ H(X_{2}|X_{1} + \gamma X_{2}) = 0 \quad \text{(17)} \]

where \( X_{1}, X_{2} \) are i.i.d. under \( \mu \).

Note: the condition on the support could me simplified but as such it makes the conclusion of the Lemma immediate. Also note that \( \lambda \) for which \( H(X_{2}|X_{1} + \gamma X_{2}) = 0 \) is clearly optimal to maximize the spread.

**Proof of Lemma 2:** The condition \( |S_{\mu} + \gamma S_{\mu}| = |S_{\mu}|^{2} \) ensures that knowing \( x_{1} + \gamma x_{2} \) with \( x_{1}, x_{2} \in S_{\mu} \) allows to exactly recover both \( x_{1} \) and \( x_{2} \).

- **Examples of distributions satisfying (16):** Let \( \mu \) be such that \( S_{\mu} = \{0, 1\} \). Picking \( \gamma = 2, \) one obtains 2\( S_{\mu} = \{0, 2\} \) and \( 2S_{\mu} = \{0, 1, 2, 3\} \), and (16) is verified. In this case, using \( \gamma = 1 \) can only provide a strictly smaller spread since it will not set \( H(X_{2}|X_{1} + \gamma X_{2}) = 0 \). It is hence better to use the 2-optimal kernel \( \left[ \begin{array}{c} 1 & 0 \\ 0 & 1 \end{array} \right] \) rather than the original kernel \( \left[ \begin{array}{c} 1 & 0 \\ 0 & 0 \end{array} \right] \), and as illustrated in Figure 4, this leads to significant improvements in the error probability at finite block length. Also note that a channel with noise \( \mu \) satisfying (16) has positive zero-error capacity, which is captured by the 2-optimal kernel as shown with the rapid drop of the error probability (it is 0 at low enough rates since half of the synthesized channels have noise entropy exactly zero). If \( \mu \) is close to a distribution satisfying (16), the error probability is also significantly improved with respect to the original kernel \( \left[ \begin{array}{c} 1 & 0 \\ 0 & 0 \end{array} \right] \).

Over \( \mathbb{F}_3 \), let \( \mu \) be such that \( S_{\mu} = \{0, 1, 2\} \). Picking \( \gamma = 2, \) one obtains 2\( S_{\mu} = \{0, 2, 4\} \) and (16) does not hold. However, picking \( \gamma = 3 \) leads to \( 3S_{\mu} = \{0, 1, 2\} \) and (16) holds. Therefore, \( \gamma^{*} \) varies with \( q \).

Over \( \mathbb{F}_q \), defining \( k = \lfloor \sqrt{q} - 1 \rfloor \), if \( S_{\mu} = \{0, 1, \ldots, k - 1\} \) and \( \gamma = k \), (16) holds.

**VI. DISCUSSION**

We have shown that over \( \mathbb{F}_q \), the martingale spread can be significantly enlarged by using 2-optimal kernels rather than the original kernel \( \left[ \begin{array}{c} 1 & 0 \\ 0 & 0 \end{array} \right] \). In some cases, this leads to significant improvements on the error probability of polar codes, even at low block length \( n = 1024 \). We have considered additive noise channels, and shown that the improvement is particularly significant when the noise distribution...
Fig. 4. Block error probability (in $\log_{10}$ scale) of a polar code using the 2-optimal kernel (red curve – lower curve) vs. original kernel (blue curve) for a block length of $n = 1024$ and an additive noise channel over $\mathbb{F}_5$ with noise distribution $\{0, 0.5, 0.5, 0, 0\}$. This channel takes any symbol of $\mathbb{F}_5$ to itself with probability $1/2$ and shifts any symbol circularly with probability $1/2$.

is concentrated on ‘small’ supports. For distributions which have full support, the improvement may not be significant. It would be interesting to investigate the improvement for the AWGN channel, and check whether this channel falls in the cases where the improvement is significant. It would also be interesting to consider polar codes that have a kernel which changes adaptively in the recursive construction. This will require a more elaborate decoding algorithm but may not hurt the complexity. Finally, it would be interesting to show analytical results on the error probability rate or exponent of 2-optimal kernels, to consider extensions to $k \times k$ rather than $2 \times 2$ kernels, or to consider other criteria for the optimization of the kernel.

ACKNOWLEDGEMENT

I would like to thank Emre Telatar for helpful comments and stimulating discussions.

REFERENCES

Sumset Differential Entropy Bounds

Ioannis Kontoyiannis
Department of Informatics
Athens University of Economics & Business
Patission 76, Athens 10434, Greece
Email: yiannis@aueb.gr
Web: http://pages.cs.aueb.gr/ yiannisk/

Abstract—Terence Tao recently developed a series of new inequalities for the (discrete) Shannon entropy, which parallel sumset and inverse sumset bounds in additive combinatorics. We examine some of their natural analogs for differential entropy. Since the main ingredient in Tao’s proofs (the submodularity of the entropy function) fails in the continuous case, interesting new phenomena arise. We review some known results and present a series of new differential entropy inequalities. These results are based, in part, on joint work with Mokshay Madiman.

I. ADDITIVE COMBINATORICS AND ENTROPY

The field of additive combinatorics [see, e.g., [7] for an introduction] is the theory of additive structures in sets equipped with a group structure. The prototypical example is the study of arithmetic progressions in sets of integers, as opposed to the multiplicative structure that underlies prime factorization and much of classical combinatorics and number theory. There have been several major developments and a lot of high-profile mathematical activity in additive combinatorics in recent years, with perhaps the most famous example being the celebrated Green-Tao theorem on the existence of arbitrarily long arithmetic progressions within the primes.

An important collection of tools in the study of additive combinatorics is a variety of sumset inequalities. Here, the sumset \( A + B \) of two discrete sets \( A \) and \( B \) is defined as, \( A + B = \{ a + b : a \in A, b \in B \} \), and a sumset inequality is an inequality connecting the cardinality \( |A + B| \) of \( A + B \) with the cardinalities of \( A \) and \( B \). Therefore, roughly and somewhat incorrectly speaking, it might be said that additive combinatorics gives bounds on the sizes of discrete additive sets.

In this setting, we recall the natural connection between entropy and set cardinality established by the AEP: The entropy \( H(X) \) can be thought of as the logarithm of the effective cardinality of the alphabet of a discrete random variable \( X \). This suggests a correspondence between bounds for the cardinalities of sumsets like, e.g., \( |A + B| \), and corresponding bounds for the entropy of sums of discrete random variables, e.g., \( H(X + Y) \). This connection appears to have first been identified by Imre Ruzsa, and in the last few years it has also been explored in different directions by, among others, Tao and Vu [6], Lapidoth and Pete [1], Ruzsa [4], Madiman, Marcus and Tetali [3], Madiman and Kontoyiannis [2], and Tao [5].

II. SUMSET BOUNDS AND DIFFERENTIAL ENTROPY

This analogy can be carried further: The continuous AEP states that the differential entropy \( h(X) \) of a continuous random vector \( X \) can be thought of as the logarithm of the (Euclidean or Lebesgue) “volume of the effective support” of \( X \). It is then natural to consider whether the recent discrete sumset entropy bounds can be extended to the continuous case.

Taking as our starting point the results in Tao’s recent work [5], we provide natural differential entropy analogs for the following inequalities:

- Rusza triangle inequality
- Sum-difference inequality
- Pl"{a}nnecke-Rusza inequality
- Iterated sum bound
- Balog-Szemerédi-Gowers lemma
- Rusza’s covering lemma
- Green-Rusza-Freiman inverse-sumset theorem

The difficulty as well as the excitement of this work stem from the fact that, in the continuous case, the natural generalizations of the proofs of the discrete versions of many of these results fail at a deep level. One reason is that the main ingredient in earlier proofs is the submodularity of the discrete entropy functional, which does not hold for differential entropy. And, further, it is the overall structure of the proofs that does not carry on to the continuous case: Not the method, but the actual intermediate steps fail to hold for differential entropy. Therefore, it is necessary to employ different tools and fundamentally new proof strategies.

REFERENCES


Coding Theory and Compressed Sensing through Convex Relaxations

Arash Saber Tehrani, Alexandros G. Dimakis
Dept. of Electrical Eng. University of Southern California
Los Angeles, CA, USA
emails: {saberteh,dimakis}@usc.edu

Abstract—We survey recent connections between convex relaxations used in coding theory and in sparse approximation theory. One important conclusion arising from our results is that graph girth can be used to certify that sparse compressed sensing matrices have good sparse approximation guarantees. This allows us to present the first deterministic measurement matrix constructions that have an optimal number of measurements for \( \ell_1/\ell_2 \) sparse approximation.

I. INTRODUCTION

Sparse approximation theory and compressed sensing have recently received significant attention in signal processing and statistics. We focus on two developments that connect this area with coding theory and allow the translation of results and techniques. The first involves mathematical links [1]–[3] between two linear programming relaxations: basis pursuit for CS reconstruction and the fundamental polytope relaxation for the decoding of binary linear codes [4], [5]. In coding theory, the linear-program (LP) relaxation was introduced by Feldman, Wainwright and Karger [4] and is closely related to the work by Koetter and Vontobel [5]. This work defined the so-called fundamental polytope and structures called pseudocodewords that cause problems to channel decoders (see also the work of Wiberg [6] and Forney et al. [7]). Our recent results [1], [8] connect this theory to the basis pursuit LP relaxation used in compressed sensing. The high-level message is that ‘good’ channel codes can be used over the reals as provably good CS measurement matrices under basis pursuit. This connection allowed us to solve a well-known open problem in compressed sensing, the deterministic construction of measurement matrices with an order-optimal number of rows [1], [8].

The second connection involves the nature of iterative message-passing algorithms used both for channel coding and compressed sensing. A number of iterative algorithms (e.g. [9]–[13]) have been proposed for compressed sensing recovery, with the benefit of faster decoding complexity and comparable performance to basis pursuit. Very similar iterative message-passing algorithms have been developed and used for the decoding of error-correcting codes [14]. More interestingly, the techniques for their analysis have recently found applicability for compressed sensing. Channel-coding-inspired message-passing decoders for compressed sensing problems have been also discussed in [15]–[17].

The fact that both iterative message-passing algorithms and LP relaxations are mathematically connected for these two problems is not an accident: For channel coding, the LP relaxation is currently understood as an approximation to iterative message-passing [18] and the theory of pseudocodewords allows a rigorous non-asymptotic theory for decoding and design of error-correcting codes under polynomial time decoding algorithms.

II. RECENT RESULTS

Assume we observe \( m \) linear measurements of an unknown vector \( \mathbf{e} \in \mathbb{R}^n \):

\[
\mathbf{H} \cdot \mathbf{e} = \mathbf{s},
\]

where \( \mathbf{H} \) is a real-valued matrix of size \( m \times n \), called the measurement matrix. When \( m < n \), this is an underdetermined system of linear equations and one fundamental compressed sensing problem involves recovering \( \mathbf{e} \) assuming that it is also \( k \)-sparse, i.e. it has \( k \) or less non-zero entries.

The sparse approximation problem goes beyond exactly sparse vectors and requires the recovery of a \( k \)-sparse vector \( \hat{\mathbf{e}} \) that is close to \( \mathbf{e} \), even if \( \mathbf{e} \) is not exactly \( k \)-sparse itself. Recent breakthrough results [19], [20] showed that it is possible to construct measurement matrices with \( m = O(k \log(n/k)) \) rows that recover \( k \)-sparse signals exactly in polynomial time. These results rely on randomized matrix constructions and establish that the optimal number of measurements will be sufficient with high probability over the choice of the matrix and/or the signal. Unfortunately, the required properties of Restricted Isometry Property (RIP) [20], Nullspace [21] and high expansion (expansion quality \( \epsilon < 1/6 \)) have no known ways to be deterministically constructed or efficiently checked.

There are several explicit constructions of measurement matrices (e.g. [22], [23]) which, however, require a slightly sub-optimal number of measurements \( m \) growing super-linearly as a function of \( n \), for \( k = p \cdot n \).

We focus on the \textit{linear sparsity} regime where \( k \) is a fraction of \( n \) and optimal number of measurements will also be a fraction of \( n \). The explicit construction of measurement matrices with an optimal number of rows is a well-known open problem in compressed sensing theory (see e.g. [24] and references therein). A closely related issue is that of checking or certifying in polynomial time that a given candidate matrix has good recovery guarantees or satisfies the RIP.

Consider a sparse matrix \( \mathbf{H} \) in \( \{0,1\}^{m \times n} \) that has \( d_v \) ones per row and \( d_c \) ones per column. If the bipartite graph
corresponding to $H$ has $\Omega(\log n)$ girth, then for $k = p \cdot n$ and an optimal number of measurements $m = c_2 \cdot n$, we show that $H$ offers $\ell_1/\ell_1$ sparse approximation under basis pursuit decoding. Our technical requirement of girth, unlike expansion or RIP, is easy to check and several deterministic constructions of matrices with $m = c \cdot n$ and $\Omega(\log n)$ exist, starting with the early construction in Gallager’s thesis [25], and progressive edge-growth Tanner graphs.

Our result is a weak bound, also known as a ‘for-every signal’ guarantee [24]. This means that we have a fixed deterministic matrix and show the $\ell_1/\ell_1$ sparse approximation guarantee with high probability over the support of the signal. To the best of our knowledge, this is the first deterministic construction of matrices with an optimal number of measurements.

Our proof relies on the discussed connections of channel decoding LP and compressed sensing. We rely on a primal-based density evolution technique initiated by Koetter and Vontobel [26] and analytically strengthened in the break-through paper of Arora et al. [27] that established the best known finite-length threshold results for LDPC codes under LP decoding. In our presentation we will survey this area, present recent results and discuss open problems.

REFERENCES


Polar Codes for the Deterministic Broadcast Channel

Naveen Goela∗†, Emmanuel Abbe∗, and Michael Gastpar∗†
∗ Ecole Polytechnique Fédérale de Lausanne, Faculté Informatique et Communications, CH-1015 Lausanne, Switzerland
† University of California, Berkeley, Department of E.E.C.S., Berkeley, CA 94720-1770 USA
Email: {naveen.goela, emmanuel.abbe, michael.gastpar}@epfl.ch

Abstract—We construct and analyze polar codes for the deterministic broadcast channel (DBC) which is comprised of one source transmitting independent messages to \( m \) receivers. For any input distribution, polar codes with rate-splitting achieve all optimal rates within the corresponding multi-user rate region, a polyhedron in \( \mathbb{R}_{+}^{m} \). For fixed \( m \), the encoding and decoding complexities remain \( O(n \log n) \) with \( O(2^{-m^\beta}) \) average block error probability where \( n \) is the block length and \( 0 < \beta < \frac{1}{2} \). In addition, a related joint polarization coding scheme without rate-splitting achieves points on the dominant face of the polyhedron.

Index Terms—Polar codes, deterministic broadcast channel (DBC), total variation distance.

I. INTRODUCTION

Traditionally, Arıkan’s channel polarization [1] was shown to achieve the capacity of binary-input symmetric channels with low encoding and decoding complexity. Subsequently, source polarization was introduced for lossless compression of binary sources [2], lossless Slepian-Wolf communication based on a reduction to the single-source setting [2], and lossy source compression [3]. In this note, we analyze the performance of polar codes for the noiseless multi-receiver deterministic broadcast channel (DBC). Several researchers have characterized (functional and random coding) dualities between the DBC, Slepian-Wolf distributed source coding, and deterministic multiple-access channel (MAC), see e.g. [4]. Polar codes were analyzed for the latter two scenarios using both single-user and joint polarization techniques in [5] and [6]; however, polar codes for the DBC shed new light on explicit, low complexity, capacity-achieving codes in contrast to random binning and joint typicality encoding strategies.

A. The Multi-Receiver DBC

Definition 1: (Deterministic BC) The DBC with \( m \) receivers consists of an input alphabet \( \mathcal{X} \), output alphabets \( \{\mathcal{Y}_{i}\}_{i=1}^{m} \), and \( m \) deterministic functions \( y_{i} = f_{i}(x) \) for \( i \in [m] \), \( x \in \mathcal{X} \), \( y_{i} \in \mathcal{Y}_{i} \). A \((2^{nR_{1}}, 2^{nR_{2}}, \ldots, 2^{nR_{m}})\), \( n \) code for the DBC with independent messages consists of an encoder

\[ x^{n} \colon 2^{nR_{1}} \times 2^{nR_{2}} \times \cdots \times 2^{nR_{m}} \rightarrow \mathcal{X}^{n}, \]

and \( m \) decoders specified by \( \hat{W}_{i} : \mathcal{Y}_{i}^{n} \rightarrow 2^{nR_{i}} \). The probability of error \( P^{(n)}_{e} \) is defined to be the probability that the decoded message is not equal to the transmitted message, i.e.,

\[ P^{(n)}_{e} = P\left( \bigvee_{i=1}^{m} \hat{W}_{i}(Y^{n}_{i}) \neq W_{i} \right), \]

where the message \((W_{1}, W_{2}, \ldots, W_{m})\) is assumed to be uniformly distributed over \( 2^{nR_{1}} \times 2^{nR_{2}} \times \cdots \times 2^{nR_{m}} \).

Theorem 1: (Channel Capacity Region [7] [8]) Let \( \bar{R} = (R_{1}, R_{2}, \ldots, R_{m}) \). The capacity region \( \mathcal{C}_{DBC} \) given deterministic functions \( f_{i}(\cdot) \) is specified as

\[ \mathcal{C}_{DBC} := \text{clo} \left( \bigcup_{X} \mathcal{R}(X) \right), \tag{1} \]

where

\[ \mathcal{R}(X) = \left\{ \bar{R} \in \mathbb{R}_{+}^{m} \bigg| \sum_{i \in S} R_{i} < H(Y(S)), \; \forall S \subseteq [m] \right\}. \tag{2} \]

The notation \( Y(S) = \{Y_{i} : i \in S\} \), \( \text{clo}(S) \) represents closure, and \( H(S) \) the convex hull operation over set \( S \). The union in Eqn. (1) is over random variable \( X \sim P_{X}(x) \) which induces a joint distribution over \( X, Y_{1}, Y_{2}, \ldots, Y_{m} \) via \( Y_{i} = f_{i}(X) \).

B. Random Coding vs. Low Complexity Codes

Shannon-theoretic coding strategies for broadcast channels (see e.g. [9] or [10, Lec. 9] for a survey) rely on random coding. Specifically for the DBC, random binning and joint typicality encoding yield the optimal rates. At the encoder, assuming for a moment \( m = 2 \) receivers, a fixed \( P_{X}(x) \) induces a joint distribution \( P_{Y_{1},Y_{2}}(y_{1},y_{2}) \). All \( y_{1}^{n} \) and \( y_{2}^{n} \) sequences are randomly assigned bin indices \( i \in [2^{nR_{1}}] \) and \( j \in [2^{nR_{2}}] \) respectively. The rates \( R_{1} \) and \( R_{2} \) are selected to ensure that at least one jointly typical pair \((y_{1}^{n}, y_{2}^{n})\) exists in each \((i, j)\) product bin. To send information \( i \) to the first receiver, and information \( j \) to the second receiver, the encoder selects a jointly typical pair \((y_{1}^{n}, y_{2}^{n})\) in the product bin \((i, j)\) and computes the \( x^{n} \) sequence which results in \( y_{1}^{n} \) and \( y_{2}^{n} \). A valid \( x^{n} \) codeword exists due to the deterministic property of \( f_{1}(\cdot) \) and \( f_{2}(\cdot) \). Each receiver decodes its message by looking up the bin index of its received sequence. Random binning and joint typicality encoding require a search over an exponential number of sequences.

Designing low-complexity codes for the DBC requires “binning” in a sense, and constraint satisfaction to ensure an \( x^{n} \) codeword exists which generates the proper \( y_{1}^{n} \) and \( y_{2}^{n} \) output sequences. If \((y_{1}^{n}, y_{2}^{n})\) are jointly typical with respect to
the distribution $P_{Y_1,Y_2}(y_1,y_2)$ induced by $P_X(x)$, a matching codeword $x^m$ is guaranteed because $P_{Y_1,Y_2}(y_1,y_2)$ has zero mass over inconsistent pairs $(y_1,y_2)$. In [11], the authors propose sparse linear coset codes to emulate binning (i.e., the syndrome is the message), combined with survey propagation to enforce the DBC channel constraints. In [12], the authors relate interference management in wireless scenarios with low-complexity coding over the DBC, and in [13], the authors describe a reinforced belief propagation algorithm with nonlinear coding for the DBC. However, going beyond ad-hoc strategies in the present paper, we design polar codes that are low-complexity and provably optimal for achieving points in the DBC capacity region.

C. Simplifying Assumptions

We make the following simplifications to Definition 1: (a) The number of receivers $m = 2$; (b) Polar code design is for achieving vertices of the polyhedron given in Eqn. (2) for fixed $P_X(x)$; (c) The output alphabets $Y_i$ are all $\mathbb{F}_2$. The first two simplifications are without loss of generality. In particular (a) is for compactness of notation and our coding scheme applies for arbitrary pair $(m, n)$, and for (b) it was shown that an arbitrary point in the achievable rate region of a DBC with $m$ receivers maps to a corresponding vertex point in the achievable region of a DBC with $(2m-1)$ receivers if rate-splitting is used [14]. Item (c) is a mild restriction due to the algebraic construction of polar codes. It is possible to generalize the polar code construction to include output alphabets of prime, prime power, and different cardinalities.

Example 1: (Blackwell Channel) In Fig. 1, the Blackwell channel is depicted with $X = \{0,1,2\}$ and $Y = \mathbb{F}_2$. For any fixed distribution $P_X(x)$, it is seen that $P_{Y_1,Y_2}(y_1,y_2)$ has zero mass for the pair $(1,0)$. Let $\alpha \in \left[\frac{1}{2}, \frac{2}{3}\right]$, and $h_{\alpha}$ denote the binary entropy function. Due to the symmetry of this channel, the capacity region is the union of two regions,

\[
\{(R_1, R_2) : R_1 \leq h_{\alpha}(\alpha), R_2 \leq h_{\alpha}(\frac{\alpha}{2}), R_1 + R_2 \leq h_{\alpha}(\alpha + \alpha), \}
\]

where the first region is achieved with input distribution $P_X(0) = P_X(1) = \frac{1}{2}$, and the second region is achieved with $P_X(1) = P_X(2) = \frac{1}{2}$ [10, Lec. 9]. The sum rate is maximized for a uniform input distribution which yields a pentagonal achievable rate region: $R_1 \leq h_{\alpha}(\frac{1}{3}), R_2 \leq h_{\alpha}(\frac{2}{3}), R_1 + R_2 \leq \log_2 3$. We construct polar codes to achieve the vertices of this pentagon, and more generally the vertices of a polyhedron in $\mathbb{R}_+^m$.

II. POLAR CODES

Using the simplifications of Sec. I-C for compactness, we analyze coding over $n$ channel uses of the DBC. Let $m = 2$ receivers, $i \in [m]$ and $j \in [n]$. The channel input is given by $X = \{X_1,X_2,...,X_n\}$ where $X_j \sim P_X$ are i.i.d. random variables. The channel output $Y_{ij} = f_i(X_j)$ and $\forall j$, $(Y_{1j}, Y_{2j}) \sim P_{Y_{1}}, Y_{2}$ where $P_{Y_{1}}, Y_{2}$ is the joint distribution on $\mathbb{F}_2^2$ induced by $P_X(x)$.

A. Polarization

Define the following row vectors of a matrix,

\[
\begin{bmatrix}
\tilde{Y}_1 \\
\tilde{Y}_2
\end{bmatrix} = \begin{bmatrix}
Y_{1,1} & Y_{1,2} & Y_{1,3} & \ldots & Y_{1,n} \\
Y_{2,1} & Y_{2,2} & Y_{2,3} & \ldots & Y_{2,n}
\end{bmatrix}.
\]

(3)

The joint distribution of all output variables is

\[
P_{Y_{1}, Y_{2}}(y_1, y_2) = \prod_{j=1}^{n} P_{Y_{1}, Y_{2}}(y_{1j}, y_{2j}).
\]

(4)

The polar algebraic transformation is defined in terms of an invertible matrix $G_n \in \mathbb{F}_2^{n \times n}$ where $n = 2^\ell$ for $\ell \geq 1$ [2]. Denote the polar transformation of the output variables by

\[
\begin{bmatrix}
\tilde{U}_1 \\
\tilde{U}_2
\end{bmatrix} = \begin{bmatrix}
\tilde{Y}_1 \\
\tilde{Y}_2
\end{bmatrix} G_n.
\]

(5)

where the transformed variables are defined,

\[
\begin{bmatrix}
\tilde{U}_1 \\
\tilde{U}_2
\end{bmatrix} \triangleq \begin{bmatrix}
U_{1,1} & U_{1,2} & U_{1,3} & \ldots & U_{1,n} \\
U_{2,1} & U_{2,2} & U_{2,3} & \ldots & U_{2,n}
\end{bmatrix}.
\]

(6)

Theorem 2 (Polarization [2]): Let the random variables $Y_1$, $Y_2$, $U_1$, $U_2$ be related according to Eqs. (3)-(6). As $n \rightarrow \infty$, for any $\epsilon \in (0,1)$,

\[
\left\{j \in [n] : H(U_{1j}|U_{1j}^{-1}) \geq 1 - \epsilon \right\} \rightarrow nH(Y_1),
\]

\[
\left\{j \in [n] : H(U_{2j}|U_{2j}^{-1}, \tilde{Y}_1) \geq 1 - \epsilon \right\} \rightarrow nH(Y_2|Y_1).
\]

Theorem 2 shows how the randomness of $Y_1$ and $Y_2$ is extracted into $nH(Y_1)+nH(Y_2|Y_1)$ nearly uniform components.

B. Message Indices

To design a polar code for the DBC, we identify the indices of variables in $\bar{U}_1$ and $\bar{U}_2$ that have (conditional) entropy close to one. The Bhattacharyya parameter is closely related to the conditional entropy.

Definition 2: (Bhattacharyya Parameter) Let $(S, V) \sim P_{S|V}$ where $S \in [0,1]$ and $V \in \mathbb{V}$ where $\mathbb{V}$ is an arbitrary countable alphabet. The Bhattacharyya parameter $Z(S|V) \in [0,1]$ is defined

\[
Z(S|V) = 2 \max_{v \in \mathbb{V}} P_{S}(v) \sqrt{P_{S|V}(0|v)P_{S|V}(1|v)}.
\]

(7)

As shown by Arikan in [2], $H(S|V)$ is close to 0 or 1 if and only if $Z(S|V)$ is close to 0 or 1. We define the message indices for $m = 2$ receivers based on the Bhattacharyya parameter of variables comprising the random vectors $U_1, \bar{U}_2, Y_1, Y_2$.

\[
I_1^{(\alpha)} = \{j \in [n] : Z(U_{1j}|U_{1j}^{-1}) \geq 1 - 2\delta_2^{\alpha}\},
\]

(8)

\[
I_2^{(\alpha)} = \{j \in [n] : Z(U_{2j}|U_{2j}^{-1}, \tilde{Y}_1) \geq 1 - 2\delta_2^{\alpha}\},
\]

(9)
where $\delta_n > 0$. According to the rate of polarization [15], we will select $\delta_n \downarrow 0$. As a result of Theorem 2 and the properties of the Bhattacharyya source parameter, for any $\tau > 0$ there exists an $n$ large enough so that both $|I_1^{(n)}| \geq n(H(Y_1) - \tau)$ and $|I_2^{(n)}| \geq n(H(Y_2|Y_1) - \tau)$.

III. Bounding The Total Variation Distance Between Probability Measures

To code over $n$ channel uses of the DBC, we insert uniformly random message bits into the position indexed by message sets $I_1^{(n)}$ and $I_2^{(n)}$. We now begin to establish that for any $\tau > 0$, with $n \to \infty$, the message rates $R_1 \geq H(Y_1) - \tau$ and $R_2 \geq H(Y_2|Y_1) - \tau$ are achievable with $P_0(n)$ to 0. For a DBC with $m = 2$ receivers, the rate pair $(R_1, R_2)$ approaches one vertex point of the pentagonal rate region (defined more generally as a polyhedron in Eqn. (2)). Other optimal vertex points of the polyhedral rate region are achieved similarly by changing the ordering of receivers.

A. Two Probability Measures on a Set of Binary Sequences

We define two probability measures on the set of all $m^n$-length binary sequences (here we assume $m = 2$) which will help in bounding the average block error probability $P_0^{(n)}$ of our encoding/decoding scheme. The i.i.d. joint distribution $P_{\bar{Y}_1, \bar{Y}_2}(\bar{y}_1, \bar{y}_2)$ defined in Eqn. (4) specifies a joint distribution $P_{\bar{U}_1, \bar{U}_2}(\bar{u}_1, \bar{u}_2)$ via the one-to-one linear transform $G_n$ of Eqn. (5). We write this distribution as

$$P_{\bar{U}_1, \bar{U}_2}(\bar{u}_1, \bar{u}_2) = P_{\bar{U}_1}(\bar{u}_1)P_{\bar{U}_2|\bar{U}_1}(\bar{u}_2|\bar{u}_1).$$  

(10)

We now factorize the above as follows,

$$P_{\bar{U}_1}(\bar{u}_1) = \prod_{j=1}^{n} P_{U_{1j}|U_{1j-1}}(u_{1j}|u_{1j-1}^{j-1}),$$  

(11)

$$P_{\bar{U}_2|\bar{U}_1}(\bar{u}_2|\bar{u}_1) = \prod_{j=1}^{n} P_{U_{2j}|U_{2j-1}, \bar{U}_1}(u_{2j}|u_{2j-1}^{j-1}, \bar{u}_1).$$  

(12)

We now define closely related conditional probability distributions $\forall j \in [n],$

$$Q_{U_{1j}|U_{1j-1}}(u_{1j}|u_{1j-1}^{j-1}) \triangleq \frac{1}{2}, \quad \text{if } j \not\in I_1^{(n)},$$

$$\quad \frac{1}{2} \sum_{u_{1j}} P_{U_{1j}|U_{1j-1}}(u_{1j}|u_{1j-1}^{j-1}), \quad \text{otherwise},$$

$$Q_{U_{2j}|U_{2j-1}, \bar{U}_1}(u_{2j}|u_{2j-1}^{j-1}, \bar{u}_1) \triangleq \frac{1}{2}, \quad \text{if } j \not\in I_2^{(n)},$$

$$\quad \frac{1}{2} \sum_{u_{2j}} P_{U_{2j}|U_{2j-1}, \bar{U}_1}(u_{2j}|u_{2j-1}^{j-1}, \bar{u}_1), \quad \text{otherwise}.$$  

Then analogous to Eqn. (11) and Eqn. (12),

$$Q_{\bar{U}_1}(\bar{u}_1) \triangleq \prod_{j=1}^{n} Q_{U_{1j}|U_{1j-1}}(u_{1j}|u_{1j-1}^{j-1}),$$  

(13)

$$Q_{\bar{U}_2|\bar{U}_1}(\bar{u}_2|\bar{u}_1) \triangleq \prod_{j=1}^{n} Q_{U_{2j}|U_{2j-1}, \bar{U}_1}(u_{2j}|u_{2j-1}^{j-1}, \bar{u}_1).$$  

(14)

Essentially $Q_{\bar{U}_1}(\bar{u}_1) = \left(\frac{1}{2}\right)^{|I_1^{(n)}|} g_1(\bar{u}_1)$ and $Q_{\bar{U}_2|\bar{U}_1}(\bar{u}_2|\bar{u}_1) = \left(\frac{1}{2}\right)^{|I_2^{(n)}|} g_2(\bar{u}_1, \bar{u}_2)$ where $g_1(\bar{u}_1)$ and $g_2(\bar{u}_1, \bar{u}_2)$ are nearly indicator functions; i.e., the distributions are approximately composed of i.i.d. Bernoulli(1/2) random variables.

B. Total Variation Bound

Theorem 3: (Total Variation Bound for Joint Distributions)

Let probability measure $P_{\bar{U}_1, \bar{U}_2}(\bar{u}_1, \bar{u}_2)$ be defined as in Eqn. (10). Let $Q_{\bar{U}_1, \bar{U}_2}(\bar{u}_1, \bar{u}_2) \triangleq Q_{\bar{U}_1}(\bar{u}_1)Q_{\bar{U}_2|\bar{U}_1}(\bar{u}_2|\bar{u}_1)$ be defined via Eqn. (13) and Eqn. (14). Then the total variation distance between $P$ and $Q$ is bounded as

$$\sum_{\bar{u}_1, \bar{u}_2} |Q(\bar{u}_1, \bar{u}_2) - P(\bar{u}_1, \bar{u}_2)| \leq 2|I_1^{(n)}|\delta_n + 2|I_2^{(n)}|\delta_n,$$

where we set $\delta_n = \frac{2^{-n^2}}{2n}$ for $0 < \beta < \frac{1}{2}$. Thus the total variation distance is bounded by $O(2^{-n^2}).$

Proof: Let probability distribution $L_{\bar{U}_1, \bar{U}_2}(\bar{u}_1, \bar{u}_2) \triangleq P_{\bar{U}_1}(\bar{u}_1)Q_{\bar{U}_2|\bar{U}_1}(\bar{u}_2|\bar{u}_1)$. Observe by the triangle inequality for total variation distance,

$$\sum_{\bar{u}_1, \bar{u}_2} |Q(\bar{u}_1, \bar{u}_2) - L(\bar{u}_1, \bar{u}_2)| \leq \sum_{\bar{u}_1, \bar{u}_2} |Q(\bar{u}_1, \bar{u}_2) - L(\bar{u}_1, \bar{u}_2)| + \sum_{\bar{u}_1, \bar{u}_2} |L(\bar{u}_1, \bar{u}_2) - P(\bar{u}_1, \bar{u}_2)|.$$

We bound the first term as follows,

$$\sum_{\bar{u}_1, \bar{u}_2} |Q(\bar{u}_1, \bar{u}_2) - L(\bar{u}_1, \bar{u}_2)| = \sum_{\bar{u}_1} \sum_{\bar{u}_2} Q_{\bar{U}_1}(\bar{u}_1)Q_{\bar{U}_2|\bar{U}_1}(\bar{u}_2|\bar{u}_1) - P_{\bar{U}_1}(\bar{u}_1),$$

$$= \sum_{\bar{u}_1} \sum_{\bar{u}_2} Q_{\bar{U}_1}(\bar{u}_1) - P_{\bar{U}_1}(\bar{u}_1) \left( \sum_{\bar{u}_2} Q_{\bar{U}_2|\bar{U}_1}(\bar{u}_2|\bar{u}_1) \right),$$

$$= \sum_{\bar{u}_1} Q_{\bar{U}_1}(\bar{u}_1) - P_{\bar{U}_1}(\bar{u}_1),$$

$$\leq \sum_{\bar{u}_1} \sum_{j \in I_1^{(n)}} \sum_{u_{1j}} \mathbb{E}P\left(\frac{1}{2} - P_{U_{1j}|U_{1j-1}}(0|U_{1j-1}^{j-1})\right).$$

(15)

Similarly, the second term is bounded.

$$\sum_{\bar{u}_1, \bar{u}_2} |L(\bar{u}_1, \bar{u}_2) - P(\bar{u}_1, \bar{u}_2)| = \sum_{\bar{u}_1} \sum_{\bar{u}_2} P_{\bar{U}_1}(\bar{u}_1)Q_{\bar{U}_2|\bar{U}_1}(\bar{u}_2|\bar{u}_1) - P_{\bar{U}_2|\bar{U}_1}(\bar{u}_2|\bar{u}_1),$$

$$\leq \sum_{\bar{u}_1} \sum_{j \in I_2^{(n)}} \sum_{u_{2j}} \mathbb{E}P\left(\frac{1}{2} - P_{U_{2j}|U_{2j-1}, \bar{U}_1}(0|U_{2j-1}^{j-1}, \bar{U}_1)\right),$$

(17)

$$\leq 2|I_2^{(n)}|\delta_n.$$  

(18)

The inequalities in Eqns. (15)-(18) are derived in a very similar way to the inequalities in the rate-distortion analysis of polar codes for (single) source coding in [3, Lemma 4, Lemma 7] and will be omitted here.

IV. POLAR CODING FOR THE DBC

A. Encoding and Decoding Steps

Assuming $n = 2$ receivers, the encoder’s task is to map a message $(W_1, W_2)$ uniformly distributed over $2^nR_1 \times 2^nR_2$ to a codeword $x^n$. The polar encoding strategy is to construct first a pair of $n$-length binary sequences $\bar{u}_1$ and $\bar{u}_2$. The bits $u_{1j}$ with indices $j \in I_1^{(n)}$ are set to the uniformly selected
message bits for the first receiver. Likewise, the bits \( u_{2j} \) with indices \( j \in T_2(n) \) are set to the uniformly selected message bits for the second receiver. Note that the message indices \( T_1(n) \) and \( T_2(n) \) defined in Eqns. (8) and Eqn. (9) are computed once during polar code construction, and do not depend on the realization of variables during the encoding process. The non-message indices in \( u_i \) and \( u_2 \) are obtained via a bit-by-bit successive randomized calculation as follows:

\[
\forall j \notin T_1(n): u_{1j} = \begin{cases} 
0, & \text{w.p. } P_{U_1|U_2|U_1^{-1}}(0|u_{1j}^{-1}), \\
1, & \text{w.p. } P_{U_1|U_2|U_1^{-1}}(1|u_{1j}^{-1}). 
\end{cases}
\]

\[
\forall j \notin T_2(n): u_{2j} = \begin{cases} 
0, & \text{w.p. } P_{U_2|U_1|U_2^{-1}}(0|u_{2j}^{-1}, \bar{u}_1), \\
1, & \text{w.p. } P_{U_2|U_1|U_2^{-1}}(1|u_{2j}^{-1}, \bar{u}_1). 
\end{cases}
\]

The probabilities \( P_{U_1|U_2|U_1^{-1}}(0|u_{1j}^{-1}) \) and \( P_{U_2|U_1|U_2^{-1}}(0|u_{2j}^{-1}, \bar{u}_1) \) above are efficiently computable in \( O(n \log n) \) time due to Arikan’s recursive polarization decomposition (see [2] for the recursive likelihood formulas). Having formed the binary sequences \( u_1 \) and \( u_2 \), the encoder applies the inverse polar transform, \( \bar{y}_1, \bar{y}_2 = [u_1; u_2 G_n^{-1}] \), where \( G_n^{-1} = G_n \) in the binary case. Each channel symbol \( x_j \) of the codeword \( x^n \) is formed by taking any \( x_j \in \bigcup_{m=1}^{T} f_{i}^{-1}(\bar{y}_j) \) if this intersection set is non-empty, otherwise the encoder declares a block error. If the encoder succeeds in transmitting a codeword, each receiver \( i \in \{m\} \) obtains the sequence \( \bar{y}_i \) exactly and applies the \( G_n \) transform to recover \( u_i \), exactly. Knowing the location of the message indices in \( u_i \), each receiver decodes its own message correctly.

**B. Error Performance**

An error event for the DBC occurs exclusively for the encoder if it is unable to construct a codeword \( x^n \). In the following theorem, we assume \( m = 2 \). \( P_{Y_1|Y_2}(y_1, y_2) \) is the induced distribution for arbitrary input distribution \( P_X \), and the target rate pair is \((R_1, R_2) = (H(Y_1), H(Y_2|Y_1))\).

**Theorem 4:** (Average Block Error Probability) Fix \( R_1 < H(Y_1) \), \( R_2 < H(Y_2|Y_1) \), and \( 0 < \beta < \frac{1}{2} \). There exists a sequence of polar codes of length \( n \) for which the achieves rates \((R_1, R_2)\), so that under successive randomized encoding, the expected average block error probability is \( P_e^{(n)} = O(2^{-\alpha n}) \).

**Proof:** Theorem 2 established that the message sets have cardinalities \( |T_1(n)| \rightarrow nH(Y_1) \) and \( |T_2(n)| \rightarrow nH(Y_2|Y_1) \). Let \( \mathcal{E} \) denote the set of all \( 2n \)-length binary sequences written as \( (y_1^{m_1}, y_2^{m_2}) \) which are inconsistent, i.e. \( \exists j \in [n] \) for which \( y_1j, y_2j \) is not a valid output of the DBC for the input symbol \( x_j \). Let \( \mathcal{E} \) denote the set of \( 2n \)-length binary sequences \( (u_1^{m_1}, u_2^{m_2}) \) that correspond to the inconsistent sequences via the one-to-one-to-one transformation \( G_n \). The distribution \( P \) is such that \( \sum_{(u_1^{m_1}, u_2^{m_2}) \in \mathcal{E}} P_{U_1|U_2}(u_1^{m_1}, u_2^{m_2}) = 0 \). Due to Theorem 3,

\[
\sum_{(u_1, u_2) \in \mathcal{E}} Q_{U_1|U_2}(u_1, u_2) = O(2^{-\alpha n}).
\]

The successive randomized encoding procedure of Sec. 4-A selects a codeword by effectively drawing from the distribution \( Q \) for a uniformly selected message. The expected average block error probability of drawing an inconsistent pair is therefore \( P_e^{(n)} = O(2^{-\alpha n}). \)

**V. JOINT/SIMULTANEOUS POLARIZATION METHOD**

Let matrix \( \bar{U} = [\bar{U}_1; \bar{U}_2] \) where \( \bar{U} \in F_2^{2 \times n} \) was defined in Eqn. (6). We make a brief remark about joint polarization methods for the DBC. It was shown in [5, Lemma 1] that,

\[
\frac{1}{n} \sum_{j \in [n]} \left| H(U_j|S) - (U_j^{-1}) \right| \leq \varepsilon
\]

where here the new notation \( U_j \) now denotes the \( j \)-th column of matrix \( \bar{U} \), \( i \) is the \( (i,j) \)-entry of matrix \( U_j \), \( U_j[S] = [U_j(i) : i \in S] \), and \( U^j = [U_1, \ldots, U_j] \). When comparing Arikan’s polarization of Theorem 2 with that of Eqn. (19), one sees that the latter involves joint polarization column by column, whereas the former involves successive polarization bit by bit. It can be shown that joint polarization methods allow for DBC coding schemes that achieve (sum rate) points on the dominant face of the polyhedron in \( R^n_+ \) without rate-splitting.

**VI. CONCLUSION**

The polar encoding strategy is a non-linear mapping from \( m \) messages to one codeword that requires \( O(n \log n) \) complexity to compute. We believe polar codes will be applied in other network communication scenarios to address the high complexity of random binning and joint typicality coding.

**ACKNOWLEDGMENT**

The authors thank S. B. Korada for the helpful discussions regarding the journal paper [3].

**REFERENCES**


Polar Codes for Coordination in Cascade Networks

Ricardo Blasco-Serrano, Ragnar Thobaben, and Mikael Skoglund
KTH Royal Institute of Technology and ACCESS Linnaeus Centre
SE-100 44, Stockholm, Sweden
E-mail: {ricardo.blasco, ragnar.thobaben, mikael.skoglund}@ee.kth.se

Abstract—We consider coordination in cascade networks and construct sequences of polar codes that achieve any point in a special region of the empirical coordination capacity region. Our design combines elements of source coding to generate actions with the desired type with elements of channel coding to minimize the communication rate. Moreover, we bound the probability of malfunction of a polar code for empirical coordination. Possible generalizations and open problems are discussed.

I. INTRODUCTION

The limits of coordination in networks have been recently studied from a mathematical point of view (e.g., [1], [2]). Simple questions like how to measure coordination or how much communication is necessary to achieve a desired level of coordination have been posed and to some extent answered. The authors of [1] developed elements of a fundamental theory with two notions of coordination. In the first one, empirical coordination, the sequences of actions generated in the network must have a type that is close to a desired probability distribution. Empirical coordination is closely related to rate-distortion theory [3]. In fact any good code for rate-distortion is useful for empirical coordination and vice versa [1]. The second notion is that of strong coordination. Here the sequences of actions generated by the nodes must be statistically indistinguishable from those obtained by sampling a certain distribution.

In this work we construct sequences of polar codes (PCs) that achieve a special region of the empirical coordination capacity region for two-node and three-node cascade networks. PCs were introduced by Arıkan as a method to achieve the capacity of any symmetric binary-input discrete memoryless channel (BI-DMC) [4]. Since then they have emerged as a powerful technique to develop achievability results in information theory with structured codes (as opposed to random coding). Korada and Urbanke established in [5] the optimality of PCs for lossy source coding of (symmetric) discrete memoryless sources (DMS) with binary reproduction alphabets. These results were later extended to non-binary channels and reproduction alphabets in [6] and [7], respectively.

Our constructions combine elements of PCs for source compression with PCs for channel coding. In addition, we show that, in line with [1], common randomness is not necessary for implementing PCs for empirical coordination, although it is useful in the proofs. We use the properties of PCs to extend the application of results on the rate of polarization [8] to PCs designed for empirical coordination. Finally, we discuss possible generalizations of our constructions as well as some open problems for future research.

This paper is organized as follows. In Section II we summarize basic results on empirical coordination and polar codes along with the notation. We analyze a simple two-node network in Section III. This serves as a building block for the cascade network, which is addressed in Section IV. We conclude our work in Section V with a discussion on the results of the paper as well as on some open problems.

II. PRELIMINARIES

A. Notation

Scalars are written using normal face x and vectors using bold face x. The i\textsuperscript{th} element of a vector x is denoted by x\textsubscript{i}. For a given set of natural numbers F with size |F|, x\textsubscript{F} is shorthand for the subvector with elements whose positions belong to F. We use upper case letters for random variables (RVs) Y and lower case letters for their realizations y. The joint probability distribution on (X, Y) is denoted by P\textsubscript{X,Y}(x, y). For convenience we shall alternatively drop the subindices or the arguments whenever they are clear from the context. We follow the standard information-theoretic notation from [3].

B. Empirical Coordination

Consider the three-node network in Fig. 1. Node X observes a sequence of N external actions \( \mathbf{X} \) chosen independently and identically distributed (i.i.d.) according to P\textsubscript{X}. Communication from Node X to Node Y and from Node Y to Node Z is possible at rates R\textsubscript{1} and R\textsubscript{2} (bits per action), respectively. We use these resources to have Node Y and Node Z generate sequences of actions Y and Z, respectively, with length N and joint type close to a desired probability function P\textsubscript{Y,Z|X}(Y,Z | X).

\[
    X \sim P_X
\]

\[
    \begin{array}{c}
    \text{Node X} \\
    \uparrow \\
    \text{R}_1 \\
    \text{Node Y} \\
    \downarrow \\
    Y \\
    \text{Node Z} \\
    \downarrow \\
    \text{R}_2 \\
    \downarrow \\
    Z
    \end{array}
\]

Fig. 1. Cascade network.

A \((2^N R_1, 2^N R_2, N)\) coordination code for the network in Fig. 1 consists of an encoding, a recoding, and two decoding functions (see [1]). All of them may have access to a source of common randomness (CR) independent of the external actions. Each coordination code induces a joint distribution on the actions Q\textsubscript{X,Y,Z}.

In this paper we are interested in the joint type of a tuple of action sequences \((x, y, z)\) which is defined as

\[
    T_{x,y,z}(x, y, z) = \frac{1}{N} \sum_{i=1}^{N} 1 \{ (x_i, y_i, z_i) = (x, y, z) \} \quad (1)
\]
for all \((x, y, z) \in X \times Y \times Z\), where \(\mathbb{I}\{\cdot\}\) is the indicator function. In order to measure the distance between two probability distributions \(P_{X,Y,Z}\) and \(Q_{X,Y,Z}\) we consider their total variation, which is defined as
\[
\|P_{X,Y,Z} - Q_{X,Y,Z}\| = \frac{1}{2} \sum_{x,y,z} |P(x, y, z) - Q(x, y, z)|.
\]

We say that a triple \((R_1, R_2, P_{X,Y,Z})\) is achievable for empirical coordination if for any \(\epsilon > 0\) there exists a sequence of \((2^{NR_1}, 2^{NR_2}, N)\) coordination codes and a choice of CR such that
\[
\Pr(||P_{X,Y,Z} - T_{X,Y,Z}|| > \epsilon) < \epsilon
\]
for sufficiently large \(N\) under the distribution induced by the codes. The empirical coordination capacity region, denoted by \(C^e\), is the closure of the set of achievable triples \((R_1, R_2, P_{X,Y,Z})\).

Due to the nature of PCs we restrict our attention to binary actions \(X\) and \(Y\) (although no restriction is placed on \(Z\)) and to choices of \(P_{Y,Z|X}\) that induce uniform distributions on \(X\) and \(Z\) for the given \(P_X\). All the results in this paper are restricted to this subset of \(C^e\) that we shall refer to as the symmetrical empirical coordination capacity region and denote by \(C^e_0\). Possible generalizations are discussed in Section V.

C. Polar Codes

Channel polarization is a method for transforming \(N\) identical copies of a BI-DMC \(P_{Y|X}\) into \(N\) distinct BI-DMCs \(P_i^{(n)}(y, u^{(i)}_n|u_i)\) \((i \in \{1, \ldots, N\})\) with extremal properties in the sense that, for sufficiently large \(N\), a fraction \(I(X; Y)\) (for \(X\) uniformly distributed) of these synthetic channels is noise-free while the rest is virtually useless.

1) Channel Coding: Channel polarization leads naturally to a code construction that achieves the capacity of any symmetric BI-DMC. These codes are known as PCs and consist of two elements: an encoding matrix \(G_N\) and a Successive Cancellation (SC) decoding algorithm. \(G_N\) synthesizes the channels with extremal properties. Fixed (i.e. frozen) bits are put into the “bad” channels, which are those in the frozen set \(F\) defined as
\[
F = \{i : Z(P^{(i)}) \geq \delta_N\}
\]
for some \(\delta_N > 0\), where \(Z(P^{(i)})\) denotes the Bhattacharyya parameter (an upper bound on the error probability for uncoded transmission [4]) of the BI-DMC \(P^{(i)}\). Information is transmitted at full rate through the remaining channels, i.e. those in the complement of the frozen set \(F^c\). The SC decoding algorithm generates sequentially estimates \(\hat{u}_i\) for the information bits using the channel distribution \(P^{(i)}(y, u^{(i)}_n|u_i)\) and the previous estimates.

The following observation about PCs designed for degraded channels (as defined in [3]) will turn out to be important in the sequel.

\footnote{We restrict our attention to PCs as introduced in [4] and therefore consider vectors of \(N = 2^n\) actions (with \(n \in \mathbb{N}\)).}

Lemma 1 (Lemma 21 in [5]). Let \(P_{Y|X}\) and \(\hat{P}_{Y|X}\) be two BI-DMCs with \(\hat{P}_{Y|X}\) degraded with respect to \(P_{Y|X}\) (denoted by \(\hat{P}_{Y|X} \leq P_{Y|X}\)). Then for all \(i \in \{1, \ldots, N\}\) the synthesized channels satisfy \(\hat{P}(i) \leq P(i)\) and \(Z(P(i)) \geq Z(\hat{P}(i))\).

2) Source Coding: Korada and Urbanke showed in [5] that PCs are also optimal for lossy source compression of a DMS \(X \sim P_X\) into \(Y\). In this context the SC algorithm is used for compression while reconstruction is performed with the matrix \(G_N\). PCs for source compression are designed upon the test channel \(P_{X|Y}\) that solves the minimization defining the (symmetric) rate-distortion function. Their fundamental property is that the distribution they induce \(Q_{X,Y}\) is arbitrarily close to the \(N\)-product design distribution \(P_{X,Y} = \prod P_{Y|X} P_X\), as summarized in the following Lemma:

Lemma 2 (Lemmas 2, 5, and Theorem 16 in [5]). For any compression rate \(R > I(Y; X)\) \((Y\) uniformly distributed) we can choose \(\delta_N > 0\) such that if the frozen set \(F\) is defined as
\[
F = \{i : Z(P^{(i)}) \geq 1 - \delta_N\}
\]
then for any \(0 < \beta < \frac{1}{2}\) we have
\[
\frac{1}{2} \sum_{x,y} |P(x, y) - Q(x, y)| \leq O(2^{-N^\beta}).
\]

We will combine this result with the optimal coupling. For any two RVs \(X \sim P_X\) and \(Y \sim Q_Y\) defined on the same space their optimal coupling \(C_{PQ}(x, y)\) is a probability distribution with marginals \(P_X\) and \(Q_Y\) and that satisfies [5, 9]
\[
\Pr(X \neq Y) = \frac{1}{2} \sum_{x,y} |P_X(x) - Q_Y(y)|.
\]

III. Two-Node Network

In this Section we restrict our attention to the two-node network in Fig. 2. A \((2^{NR}, P_{Y|X})\) coordination code for this scenario consists only of an encoding and a decoding function.

\[
X \sim P_X
\]

\[
\text{Node } X \xrightarrow{R} \text{Node } Y
\]

The empirical coordination capacity region for the network in Fig. 2 is given by [1]
\[
C_P = \{(R, P_{Y|X}) : R \geq I(Y; X)\}.
\]

Theorem 1. For any pair \((R, P_{Y|X}) \in C_P\) (i.e. considering the aforementioned additional restrictions with respect to \(C_P\)) there exists a sequence of PCs that achieves empirical coordination in the two-node network in Fig. 2.

Proof: Let \(P_{Y|X}\) be the desired distribution and let
\[
P_{X|Y} = P_{X|Y} = \frac{P_{Y|X} P_X}{P_Y}
\]
where \(P_Y\) is the uniform distribution. Construct a PC for source compression upon \(P_{X|Y}\) with the frozen set defined
as in (3). For any compression rate \( R > I(Y;X) \) we know from the results on PCs for source coding in [5] that \( R > R^f \) if \( N \) is sufficiently large. Using the CR both nodes generate \( F \) i.i.d. random bits \( U_F \) according to a uniform distribution. Node \( X \) compresses its observation \( X \) using the SC encoding algorithm with frozen bits set to \( N \) or any pair of PCs achieves empirical coordination. A fixed choice of the values of these bits such that the sequence of bits using CR. The following corollary shows that there exists a sequence of PCs that achieves empirical coordination in the cascade network in Fig. 1.

**Theorem 2.** For any triple \((R_1, R_2, F_{Y|Z}|X) \in C^f_{P_X} \) (i.e. considering the aforementioned additional restrictions with respect to \( C^f_{P_X} \)) there exists a sequence of PCs that achieves empirical coordination in the cascade network in Fig. 1.

**Proof:** Let \( P_{Y|Z}|X \) be the desired distribution. Design a PC for source compression based on the distribution \( P_{Y|Z}|X \) by conditioning and marginalizing. For any compression rate \( R > I(Z;X) \) (for \( Z \) uniformly distributed) and any \( 0 < \beta < \frac{1}{2} \) we know that

\[
|P_{X,Z} - Q_{X,Z}| \leq O(2^{-N^\beta})
\]

where \( P_{X,Z} = P_{Y|Z}|X P_{X} \) and \( Q_{X,Z} \) is the distribution induced by the code. The values of the frozen bits are chosen i.i.d. according to a uniform distribution using CR so that they are also available at Nodes \( Y \) and \( Z \). The vector resulting from source compression is sent to Node \( Y \) and then forwarded to Node \( Z \). This allows both nodes to generate \( Z \). Therefore

\[
R_1 \geq R_1 + I(Z;X)
\]

\[
R_2 \geq I(Z;X)
\]

where \( R_1 \) is the fraction of \( R_1 \) which is not yet used. Clearly we need \( R_1 \) to be arbitrarily close to \( I(Y;Z|X) - I(Z;X) \). Now assume that \((X,Z) \sim P_{X,Z} \) (instead of \( Q_{X,Z} \)). Design a new PC for compression of \((X,Z)\) into \( Y \) using the conditional probability \( P_{X|Y,Z} \). Let \( Q_{Y|X,Z} \) be the distribution induced by this new PC. We know from Section III that for any compression rate \( R > I(Y;X,Z) \) (for \( Y \) uniformly distributed) and any \( 0 < \beta < \frac{1}{2} \) we can choose the frozen set \( F \) as in (3) so that for \( P_{Y|X,Z} = \prod P_{Y|X,Z} \)

\[
|P_{Y,X,Z}\|P_{X,Z} - Q_{Y,X,Z}\|P_{X,Z}| \leq O(2^{-N^\beta})
\]

Using the triangle inequality it is easy to show that (6) and (7) imply that for the true distribution on \((X,Z)\), i.e. \( Q_{X,Z} \).

\[
|P_{Y|X,Z}P_{X,Z} - Q_{Y|X,Z}\|P_{X,Z}| \leq O(2^{-N^\beta})
\]

for any \( 0 < \beta < \frac{1}{2} \). As in Section III we use this result to build the optimal coupling \( C^f_{P_Q} \) between \( P_{X,Y,Z} \) and \( Q_{Y,X,Z} \) which satisfies, for any \( 0 < \beta < \frac{1}{2} \),

\[
|P_{Y|X,Z}P_{X,Z} - Q_{Y|X,Z}\|P_{X,Z}| \leq O(2^{-N^\beta})
\]

This allows us to evaluate the probability of the event

\[
\mathcal{E}_1 \triangleq \left\{ \left| P_{X,Y,Z} - T_{X,Y,Z} \right| > \epsilon \right\}
\]

and bound it, for any \( 0 < \beta < \frac{1}{2} \), as

\[
Pr(\mathcal{E}_1) \leq Pr(\mathcal{E}_1) + Pr(\mathcal{E}_1) \leq O(2^{-N^\beta})
\]

This means that our construction will yield sequences of actions with the desired type with high probability. Now we only need to make \( Y \) available at Node \( Y \). To accomplish this at the desired rate we take advantage of the fact that \( Z \) is already available at Node \( Y \) and that it is indeed correlated with \( Y \). We model this correlation as transmitting \( Y = UG_N \) (i.e. a codeword from a PC) through the DMC \( P_{Z|Y} \) and use the SC decoding algorithm to obtain \( Y \), an estimate of \( Y \).
Int. Zurich Seminar on Communications (IZS), February 29 – March 2, 2012

Such a PC for transmission over $P_{Z|Y}$ would have a frozen set $F_V$ as defined in (2). To obtain $Y$ the decoder needs to have access to the frozen bits $U_{F_V}$. Moreover, since due to Lemma 1 we know that $F_{Q} \subseteq F_{V}$ for $\delta_{N}^{2} < \delta_{N}$ and sufficiently large $N$, only the bits in the set $F_{V} \cap F_{Q}$ need to be conveyed (see Figure 3). This can be done at any rate

$$R_{t}^{e} \geq \frac{|F_{V}| - |F_{Q}|}{N} \geq I(Y;X,Z) - I(Y;Z),$$

or equivalently $R_{t}^{e} \geq I(Y,Z;X) - I(Z;X)$, as desired.

It is easy to show that this design will also work fine when $(\hat{Y},Z) \sim \hat{Q}_{Y,Z}$ by considering the optimal coupling between $P_{Y,Z}$ and $\hat{Q}_{Y,Z}$ and the fact that, for any $0 < \beta < \frac{1}{2}$,

$$\frac{1}{2} \sum_{y,z} |P_{Y,Z}(y,z) - \hat{Q}_{Y,Z}(y,z)| \leq O(2^{-N^{\beta}}),$$

which is derived from (8) with the triangle inequality. That is,

$$\Pr(\mathcal{E}_{Y}) \triangleq \Pr(Y \neq \hat{Y}) \leq O(2^{-N^{\beta}})$$

for any $0 < \beta < \frac{1}{2}$.

Finally, we see that the probability of the event

$$\mathcal{E} = \{||P_{X,Y,Z} - T_{X,Y,Z}|| > \varepsilon\},$$

when evaluated over the distribution induced by the code

$$Q_{X,Y,Z} = P_{X}\hat{Q}_{Z,X}\hat{Q}_{Y,X,Z}\hat{Q}_{Y,Y},$$

where $Q_{Y,Y}$ accounts for the possible errors in reproducing $\hat{Y}$ at Node Y, is arbitrarily low. That is, for any $0 < \beta < \frac{1}{2}$

$$\Pr(\mathcal{E}) \leq \Pr(\mathcal{E}_{Y}) + \Pr(\mathcal{E} \backslash \mathcal{E}_{Y})$$

$$= \Pr(\mathcal{E}_{Y}) + \Pr(\mathcal{E}_{1}) \leq O(2^{-N^{\beta}}).$$

Hence the sequence of PC achieves empirical coordination.

As for the two-node network, there exists a choice of the values of the frozen bits such that the sequence of PCs achieves empirical coordination.

**Corollary 2.** For any triple $(R_{1}, R_{2}, P_{Y,Z|X}) \in \mathcal{C}_{P_{X}}$ there exists a sequence of PCs and a choice of frozen bits that achieves empirical coordination in the network in Fig. 1.

**Proof:** The proof is similar to that of Corollary 1.

**V. DISCUSSION**

The previous sections show that PCs are suitable for empirical coordination. However, a few questions remain open. First of all, our discussion has been restricted to the symmetrical empirical coordination capacity region, a portion of the region $\mathcal{C}_{P_{X}}$. Preliminary results show that the usual techniques for extending the applicability of PCs (see [4]–[7]) may also be useful here to make more general statements as one would expect from [1, Section VII]. Moreover, we have only considered empirical coordination. No practical codes for strong coordination have been designed so far. The problem gets more involved due to the need for exploiting common randomness.

**ACKNOWLEDGMENT**

The authors would like to thank one anonymous reviewer for helpful comments.

**APPENDIX**

**Proof of Corollary 1:** Since the total variation is a bounded measure, Theorem 1 implies that there is a sequence of coordination codes such that

$$\lim_{N \to \infty} \mathbb{E}_{X,Y}(||T_{X,Y} - P_{X,Y}||) = 0.$$

The expectation, which is taken with respect to the induced distribution, can be written as

$$\mathbb{E}_{X,Y}(||T_{X,Y} - P_{X,Y}||) = \mathbb{E}_{X,U}(||T_{X,U} - P_{X,U}||)$$

$$= \sum_{x,u} Q(x,u)||T_{x,u} - P_{x,u}||$$

$$= \sum_{x,u} Q(u_{F}) \sum_{x,u_{F}} Q(x,u_{F})||T_{x,u} - P_{x,u}||$$

$$= \mathbb{E}_{u_{F}} \mathbb{E}_{x,u_{F}}(||T_{x,u_{F},u_{F}} - P_{x,y}||).$$

In (9) and (10) we have used the fact that $G_{N}$ is a one-to-one mapping to modify slightly the definitions of $Q_{X,Y}$ and of the type function to depend on $u$ by setting $y = uG_{N}$. The notation $T_{x,u_{F},u_{F}} = T_{x,u}$ in (11) simply makes explicit the fact that $u = (u_{F},u_{F})$. For the outer expectation in (11) to go to zero with the block length there must be a choice of the values of the frozen bits $u_{F}$ such that

$$\mathbb{E}_{x,u_{F}}(||T_{x,u_{F}} - P_{x,y}||) \leq \mathbb{E}_{x,u}(||T_{x,u} - P_{x,y}||).$$

Moreover, since convergence in the first mean implies convergence in probability, we conclude that there exists a sequence of PCs for coordination and a choice of the frozen bits that achieves empirical coordination.

**REFERENCES**


Polar Codes for Degraded Relay Channels

Mohammad Karzand
Ecole Polytechnique Fédérale de Lausanne
CH-1015 Lausanne, Switzerland
mohammad.karzand@epfl.ch

Abstract—Polar coding is a recent channel coding technique invented by Arıkan to achieve the ‘symmetric capacity’ of binary-input memoryless channels. Subsequently it was observed that such codes are also good for lossy channel coding, general memoryless channels without feedback and several multiterminal settings. In this paper, we apply polar codes to achieve the capacity of binary input symmetric degraded relay channels. The main novelty is to show how polar codes can implement block Markov coding in this degraded setting, and consequently yielding a low complexity method to achieve “decode-and-forward” rates.

I. INTRODUCTION

The relay channel was introduced by van der Meulen, and has been studied for forty years in the community. Some of the well-known capacity theorems for different classes of relay channels is proved by El Gamal and Cover in [1]. In this note, we are going to construct a polar coding scheme to achieve the rate given by [1] for binary stochastically-degraded relay channels. Note that this bound coincides with the upper bound of [4] where the receiver observes the multiple access nature of relay channel at its receiver is removed. The nested polar code structure of [4] makes crucial use of this orthogonality and the code is not extensible to the general relay channel [1]. Here, we do not assume the orthogonality of the channels, and thus need a new technique to be able to use polar codes.

Channel polarization technique was introduced in [2] to construct capacity achieving codes for discrete memoryless channels. The encoding and decoding of polar codes with blocklength $n$ take $O(n \log(n))$ arithmetic operations. It is shown in [5] and [3] that the block error probability of these codes decays roughly like $2^{-\sqrt{n}}$ asymptotically in $n$.

Channel polarization technique was considered for orthogonal relay channels in [4] where the receiver observes the relay’s and transmitter’s signals separately via independent channels. By the orthogonality assumption on the receiver side, the multiple access nature of relay channel at its receiver is removed. The nested polar code structure of [4] makes crucial use of this orthogonality and the code is not extensible to the general relay channel [1]. Here, we do not assume the orthogonality of the channels, and thus need a new technique to be able to use polar codes.

We face two important challenges in order to implement a low complexity scheme for the relay channel using polar codes. One is that the outputs of the relay and the transmitter should be correlated with each other, which is not trivial to achieve using polar codes. The second one is to avoid implementing a list decoder with a list size increasing exponentially with blocklength. After a brief review on the relay channel problem and polar coding, in section III, we state the main theorem with the proof, and provide the solutions for these challenges. In the last section we discuss the results.

II. REVIEW

A discrete memoryless relay channel consists of four finite sets $\mathcal{X}, \mathcal{X}', \mathcal{Y}, \mathcal{Y}'$ and a collection of conditional probability mass functions $\Pr(y, y|x, \bar{x})$ on $\mathcal{Y} \times \mathcal{Y}'$. A $(M, n)$ code consists of an encoder that assigns a codeword $x^n(w)$ to each message $w \in \{1, \ldots, M\}$, a relay that assigns at time $i \in \{1, \ldots, n\}$ a symbol $\bar{x}_i(y_{i-1}^i)$ to each received sequence $y_i^{i-1}$, and a decoder that assigns a message $\hat{w}$ to each received sequence $y_n^n$. The channel is memoryless in the sense that the current received symbols and the past symbols are conditionally independent given the current transmitted symbols.

The average probability of error is $P_e = \Pr(W \neq \hat{W})$ with message $W$ chosen uniformly at random. The rate $R = \frac{\log M}{n}$ is achievable if there exists a sequence of $(2^{nR}, n)$ codes with vanishing average probability of error. The capacity $C$ is the supremum of all achievable rates.

The relay channel is physically degraded if $\Pr(y|x, \bar{x})$ can be written in the form

$$\Pr(y|x, \bar{x}) = \Pr(\tilde{y}|\bar{x}, x) \Pr(y|\tilde{y}, \tilde{x}).$$

Furthermore, it is stochastically degraded if there exists a set of conditional distributions $q(y|x, \bar{x})$ such that

$$\Pr(y|x, \bar{x}) = \sum_{\tilde{y}} \Pr(\tilde{y}|\bar{x}, x) q(y|\tilde{y}, \tilde{x}).$$

Theorem 1 ([1]). The capacity of a physically degraded relay channel is given by

$$C = \sup_{I\{X; \tilde{X} \}} \min \{I(X; \tilde{X}, Y), I(X; \tilde{Y} \bar{X})\}$$

Pr(\tilde{x})Pr(x|\tilde{x})

II. REVIEW

A discrete memoryless relay channel consists of four finite sets $\mathcal{X}, \mathcal{X}', \mathcal{Y}, \mathcal{Y}'$ and a collection of conditional probability mass functions $\Pr(y, y|x, \bar{x})$ on $\mathcal{Y} \times \mathcal{Y}'$. A $(M, n)$ code consists of an encoder that assigns a codeword $x^n(w)$ to each message $w \in \{1, \ldots, M\}$, a relay that assigns at time $i \in \{1, \ldots, n\}$ a symbol $\bar{x}_i(y_{i-1}^i)$ to each received sequence $y_i^{i-1}$, and a decoder that assigns a message $\hat{w}$ to each received sequence $y_n^n$. The channel is memoryless in the sense that the current received symbols and the past symbols are conditionally independent given the current transmitted symbols.

The average probability of error is $P_e = \Pr(W \neq \hat{W})$ with message $W$ chosen uniformly at random. The rate $R = \frac{\log M}{n}$ is achievable if there exists a sequence of $(2^{nR}, n)$ codes with vanishing average probability of error. The capacity $C$ is the supremum of all achievable rates.

The relay channel is physically degraded if $\Pr(y|x, \bar{x})$ can be written in the form

$$\Pr(y|x, \bar{x}) = \Pr(\tilde{y}|\bar{x}, x) \Pr(y|\tilde{y}, \tilde{x}).$$

Furthermore, it is stochastically degraded if there exists a set of conditional distributions $q(y|x, \bar{x})$ such that

$$\Pr(y|x, \bar{x}) = \sum_{\tilde{y}} \Pr(\tilde{y}|\bar{x}, x) q(y|\tilde{y}, \tilde{x}),$$

Theorem 1 ([1]). The capacity of a physically degraded relay channel is given by

$$C = \sup_{I\{X; \tilde{X} \}} \min \{I(X; \tilde{X}, Y), I(X; \tilde{Y} \bar{X})\}$$

where the supremum is over all joint distributions $Pr(x, \tilde{x})$ on $\mathcal{X} \times \mathcal{X}$. Furthermore, this rate gives a lower bound on the capacity of a stochastically degraded relay channel.

Proof: We present an overview of the achievability here, so we will identify the requirements on decoder that can perform well on this channel.

Consider $B$ blocks of transmission, each of $n$ symbols. A sequence of $B-1$ indices $w^{(i)} \in \{1, \ldots, 2^{nR}\}$ will be transmitted over the channels in $nB$ transmissions. We partition the set $\{1, \ldots, 2^{nR}\}$ through a appropriate hash function $s^{(i)} = \text{hash}(w^{(i-1)})$, $s^{(i)} \in \{1, \ldots, 2^{nR_0}\}$.

A doubly indexed set of codewords is generated using random coding as follows. We fix $Pr(\tilde{x}) Pr(x|\tilde{x})$, and generate $2^{nR_0}$ i.i.d. $n$-sequences in $\mathcal{X}^n$, each drawn according to $Pr(\tilde{x})$, and for each of them generate $2^{nR}$ i.i.d. $n$-sequences, each drawn independently according to $Pr(x|\tilde{x})$. 

59
Let \( w^{(i)} \) be the new index to be sent in block \( i \) and \( s^{(i)} \) be defined as the partition corresponding to \( w^{(i-1)} \). The transmitter sends \( x(w^{(i)}, s^{(i)}) \). The relay has an estimate of \( w^{(i-1)} \) and it sends \( \tilde{x}(s^{(i)}) \) in block \( i \).

Decoding is accomplished in three steps:
1. Given \( s^{(i)} \) and upon receiving \( \tilde{g}^{(i)} \), the relay estimates the transmitted message \( w^{(i)} \). This will succeed with low probability of error if \( R < I(X; Y|X) \) and \( n \) is sufficiently large.
2. The receiver estimates \( s^{(i)} \) using a jointly typical decoder for the pair \( (\tilde{x}(s^{(i)}), y^{(i)}) \). This can be done with arbitrarily small probability of error if \( R_0 < I(X; Y) \).
3. Assuming \( s^{(i)} \) is decoded correctly at the receiver, the receiver looks for a unique \( u^{(i-1)} \) among the \( 2^{n(R-R_0)} \) indices that satisfies \( \text{hash}(u^{(i-1)}) = s^{(i-1)} \) and is jointly typical with \( y^{(i-1)} \). This can be done if \( n \) is sufficiently large and if \( R < I(X; Y|X) + R_0 \).

In this paper we aim to introduce the code so that all three decoding steps can be done using the polar decoder and thus with low complexity. Before we proceed to present our results, let us give a brief overview of polar codes.

We briefly recall how polarization is done for the \( q \)-ary input channels when \( q \) is a prime number.

The basic idea behind the polarization technique is to take two independent uses of the same channel, and by pre-processing their inputs construct two unequal channels with different mutual informations such that the sum of mutual information remains unchanged. The polarization construction is obtained by repeating this operation \( l \) times to obtain from \( N = 2^l \) independent uses of the channel \( W \) the \( N \) synthesized channels. The synthesized channels are denoted by \( I(W^s), s \in \{+, -\}^l \). Polarization means that as \( l \) gets large, almost all the channels at level \( l \) are either almost perfect or almost pure noise. As discussed earlier, the transformation preserves mutual information; putting these two facts together, one concludes that the fraction of almost perfect channels is equal to the symmetric channel capacity.

In order to construct a polar code \( C_{\alpha}(F, u_F) \) of blocklength \( n = 2^l \) based on this, one finds \( F^c = \{ s \in \{+, -\}^l : I(W^s) > 1 - \delta \} \) for some sufficiently small \( \delta > 0 \) and sends information through these ‘good’ channels. For the other channels indexed by \( F = \{+, -\}^l \setminus F^c \), the decoder and encoder, prior to the communication, agree on a sequence \( u_F \) that will be sent over these channels; these values are said to be ‘frozen’.

The relation between \( U \) and \( X \) as follows:

\[ X = U H_1, \]

where \( H_1 \) is the \( l \)-fold Kronecker product of the matrix \[ \begin{bmatrix} 1 & 0 \end{bmatrix} \].

The encoder represents the message as \( u_F \), and concatenates it with a randomly selected \( u_F \) to form the vector \( u \). \( u_F \) is revealed to the decoder.

**Theorem 2** ([2],[5]), Given a \( q \)-ary discrete channel, with \( q \) prime, and a fixed rate \( R < I(W) \), where \( I(W) \) is the symmetric channel capacity of the channel, there exists a sequence of polar codes \( C_{\alpha}(F, u_F) \) of rate \( R_0 > R \) with low encoding and decoding complexity, and with vanishing error probability.

In the next section, this theorem provides the essential tools to perform the first two decoding steps successfully in the achievability proof of the degraded relay channel. However, we still need another result from the polar coding literature to guarantee the success of the third step.

We say \( W_b(y_2|x) \) is a stochastically degraded version of \( W_g(y_1|x) \) if there exists a distribution \( q(y_2|y_1) \) such that

\[ W_b(y_2|x) = \sum W_g(y_1|x) q(y_2|y_1). \]

Consider further, two polar constructions and \( C_{\alpha}(F_b, u_{F_b}) \) and \( C_{\alpha}(F_g, u_{F_g}) \) for \( W_b(y_2|x) \) and \( W_g(y_1|x) \). The following lemma is proven in [6]:

**Lemma 1.** [6] If \( W_b(y_2|x) \) is a degraded version of \( W_g(y_1|x) \), then for a given \( \delta \) the frozen set for the good channel \( F_g \) is a subset of the frozen set for the bad channel \( F_b \).

Thus, all good channels for \( W_b \) are also good channels for \( W_g \). Comparing the two polar constructions and considering Lemma 1, we label the channels in three groups. \( I(W_b) \) fraction of all channels consists of channels which are noiseless for both \( W_b \) and \( W_g \), \( I(W_g) - I(W_b) \) fraction of channels consist of those channels which are noiseless for \( W_b \) but completely noisy for \( W_g \). The remaining \( 1 - I(W_g) \) fraction of channels are completely noisy for both \( W_b \) and \( W_g \). Suppose one uses polar codes to multicast common information with the rate \( I(W_b) \) over both these channels. Knowing the frozen bits, the decoder for the channel \( W_b \) is able to decode everything, but the decoder for the channel \( W_g \) cannot decode anything because the transmission rate is above its capacity. At this point a list decoder for the channel \( W_b \) is able to pin down the transmitted codeword to a list of codewords of size \( q^{n(I(W_b) - I(W_g))} \). Suppose a genie reveals the value of the information bits in the second group of channels to the decoder at \( W_b \) in each block, which results in decreasing the rate of the code to \( I(W_b) \). Now, the decoder is able to decode the remaining bits using the polar decoder for \( W_g \).

We will see in the following that the concept of coding for the degraded relay channel regarding the transmission from relay to receiver consists in sending only the values corresponding to the intersection of the two frozen sets in order to support the decoding at the receiver side of the codeword that is sent by the transmitter over the degraded channel.

### III. Polar Codes for the Degraded Relay Channel

In what follows, we consider \( |X| = |\tilde{X}| = 2 \). We consider the marginal probability distribution of \( x \) and \( \tilde{x} \) to be uniform and \( Pr(x \neq \tilde{x}) = \alpha \), \( 0 \leq \alpha \leq 1 \). We define the symmetric rate of the stochastically degraded relay channel to be \( R_{\alpha} = \min \{ I(X, \tilde{X}; Y), I(X; Y|X) \} \).

**Theorem 3** (Polar codes achieve \( \sup_{\alpha} R_{\alpha} \) of degraded relay channels), Given a binary-input stochastically degraded relay channel \( Pr(y, y_1|x, x_1) \), \( 0 \leq \alpha \leq 1 \) and \( R < R_{\alpha} \), there exists
a sequence of codes based on the polar encoder and decoder with low encoding and decoding complexity of rate $R_N > R$ with vanishing error probability.

**Proof:** Since $\alpha \rightarrow R_N$, it suffices to consider $\alpha$ of the form $\alpha = \frac{k}{n}$ where $k \in \mathbb{N}$ and $q$ is prime.

As in [1], we consider $\beta B$ blocks of transmission, each consisting of $n$ symbols. A sequence of $B - 1$ indices will be transmitted over the channel in $nB$ transmissions. We fix $R = \frac{\log M}{n}$ and $R_0$ as design parameter.

Let $w(i) \in \{1, \ldots, M\}$ be the new index to be sent in block $i$, and let $s(i)$ be an integer in the set $\{1, \ldots, 2^{nR_0}\}$ and be a hash of $w(i-1)$. We will define this hash function further into the proof. Note that $W(i)$ and $S(i)$ are independent. We assume that at the end of block $i - 1$ the receiver knows $(w(1), w(2), \ldots, w(i-2))$ and $(s(1), s(2), \ldots, s(i-2))$ and the relay knows $(w(1), w(2), \ldots, w(i-1))$ and $(s(1), s(2), \ldots, s(i))$.

As the proof of Theorem 1 suggests, the following three tasks should be completed at the end of block $i$.

- Both the relay and the transmitter have access to $s(i)$, so they should both cooperatively transmit $s(i)$ successfully to the receiver.
- The transmitter should transmit $w(i)$ successfully to the relay.
- The receiver should decode $w(i-1)$ knowing $y(i-1)$, $s(i-1)$ (that has been obtained in the previous block) and $s(i)$.

An overview of the system can be found in the next column and as we go through our proof we explain each part of it.

We suggest using the following scheme. Suppose $\bar{x} = uH_n$ and $x = j + \bar{x}$. For now, to satisfy the condition on the probability distribution, we only assume that $U$ is an $n$-tuple vector which is derived from $S(i)$ and has independent uniformly distributed components, $j$ is an $n$-tuple vector which is a function of $w(i)$ and has independent and identical components distributed as Bernoulli with parameter $\alpha$, and $H_n$ is the $n$-fold Kronecker product of the matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Observe that the channel between $\bar{X}$ and $Y$ is governed by the following conditional probability distribution:

$$
\Pr(y|\bar{x}) = \sum_j \Pr(y|x, j) \Pr(j)
= \prod_{i=1}^{n} \sum_{j_i} \Pr(y_i|x_i, j_i + \bar{x}_i) \Pr(j_i)
= \prod_{i=1}^{n} \sum_{j_i} \left( \sum_{\bar{x}_i \in \{0, 1\}} \Pr(y_i, \bar{y}_i|x_i, j_i + \bar{x}_i) \right) \Pr(j_i),
$$

so that the channel is memoryless. Therefore, we consider $\bar{X}$ to be a codeword of a binary polar code $C_n(F; U_F)$ designed for the channel

$$
\Pr(y|\bar{x}) = \sum_j \left( \sum_{\bar{y}} \Pr(y, \bar{y}|\bar{x}, j + \bar{x}) \right) \Pr(j).
$$

Choosing $U_F$ uniformly at random makes $\bar{X}$, the codeword of a binary polar code, have a uniform distribution, and hence $\bar{X}$ satisfies the constraint on its distribution. By Theorem 2, we know that a sequence of codes with rate $R_0 > R_0$ exists for

$$
R_0 < I(\bar{X}; Y) \quad (1)
$$

with vanishing error probability as the length increases. With this, our scheme succeeds in performing the first task in the achievability scheme.

Similarly, observe that there exists an equivalent channel between $J$ and $\bar{Y}$ which is also memoryless. If we follow the steps of the previous part, we will not be able to construct a codeword which satisfies the condition on the probability

Fig. 1. Schematic diagram of transmitter

Fig. 2. Schematic diagram of relay

Fig. 3. Schematic diagram of receiver

61
distribution of $J$. In this case, we need to proceed as follows.

Recall $\alpha = \frac{1}{2}$. Consider the operator $\mathcal{L}(x_q): \{0, \cdots, q - 1\} \rightarrow \{0, 1\}$ as follows

$$
\mathcal{L}(x_q) = \begin{cases} 
1 & \text{if } x_q < k, \\
0 & \text{if } x_q \geq k.
\end{cases}
$$

Observe that if $x_q$ is uniformly distributed on the set $\{0, \cdots, q - 1\}$, then $\mathcal{L}(x)$ has a Bernoulli distribution with parameter $\alpha$. This trick is mentioned in [7]. This enables us to provide arbitrary correlation between the output of the relay and the transmitter.

Now, we consider $J = \mathcal{L}(X_q)$, where $X_q = VH_n$ is a codeword of a $q$-ary polar code $C_n(\hat{G}, V_{\hat{G}})$ designed to encode $w^{(i)}$ for the auxiliary channel governed by the following transition probability:

$$
Pr(y, \hat{X}|X_q) = Pr(\hat{Y}|\mathcal{L}(X_q), \hat{X}) Pr(\hat{X}) = Pr(\hat{X}),
$$

$$
\prod_{i=1}^{n} Pr(\hat{y}_i|\hat{x}_i, \mathcal{L}(x_{q_i}) + \hat{x}_i).
$$

Observe that $J$ has Bernoulli distribution with parameter $\alpha$. We can transmit the message to the relay by using a polar encoder to encode $w^{(i)}$ to $J$. As the relay has access to $\hat{Y}$ and $\hat{X}$ such a power encoder exits for rates up to $I(J; \hat{Y}|\hat{X}) = I(J; \hat{Y}, \hat{X})$. By Theorem 2, we know a sequence of codes with rate $R_N > R$ exists for

$$
R < I(X_q; \hat{Y}, \hat{X}) = I(X; \hat{Y}|\hat{X})
$$

with vanishing error probability as the length increases.

This scheme succeeds in performing the second task in the achievability scheme. Note that it is easy to extend the ordinary polar decoder with the same complexity to this case by using $(\hat{Y}, \hat{X})$ as a super alphabet as the output.

Now the only remaining task is to decode $w^{(i-1)}$ at the receiver by using $y^{(i-1)}$, $s^{(i)}$, and $s^{(i-1)}$. Up to now, we have not chosen the hash function relating $s^{(i)}$ and $w^{(i-1)}$. Now, we should choose the relation between $s^{(i)}$ and $w^{(i-1)}$ so that we help the receiver to decode $w^{(i-1)}$. Consider the two channels

$$
X_q^{(i-1)} \rightarrow (\hat{Y}^{(i-1)}, \hat{X}^{(i-1)})
$$

and

$$
X_q^{(i-1)} \rightarrow (y^{(i-1)}, x^{(i-1)})
$$

Note that the second of these is a degraded version of the first one. Further, consider the polar code $C_n(\hat{G}, V_{\hat{G}})$ used to transmit $w^{(i-1)}$ to the relay. According to Lemma 1 and the discussion that follows, we need to reveal at least $n[I(X_q; Y, \hat{X}) - I(X_q; \hat{Y}, \hat{X})] = n[I(X_q; Y, \hat{X}) - I(X_q; \hat{Y}|\hat{X})]$ bits to the receiver to ensure a successful decoding of $w^{(i-1)}$ at the receiver. We will use $s^{(i)}$ to reveal these values to the receiver. Observe that $s^{(i)}$ should be the value of those positions that are not in the frozen set $\hat{G}$ but should be considered frozen and revealed to the decoder for the channel $X_q^{(i-1)} \rightarrow (y^{(i-1)}, x^{(i-1)})$ because of a lower symmetric channel capacity. We denote the frozen set of the polar code designed for the channel $X_q^{(i-1)} \rightarrow (y^{(i-1)}, x^{(i-1)})$ to be $G$. The figure below shows the relationship between $W^{(i)}$, $V^{(i)}$, $U^{(i+1)}$, and $S^{(i+1)}$.

By Lemma 1, we know that $\hat{G} \subset G$. We need to transmit $|G| - |\hat{G}|$ $q$-ary digits to the receiver through $nR_0$ bits (i.e., $s^{(i)}$) to the receiver, so we should have

$$
R_0 > I(X_q; \hat{Y}|\hat{X}) - I(X_q; Y|\hat{X}).
$$

Putting (1), (2) and (3) together, we have the following conditions on the successful transmission of $w^{(i-1)}$ to the receiver at the end of time $i$:

$$
R < I(X_q; \hat{Y}|\hat{X})
$$

$$
R < I(X, \hat{X}; Y).
$$

By theorem (2), this implies that there exist specific values of the frozen bits so that all error probabilities are small for all decoders.

**IV. Conclusion**

The main novelty is to adapt polar codes to implement the block Markov scheme of [1] and to show that in the degraded case the polar decoder will succeed with low complexity.

**Acknowledgment**

The author wishes to thank Prof. Emre Telatar for fruitful discussions and helpful comments on the paper.

**References**


Unambiguous Decoding of Generalized Reed–Solomon Codes Beyond Half the Minimum Distance

Alexander Zeh¹,², Antonia Wachter¹,³, and Martin Bossert¹

¹ Institute of Telecommunications and Applied Information Theory, Ulm University, Ulm, Germany
² École Polytechnique, Paris, France
³ Inst. de recherche math. de Rennes (IRMAR), Université de Rennes 1, Rennes, France

{alexander.zeh, antonia.wachter, martin.bossert}@uni-ulm.de

Abstract—The Schmidt–Sidorenko–Bossert scheme extends a low-rate Reed–Solomon code to an Interleaved Reed–Solomon code and achieves the decoding radius of Sudan’s original list decoding algorithm while the decoding result remains unambiguous. We adapt this result to the case of Generalized Reed–Solomon codes and calculate the parameters of the corresponding Interleaved Generalized Reed–Solomon code. Furthermore, the failure probability is derived.

I. INTRODUCTION

Two approaches to decode an Reed–Solomon (RS) code of length \( n \) and dimension \( k \) beyond half the minimum distance \( \frac{n-k}{2} \) with polynomial time and space complexity exist. The first one — formulated by Guruswami and Sudan (GS, [1], [2]) — considers the decoding problem of an RS code as interpolation problem and returns a list of all possible candidates within the increased decoding radius. The second one — invented by Schmidt, Sidorenko and Bossert (SSB, [3]) — extends an RS code virtually to an Interleaved RS code [4]–[8] and achieves the same decoding radius as Sudan’s original approach, where a multiplicity one [1] for the interpolation is used. The decoding result is unambiguous and therefore it is interesting to investigate its failure probability. For further parallels between these two schemes see [9], [10].

While the GS approach was formulated for Generalized RS (GRS) codes, the SSB adaption for GRS codes is still missing. We fill the lack in this contribution by giving an explicit expression for the virtually generated Interleaved Generalized RS (IGRS) code. Furthermore, we bound the failure probability for this unique decoding approach.

Our contribution is organized as follows. In Section II, Interleaved Generalized Reed–Solomon (IGRS) codes are defined and basic properties are discussed. The joint decoding of IGRS codes is explained in Section III. The parameters and the technique of a virtual extension of an low-rate GRS to an IGRS codes is explained in Section IV. The failure probability for this particular IGRS case is derived in Section V. Section VI concludes our contribution.

II. INTERLEAVED GENERALIZED REED–SOLomon CODES

Let \( \mathcal{L} = \{\alpha_1, \alpha_2, \ldots, \alpha_n\} \) denote a set containing \( n \) non-zero distinct elements (code locators) of the finite field \( \mathbb{F} = \text{GF}(q) \) of cardinality \( n < q \). Let \( V' = \{\nu'_1, \nu'_2, \ldots, \nu'_n\} \) be a set of non-zero elements of \( \mathbb{F} \). Denote

\[
\nu'(V', \mathcal{L}) = (\nu'_1 f(\alpha_1), \nu'_2 f(\alpha_2), \ldots, \nu'_n f(\alpha_n))
\]

for a given polynomial \( f(x) \) over \( \mathbb{F} \).

An GRS code \( \mathbb{G}RS(V'; n, k) \) of length \( n \) and dimension \( k \) over \( \mathbb{F} \) with \( n < q \) is given by

\[
\mathbb{G}RS(V'; n, k) = \{c = \nu'(V', \mathcal{L}) : f(x) \in \mathbb{F}_k[x]\},
\]

where \( \mathbb{F}_k[x] \) denotes the set of all univariate polynomials with degree less than \( k \) and indeterminate \( x \). The generator matrix \( \mathbb{G} \) of the GRS code is:

\[
\mathbb{G} = \begin{pmatrix}
1 & 1 & \cdots & 1 \\
\alpha_1 & \alpha_2 & \cdots & \alpha_n \\
\vdots & \vdots & \ddots & \vdots \\
\alpha_1^{n-1} & \alpha_2^{n-2} & \cdots & \alpha_n^{n-1}
\end{pmatrix}
\begin{pmatrix}
\nu'_1 \\
\nu'_2 \\
\vdots \\
\nu'_n
\end{pmatrix},
\]

and the parity check matrix \( \mathbb{H} \) is given by:

\[
\mathbb{H} = \begin{pmatrix}
1 & 1 & \cdots & 1 \\
\alpha_1 & \alpha_2 & \cdots & \alpha_n \\
\vdots & \vdots & \ddots & \vdots \\
\alpha_1^{n-k-1} & \alpha_2^{n-k-2} & \cdots & \alpha_n^{n-k-1}
\end{pmatrix}
\begin{pmatrix}
\nu_1 \\
\nu_2 \\
\vdots \\
\nu_n
\end{pmatrix}.
\]

Since \( \mathbb{G}^{\mathbb{T}} = 0 \), we obtain an explicit relation for the column multipliers [11]:

\[
\sum_{j=1}^{n} \nu_j \nu'_j \alpha^\ell = 0, \quad 0 \leq \ell \leq n - 2.
\]

GRS codes are maximum distance separable (MDS), i.e., their minimum Hamming distance is \( d = n - k + 1 \). Analog to interleaved RS (IRS) codes, we introduce interleaved generalized RS codes as follows.
Definition 1 (Interleaved GRS (IGRS) Code) \(\text{Let the set } \mathcal{K} = \{k_1, k_2, \ldots, k_s\},\) consist of \(s\) integers, where all \(k_i < n\). Let \(\mathcal{M} = (Y_1', Y_2', \ldots, Y_r')\), be a tuple of \(n\) non-zero elements in \(\mathbb{F}\). An Interleaved Generalized Reed–Solomon code \(\mathcal{IGRS}(n, \mathcal{K}, \mathcal{M}, s)\) of interleaving order \(s\) is given by

\[
\mathcal{IGRS}(n, \mathcal{K}, \mathcal{M}, s) = \left\{ \begin{array}{c}
\{ e^{(1)}, e^{(2)}, \ldots, e^{(s)} \}
\end{array} \right\}
\]

where each submatrix \(e^{(i)}\) is a \((n - k_i - t) \times t\) matrix and each \(T^{(i)}\) is a column vector of length \(n - k_i - t\):

\[
S^{(i)} = \begin{pmatrix}
S^{(i)}_{1,1} & S^{(i)}_{1,2} & \cdots & S^{(i)}_{1,t} \\
S^{(i)}_{2,1} & S^{(i)}_{2,2} & \cdots & S^{(i)}_{2,t} \\
\vdots & \vdots & \ddots & \vdots \\
S^{(i)}_{n-k_i,1} & S^{(i)}_{n-k_i,2} & \cdots & S^{(i)}_{n-k_i,t}
\end{pmatrix},
\]

\[
T^{(i)} = \begin{pmatrix}
-S^{(i)}_{1,1} \\
-S^{(i)}_{2,1} \\
\vdots \\
-S^{(i)}_{n-k_i,1}
\end{pmatrix}.
\]

To obtain a unique solution of (5), the number of equations has to be greater than or equal to the number of unknowns. By counting both, we obtain the joint error–correcting capability of a heterogeneous \(\mathcal{IGRS}(n, \mathcal{K}, \mathcal{M}, s)\) code [7]:

\[
\tau_{\text{IRS}} = \left\lfloor \frac{s - 1}{s} \left( n - \sum_{i=1}^{s} k_i \right) \right\rfloor.
\]

An efficient solution of the system of equations (5) can be obtained by multi-sequence shift-register synthesis as proposed in [3], [12].

IV. VIRTUAL EXTENSION TO AN IGRS CODE

We extend the Schmidt–Sidorenko–Bossert scheme [3] to the case of Interleaved Generalized Reed–Solomon codes (see Definition 1) and give the corresponding parameters.

A low-rate GRS code can be virtually extended to an IGRS code. This IGRS code is denoted by \(\mathcal{VIRS}(V^r'; n, k, s)\), where \(n, k\) and \(V^r\) are the original parameters of the \(\mathcal{GRS}(V^r'; n, k)\) code. The parameter \(s\) denotes the order of (virtual) interleaving. Let the vector \(c = (c_1, c_2, \ldots, c_n)\) and let \(c^{(i)}\) denote the vector, where each coefficient is raised to the power \(i\), i.e., \(c^{(i)} = (c_1^i, c_2^i, \ldots, c_n^i)\). The virtual IGRS code is defined as follows.

Definition 2 (Virtual Extension to an IGRS code) \(\text{Let } \mathcal{GRS}(V^r'; n, k)\) be an GRS code with the evaluation polynomials \(f(x)\) as defined in (2). The virtually extended Interleaved Generalized Reed–Solomon code \(\mathcal{VIRS}(V^r'; n, k, s)\) of extension order \(s\) is given by

\[
\mathcal{VIRS}(V^r'; n, k, s) = \left\{ \begin{array}{c}
\{ e^{(1)}, e^{(2)}, \ldots, e^{(s)} \}
\end{array} \right\}
\]

where each submatrix \(e^{(i)}\) is a \((n - k_i - t) \times t\) matrix and each \(T^{(i)}\) is a column vector of length \(n - k_i - t\):
GRS codes (see [3]). We obtain a heterogeneous Interleaved Generalized Reed–Solomon code of order $s$, where $s$ is chosen s.t. $s(k - 1) < n$ and the decoding radius is maximized. The parameters of the IGRS code are:

$$k_i = i(k - 1) + 1,$$

$$\nu_j^{(i)} = (\nu_j)^i,$$

for $i = 1, \ldots, s$ and $j = 1, \ldots, n$. The following theorem shows the relation between the column multipliers $\nu_j^{(i)}$ and $\nu_j$ of the virtually created GRS code.

**Theorem 1 (Column Multipliers for VIRS Code)** Let an $\mathcal{GRS}(V; n, k)$ code with evaluation polynomial $f(x)$ as defined in (2) be given and let $\nu_j$, $j = 1, \ldots, n$, be given, such that (3) holds.

Furthermore, let the virtually extended Interleaved Generalized Reed–Solomon code $\mathcal{VIRS}(V; n, k, s)$ for a given parameter $s$ with $k_i$ and $\nu_j^{(i)}$ be given as in (9). Then, the corresponding column multipliers of the $i$th subcode $\{f^{(i)}(L, V_j^{(i)})\}$ are given by

$$\nu_j^{(i)} = (\nu_j)/\nu_j^{(i-1)},$$

(10)

**Proof:** With (3) we have for the $i$th subcode $\{f^{(i)}(L, V_j^{(i)})\}$:

$$\sum_{j=1}^n \nu_j^{(i)}(\nu_j)^{\alpha_j^i} = \sum_{j=1}^n (\nu_j)^{(\nu_j^{(i-1)}-1)}(\nu_j)^{\alpha_j^i} = \sum_{j=1}^n \nu_j\nu_j^{(i-1)} = 0, \quad 0 \leq \ell \leq n - 2.$$

The decoding radius of a $\mathcal{VIRS}(V; n, k, s)$ code is the same as in [3]:

$$\tau_{\mathcal{VIRS}} = \left[\frac{s}{s+1}\left(n - \left(\frac{s+1}{2}(k - 1) + 1\right)\right)\right],$$

(11)

where we choose $s$, such that $\tau_{\mathcal{VIRS}}$ is maximized. Note that this decoding radius results from (8) using an IGRS code with mean dimension

$$\bar{k} = \frac{1}{s} \sum_{i=1}^s k_i = \frac{1}{s} \sum_{i=1}^s (i(k - 1) + 1) = \frac{(k - 1)(s + 1)}{2} + 1.$$ 

Decoding can be done as for IGRS codes by solving (5) with multi-sequence shift-register synthesis.

**V. Failure Probability**

Since the virtual extension searches a unique solution for the error locator polynomial, a decoding failure occurs if the system of equations (5) has more than one solution. In the following, we derive an upper bound on the failure probability, which is the same as for the virtual extension of the RS codes used in [3] and therefore independent of the column multipliers.

We bound the probability that the $s(n - \bar{k} - t) \times t$ matrix $S$ does not have full rank $t$ and denote the failure probability, if $t$ errors occurred, by:

$$P_f(t) \leq P(\text{rank}(S) < t \mid |E| = t).$$

The following theorem states the failure probability.

**Theorem 2 (Upper Bound on the Failure Probability)** Let a codeword of an $\mathcal{GRS}(V; n, k)$ code be corrupted by an error of weight $t \leq \tau_{\mathcal{VIRS}}$ (11). Let the GRS code be virtually extended to an IGRS code $\mathcal{VIRS}(V; n, k, s)$ of extension order $s$ with the dimensions $k_i$ and the set of column multipliers $\nu_j^{(i)}$, for $i = 1, \ldots, s$ as in (9).

Assume, for decoding we solve the system of equations from (5). The probability for a decoding failure is upper bounded by:

$$P_f(t) \leq \left(\frac{q}{q-1} + \frac{1}{q}\right)^t \cdot q^{-3\tau_{\mathcal{VIRS}}t}.$$

(12)

**Proof:** As in the proof of [3, Theorem 3], this is equivalent to the case that there exists a vector $u \neq 0$ of length $t$, such that

$$\exists u \neq 0 : S(u^T) = 0, \forall i = 1, \ldots, s.$$ 

(13)

Each syndrome matrix can be decomposed into five matrices (in [3], the decomposition consists only of four matrices):

$$S = H \cdot \nu^{(i)} \cdot F \cdot D \cdot V,$$

(14)

where $D$ and $V$ are the same full-rank $t \times t$ matrices as in [3, Proof of Theorem 3] and

$$H = (x^{(\mu-1)}j_\nu)_{\mu=1,\ldots,n-k_i-t, \nu=1,\ldots,t},$$

$$\nu^{(i)} = \text{diag} (\nu_j^{(i)}, \nu_j^{(i)}, \ldots, \nu_j^{(i)}),$$

$$F = \text{diag} (e_j^{(i)}_1, e_j^{(i)}_2, \ldots, e_j^{(i)}_t),$$

where $E = \{j_1, j_2, \ldots, j_t\}$ denotes the union of the error positions and $e_j^{(i)}$ denotes the error value at the $j$th position of the $i$th received word. Since $\nu^{(i)}$ and $F$ are both diagonal matrices, we can switch their order. Since $\nu^{(i)}, D, V$ are nonsingular, there is a one-to-one mapping from $u$ to $v$, where $v^T = \nu^{(i)} \cdot D \cdot V \cdot u^T = (v_1, v_2, \ldots, v_t)^T$. Hence, (13) is equivalent to

$$\exists v \neq 0 : H \cdot F \cdot v^T = 0, \forall i = 1, \ldots, s.$$ 

(15)

This is the same as [3, Proof of Theorem 3, Equation (22)] and using Lemma 1 in the appendix for arbitrary $q$, the rest of the proof is analog.

Thus, the upper bound on the failure probability is independent of the column multipliers and in particular independent of using GRS codes or the RS codes from [3].

Note that this upper bound generalizes [3, Theorem 3] from RS to GRS codes and also to arbitrary $q$ (in [3, Theorem 3] it was only shown for $q = 2$). Moreover, the bound does not only hold for $s = 2$ (as indicated in [3]), but also upper bounds the
cases with \( s > 2 \), although the bound is not very tight then. This is due to the fact that we can upper bound the probability that all sub-matrices are singular by the probability that some sub-matrices are singular.

VI. CONCLUSION

We considered unambiguous decoding of low-rate GRS codes beyond half the minimum distance. For this purpose, the received word of a usual GRS codeword was virtually extended to an interleaved GRS code, similar to the Schmidt–Sidorenko–Bossert scheme. We derived the parameters of the extended code and proved that the failure probability is the same as for the RS codes from [3]. Moreover, we generalized the known bound on the failure probability to arbitrary fields.

VII. ACKNOWLEDGMENT

We would like to thank Markus Ulmschneider for implementing the decoding algorithm.

APPENDIX

In the following, we extend [3, Lemma 4] to arbitrary fields.

Lemma 1 Let \((v, e, c)\) be three non-zero elements from a field \(\mathbb{F} = GF(q)\). Then, the set

\[
\mathcal{V} = \left\{ (v, e, c) \in \mathbb{F}^3 : v, e \in \mathbb{F} \setminus \{0\} \right\}
\]

with \(e^{(2)} = 2c \cdot e + e^2\) forms the set of all full weight vectors of length 2, i.e.

\[
\mathcal{V} = \left\{ v \in \mathbb{F}^2 : \text{wt}(v) = 2 \right\} = \left( \mathbb{F} \setminus \{0\} \right)^2.
\]

Proof: It is sufficient to show that all \((q - 1)^2\) possible vectors \(v \in \mathcal{V}\) are pairwise different. For any fixed \(c\), consider two vectors \(v, \tilde{v} \in \mathcal{V}\), and assume that \(v = \tilde{v}\), then

\[
v \cdot e = \tilde{v} \cdot e,
\]

\[
v \cdot e^{(2)} = \tilde{v} \cdot e^{(2)}.
\]

Dividing (17) by (16) yields

\[
\frac{2c \cdot e + e^2}{e} = \frac{e^{(2)}}{e} = \frac{\tilde{c} \cdot e + e^2}{\tilde{e}}.
\]

Therefore, \(2c + e = 2c + \tilde{e}\) and hence, \(e = \tilde{c}\). Inserting this into (16), we obtain \(v = \tilde{v}\). Thus, for any \(c\), two different pairs \((v, e) \neq (\tilde{v}, \tilde{e})\) always result in two different vectors \(v, \tilde{v}\).

REFERENCES


66
Iteration-constrained design of IRA codes

Alex Grant, Ingmar Land and Guangsong Wang
Institute for Telecommunications Research
University of South Australia
{alex.grant,ingmar.land}@unisa.edu.au, wangy012@mymail.unisa.edu.au

Abstract—This paper addresses extrinsic information chart-based design of non-systematic irregular repeat-accumulate codes for a given number of decoding iterations. This criterion is of practical importance in many applications where complexity or latency is limited. Our main contribution is a novel formulation of the optimization problem in a particular way that makes its actual evaluation possible. This is achieved by introducing additional optimization variables and constraints which have the effect of “unrolling” the iteration. Our approach enforces the finite iteration condition, while avoiding the need to know arbitrary repeated functional compositions of the component EXIT functions. We restrict attention to the binary erasure channel, for which the EXIT chart approach is exact. Extension to other sparse-graph codes and other communication channels is straightforward.

I. INTRODUCTION

Sparse-graph codes with iterative message-passing decoding represent the state-of-the-art of modern channel coding. The two major classes are low-density parity-check (LDPC) codes, and irregular repeat-accumulate (IRA) codes. For both classes, encoding and decoding complexity are linear in the code length, and there are efficient code design methods [1–3].

The typical design goal in the literature is capacity-approaching codes. These codes that have maximum rate while the probability of error diminishes with increasing code length and increasing number of iterations. The predominant approaches are density evolution and extrinsic information transfer (EXIT) charts [1, 4, 5]. While density evolution provides exact results for the decoding threshold, the EXIT chart method employs a Gaussian approximation. The advantage of the former, however, is that code design can often be formulated in terms of a convex optimization problem, allowing convenient numerical evaluation. Tradeoffs between the two methods for the design of IRA codes were discussed in [6]. For erasure channels, the two methods are equivalent.

Two important parameters characterizing implementation complexity are the parity-check matrix density and the number of decoding iterations. The relationship between parity-check density and performance in terms of the gap to capacity have been analyzed in [7, 8], the required number of iterations for successful decoding and corresponding bounds have been addressed in [9]. As opposed to LDPC codes, non-systematic IRA codes can achieve capacity on the binary erasure channel with bounded complexity per information bit [7].

Whereas the above approaches assume infinite iteration, the number of iterations required to achieve a target performance is of practical interest. In [10] a method for the design of irregular LDPC codes was proposed, which minimizes the number of iterations for a given target error probability. The key concept is to approximate the number of iterations by a continuous function, and use this as the objective function in the optimization. Starting from a capacity-achieving code, the variable-node degree distribution is iteratively adapted to improve this objective function.

We take a different approach, seeking a code that is optimized for a fixed number of iterations. We restrict ourselves to non-systematic IRA codes over the binary erasure channel (BEC). Extension to other spars-graph codes and to other communication channels (given the usual assumptions and approximations with EXIT charts) is possible.

II. IRA CODES AND EXIT CHARTS

We assume familiarity with low-density parity-check codes, their graphical representation, iterative decoding, and EXIT chart based design [1–3, 5]. We focus on non-systematic irregular repeat accumulate codes, where information bits are repeated, interleaved, passed through parity-checks, and finally scrambled by an accumulator [6, 11]. Only the code bits produced by the accumulator are transmitted over the channel. We restrict our analysis to the binary erasure channel, for which the EXIT chart approach is exact [12].

The encoder maps k information bits onto n code bits, the code rate is \( R = k/n \). The code is defined by the edge perspective degree polynomials, \( \lambda(z) = \sum_i \lambda_i z^{i-1} \) for the variable-nodes and \( \rho(z) = \sum_i \rho_i z^{i-1} \) for the check-nodes, where \( \lambda_i, i = 1, 2, \ldots \) denotes proportion of edges connected to variable nodes of degree \( i \), and \( \rho_i, i = 1, 2, \ldots \) denotes the proportion of edges connected to check nodes of degree \( i \). According to common practice in the literature, \( \rho_i \) does not count the connection to the accumulator. The design rate is

\[
R_d = \frac{\sum_i \lambda_i / i}{\sum_i \rho_i / i} = \int_0^1 \frac{\lambda(z)dz}{\int_0^1 \rho(z)dz} \leq R,
\]

The code bits are transmitted over a binary erasure channel with erasure probability \( \delta \) and capacity \( C = 1 - \delta \).

The iterative decoder consists of three components: the variable-node decoder, the check-node decoder, and the accumulator decoder. Only the accumulator obtains observations from the channel. In every iteration the component decoders are activated in the order variable-check-accumulator-check.

In the EXIT chart method, the mutual information transfer between the component decoders is modeled and used to analyze convergence behavior [5]. For the following analysis,
we combine the check-node decoder and the accumulator decoder into a single unit, henceforth referred to as the check-accumulator decoder. Since we have assumed a binary erasure channel, all virtual channels are also erasure channels and EXIT chart analysis is exact [12].

As shown in Figure 1, we orient the extrinsic information transfer chart with the $x$-axis representing the variable-node extrinsic information $I_{Ev}$ and the check-accumulator a-priori information $I_{Av}$. The $y$-axis carries the variable-node a-priori information $I_{Av}$ and check-accumulator extrinsic information, $I_{Eca}$. In order to avoid proliferation of subscripts, where it will not cause confusion, we simply use $x$ and $y$ to represent these quantities. The variable-node EXIT function $f(y)$ maps from $y = I_{Av}$ onto $x = I_{Ev}$. Conversely, the check-accumulator function $g(x)$ maps from $x = I_{Eca}$ onto $y = I_{Eca}$.

![EXIT chart](image)

Fig. 1. Example EXIT chart of a non-systematic IRA code: variable-node EXIT function $f(y)$ and check-accumulator EXIT function $g(x)$.

The variable node EXIT function is given by [12]

$$f(y) = \sum_i \lambda_i f_i(y)$$

$$f_i(y) = 1 - (1 - y)^{1-i}, \quad i = 1, 2, \ldots$$

(2)

(3)

where $f_i$ is the transfer function for a degree-$i$ variable node. The check-accumulator EXIT function is [12]

$$g(x) = \sum_i \rho_i g_i(x),$$

$$g_i(x) = x^{i-1} \left( \frac{C}{1 - (1 - C)x^i} \right)^2, \quad i = 1, 2, \ldots$$

(4)

(5)

where $g_i$ is the transfer function for a degree-$i$ check node combined with the accumulator. We can show that $f(y)$ and $g(x)$ are linear in $\lambda$ and $\rho$ and convex in $y$ and $x$, respectively. Denote $x^{(\ell)} = I_{Ev}^{(\ell)}$ the extrinsic information at the output of the variable node decoder after iteration $\ell$, and let $y^{(\ell)} = f_{Av}^{(\ell)}$ be the corresponding a-priori information. With reference to Figure 1, the corresponding values of the trajectory for $L$ iterations are given recursively for $\ell = 1, 2, \ldots$ by

$$x^{(\ell)} = f(y^{(\ell-1)}), \quad y^{(\ell)} = g(x^{(\ell)}).$$

(6)

The initial values are $x^{(0)} = 0$ and $y^{(0)} = g(0)$, resulting from the fact that the variable nodes are not directly connected to the communication channel.

We can eliminate the $y^{(\ell)}$ from (6) to obtain $x^{(\ell)} = f(g(x^{(\ell-1)}))$. Going a step further, we may also substitute these equalities into each other to express the variable node extrinsic information after $L$ iterations $I_{Ev}^{(L)}$ as

$$x^{(L)} = h^L(0)$$

(7)

where $h(x) = f(g(x))$ and $h^L$ denotes $L$-fold functional composition.

The areas under the variable node curve (with the orientation indicated in Figure 1) and under the check-accumulator curve are given by

$$1 - \int_{0}^{1} f(y) \, dy = \sum_i \lambda_i = \int_{0}^{1} \lambda(z) \, dz,$$

(8)

$$\int_{0}^{1} g(x) \, dx = C \sum_j \frac{\rho_j}{j} = C \int_{0}^{1} \rho(z) \, dz,$$

(9)

respectively. Substituting from (1), we have the following theorem, first proved for low-density parity-check codes in [12].

**Theorem 1 (Area Theorem):**

$$C - R_d = \frac{A}{\int_{0}^{1} \rho(z) \, dz},$$

(10)

$$A = \int_{0}^{1} g(x) \, dx - \left(1 - \int_{0}^{1} f(y) \, dy\right).$$

(11)

where $A$ is the area between the check-accumulator curve $g$ and the variable node curve $f$.

Thus, finding the code with the smallest rate gap from capacity corresponds to minimizing the area between $f$ and $g$. Note a minor difference from the original LDPC result, where $\int \rho$ sets a “scaling factor”. We do not require the inner check-accumulator code to have rate 1.

For code analysis and design, it is useful to express the (information) bit error rate of the decoder as a function of the mutual information exchanged during the iterative process.

**Theorem 2 (Bit Error Rate):** The bit error rate $P_b$ of a non-systematic IRA code transmitted over a BEC, with variable node degree distribution $\lambda$ and a-priori information $I_{Av}$ (to the variable nodes) is given by

$$P_b = \frac{1 - I_v}{2}$$

(12)

$$I_v = \left(\sum_{j} \frac{\lambda_j}{j}\right)^{-1} \sum_i \frac{\lambda_i}{i} \left(1 - (1 - I_{Av})^i\right).$$

(13)

The value $I_v$ denotes the overall variable node information.
Note that $P_b$ is monotonically increasing in $I_{AV}$. For fixed design rate $R_d$, 
\[ I_v = \left( R_d \sum_j \frac{P_j}{j} \right)^{-1} \sum_i \lambda_i \left( 1 - (1 - I_{AV})^i \right) \]  
which is linear in the $\lambda_i$, convex in the $P_j$ and concave in $I_{AV}$.

With sufficiently many iterations, the decoder will converge to the fixed point $x = f(g(x)) = h(x)$, which for a well-designed code will occur at a value of $x$ very close to 1, corresponding to a low bit error rate. To prevent an undesirable error floor, we may wish to enforce a condition that the iteration does not get stuck at a fixed point prior to some target value $x = 1 - \xi$ for some small $\xi$. To this end, we require $x < h(x)$ for all $x \in (1 - \xi, 1)$. For this range of $x$, we use a Taylor series expansion around $x = 1$, and obtain the condition $x < h(1) + h'(1) \cdot (x - 1)$, which is equivalent to 
\[ h'(1) = \lambda_2 \cdot \left( \frac{2 - C}{C} \sum_{j \geq 1} j \rho_j - 1 \right) < 1, \]  
referred to as the stability condition. This condition is always met if $\lambda_2 = 0$ (this choice is usually bad for capacity-achieving codes). Otherwise it is equivalent to 
\[ \sum_{j \geq 1} j \rho_j < \frac{1 + \lambda_2}{\lambda_2} \cdot \frac{C}{2 - C}. \]  

### III. CODE DESIGN

The prevailing approach to code design finds the degree distribution which results in the minimal rate loss from capacity. According to Theorem 1, this corresponds to a curve fitting problem. Equivalently, for fixed $P_j$, the maximum design rate is achieved by maximization of $\sum_i \lambda_i / i$. This results in the following linear program.

**Problem 1 (Capacity Approaching Code):** Given the channel capacity $C$ and check-node degree distribution $\rho$, find the variable-node degree distribution $\lambda^*$ as the solution to the following linear program:

\[ \max \lambda \]  
\[ \text{s.t.} \quad \sum_i \lambda_i = 1 \]  
\[ \sum_i \lambda_i \cdot f_i(y) > g^{-1}(y), \quad y \in [0, 1] \]  
\[ (1 + \lambda_2) \frac{C}{2 - C} - \lambda_2 \sum_{j} j \rho_j > 0 \]  
\[ \lambda_i \geq 0, \quad i = 1, 2, \ldots \]  
\[ \sum_i \lambda_i = 1. \]  

The constraints (18) ensure that there are no sub-optimal fixed points and (19) is the stability condition.

In many situations of practical interest, the implementation complexity of the decoder is limited, and it is therefore of interest to consider the design of codes that reduce decoder complexity, even if this is at the expense of reduced code rate. Complexity constraints may be introduced into the optimization problem (17) to a certain extent via (a) fixing the maximal variable node degree (which needs to be done anyhow in order to have a finite number of variables in Problem 1), or (b) introducing other linear constraints on the $\lambda_i$, e.g. corresponding to the cost of high degree nodes.

For a code optimized according to (17), operating at rates close to capacity, it may take many iterations to achieve the target bit error rate. It is therefore of great practical interest to consider the design of codes that achieve the best possible performance after a fixed number of iterations, denoted by $L$. One obvious approach would be to replace the objective function in (17) with the bit error rate at iteration $L$. From (12) and (13), we see that this is equivalent to maximizing the variable node information at iteration $L$,

\[ I_v^{(L)} = \left( \sum_i \lambda_i \frac{P_i}{i} \right)^{-1} \sum_i \lambda_i \left( 1 - (1 - g(L^{-1}(0)))^i \right) \]  

Note that $I_v^{(L)}$ is a multinomial of degree $L$ times the square of the maximal variable node degree. This could potentially present numerical difficulties for optimization. Furthermore, this formulation requires us to compute $h^L$ for each value of $L$ of interest. In the case of IRA codes and the BEC, we have analytical expressions for $f_i(y)$ and $g_i(x)$. In more general settings, we may only have numerical samples of these functions.

Motivated by (6), the key novel step in this paper is to introduce dummy variables $x_i, y_{\ell}, \ell = 0, 1, \ldots, L$. With reference to Figure 1, these are the values of the variable node extrinsic and a-priori information at iteration $\ell$. For given target rate $R$, we formulate our design problem as follows (where we have used (14)).

**Problem 2 (Minimum bit error rate after $L$ iterations):** Given $R < C$, determine the variable node degree distribution $\lambda^L$ and check node degree distribution $\rho^L$ that minimize the bit error rate after $L$ iterations as the solution to:

\[ \max_{\lambda, \rho, x, y} \left( R_d \sum_i \frac{P_i}{i} \right)^{-1} \sum_i \lambda_i \left( 1 - (1 - y_L)^i \right) \]  
\[ \text{s.t.} \quad (1), (19), (20), (21) \]  
\[ \rho_i \geq 0, \quad i = 1, 2, \ldots \]  
\[ \sum_i \rho_i = 1, \]  
\[ x_0 = 0, y_0 = g(x_0) \]  
\[ x_{\ell} = \sum_j \lambda_j f_i(y_{\ell-1}), \quad \ell = 1, 2, \ldots, L \]  
\[ y_{\ell} = \sum_j \rho_j g_i(x_{\ell}), \quad \ell = 1, 2, \ldots, L \]  

In this setup, the target rate $R$ would be chosen to be less than capacity, sacrificing some code rate for potential performance improvements after $L$ iterations.
The new constraints (25),(26),(27) ensure consistency of the decoding trajectory according to (6). The trajectory constraints are convex, however as discussed earlier, the objective function is neither convex nor concave.

We have empirically observed that there is very little bit error rate penalty incurred by replacing the bit error rate objective function (22) with $y_L$ or $x_L$, i.e. maximize the information passed between the decoders. In fact, this may be of interest if the code is an inner component of some other outer iteration, e.g. a multi-user decoder. This results in the following optimization problem:

**Problem 3 (Maximal information after L iterations):**

Given $R < C$ determine the variable node degree distribution $\lambda^L$ and check node degree distribution $\rho^L$ that maximizes the variable node extrinsic information after $L$ iterations as the solution to the following convex optimization problem:

$$
\max_{\lambda, \rho, x, y} x_L \\
\text{s.t. } (1), (19), (20), (21), (23), (24), (25), (26), (27)
$$

Note that by “unrolling” the iteration, we obtain constraints that are independent of the maximum number of iterations $L$. Furthermore, we do not need to know the $L$-fold functional composition $f(g(f(\ldots \ldots )))$. Instead, we only need to know $f(y)$ and $g(x)$ individually. This could be an additional advantage if these characteristics are only available numerically (e.g. for other kinds of codes).

### IV. Numerical Example

We seek for a code of rate $R = 0.5$ for transmission over a BEC with erasure rate $\delta = 0.3$, that achieves a low bit error probability with $L = 10$ decoding iterations. We consider variable node degrees from the set $\{2, 3, 4, 5, 6, 13, 20, 30\}$, and (for simplicity) the fixed check-node distribution $\rho_1 = 0.2$, $\rho_2 = 0.8$. (Note that degree-1 check nodes are required for non-systematic IRA codes.) Solving Problem 3 for maximal information, we obtain the variable node degree distribution $\lambda(1)$, see Table I, and the EXIT function $f(1)$, depicted in Fig. 2.

As an alternative approach, we designed a capacity-approaching code, according to Problem 1, for a BEC with a higher erasure rate, namely $\delta = 0.47$, to obtain a code rate of $R = 0.5$. We then use this code with $L = 10$ decoding iterations for the given BEC with $\delta = 0.3$. The resulting variable node distribution $\lambda(2)$ is given in Table I, and the EXIT function is depicted in Fig. 2.

For the maximal-information code, the tunnel between the EXIT functions is clearly more open towards the end, and for a given number of iterations a better performance can be achieved. Resulting from that, the bit error rate after $L = 10$

### TABLE I

**VARIABLE NODE DEGREE DISTRIBUTIONS (TWO-DIGIT PRECISION).**

<table>
<thead>
<tr>
<th>i</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>13</th>
<th>20</th>
<th>30</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\lambda(1)$</td>
<td>0.16</td>
<td>0.15</td>
<td>0</td>
<td>0</td>
<td>0.54</td>
<td>0.14</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$\lambda(2)$</td>
<td>0.01</td>
<td>0.08</td>
<td>0.06</td>
<td>0.06</td>
<td>0.02</td>
<td>0.02</td>
<td>0.01</td>
<td>0.01</td>
</tr>
</tbody>
</table>

![EXIT chart and decoding trajectories: check-accumulator EXIT function $g$; variable-node EXIT functions for the maximal-information code (Problem 3), $f(1)$, and the ‘capacity-achieving’ code (Problem 1), $f(2)$.](image)

**ACKNOWLEDGMENT**

This work has been supported in parts by the Australian Research Council under the ARC Discovery Grant DP0986089.

### REFERENCES


Abstract—This paper presents a fundamental information-theoretic scaling law for a heterogeneous cascade of links corrupted by Gaussian noise. For any set of fixed-rate encoding/decoding strategies applied at the links, it is claimed that a scaling of $\Theta(\log n)$ in block length is both sufficient and necessary for reliable communication. A proof of this claim is provided using tools from the convergence theory for inhomogeneous Markov chains.

I. INTRODUCTION

Consider a line network in which a message originating at a certain node is conveyed to the intended destination through a series of hops. The reception at every hop is impaired by zero-mean additive white Gaussian noise (AWGN) of a certain variance. The originating node as well as the intermediate nodes are subject to an average transmit-power constraint $P_0$ for the duration of transmission of any message. The messages, drawn from a certain set of size $M$, are encoded and transmitted as codewords in $\mathbb{R}^N$ that satisfy the transmit power constraint. Every intermediate hop decodes (possibly erroneously) the original message from its noisy observation and re-encodes it before transmitting to the next hop. One can form the (row-stochastic) probability transition matrix $P_i$ for the $i$th hop in which each row gives the conditional probability distribution of the message decoded at hop $i$, given a certain message sent by the previous hop:

$$P_i = \begin{pmatrix}
p_i(1|1) & p_i(2|1) & \cdots & p_i(M|1) \\
p_i(1|2) & p_i(2|2) & \cdots & p_i(M|2) \\
\vdots & \vdots & \ddots & \vdots \\
p_i(1|M) & p_i(2|M) & \cdots & p_i(M|M)
\end{pmatrix}.$$  

Assume that a network of the type outlined above consists of $n$ hops. If the encoder-decoder pairs are identical at the $i$th hop and $P_i$ is identical for all $i$, then the rows of $P^n$ will give the conditional probability distributions of the message $W_n$ decoded at the final destination, given a certain message $W$ at the originating node. For decisions made on signals corrupted by Gaussian noise, $P$ has the property that any column is either all-zero or contains only non-zero entries. For such a matrix $P$, the rows of $P^n$ tend to be identical for large $n$ (see Theorem 4.9 in [1]), if $M$, $N$, $P_0$, and $\sigma$ are independent of $n$. In other words, the probability distribution of $W_n$ will be almost independent of the original message $W$. This implies that the mutual information $I(W;W_n)$ between the original message and the decoded message tends to zero with $n$. Hence, communication in the network is highly unreliable if $N$ and $M$ do not vary with the number of hops $n$.

On the other hand, if $N$ is large and if one chooses $M = 2^{NR}$ for any $R < \frac{1}{2} \log (1 + \frac{P_0}{\sigma^2})$, random-coding theorem states that there exists a channel code of block length $N$ such that the probability of error during decoding at any link is bounded above by $e^{-N\Theta(R,P/\sigma^2)}$, where $E$ is the random coding exponent for the corresponding AWGN channel [2], [3]. By employing such a code for each link in the line network model, choosing any $f(n) \in o(1)$, and letting $N$ vary with $n$ as $N = \frac{\log n}{f(n)}$, one obtains the following union bound on the probability of communication failure in the network:

$$P \left[ W_n \neq W \right] \leq nP_E \leq ne^{-N\Theta(R,P/\sigma^2)} = e^{-f(n)} \to 0.$$  

(1)

Hence, it is possible to transmit messages with very high reliability in the network for a fixed code rate $R$, if the code length $N$ satisfies $N(n) \in \Theta(\log n)$. On the other hand, the previous discussion about diminishing $I(W;W_n)$ implies that any fixed-rate fixed-length coding scheme is not scalable for the line network. This leads to the natural question whether the scaling $\Theta(\log n)$ for $N$ is indeed optimal. In this paper, we show that for any scaling of $N$ satisfying $N(n) \in o(\log n)$, the mutual information $I(W;W_n)$ diminishes to zero with $n$ for any set of fixed-rate codes. This implies that the scaling order $\Theta(\log n)$ for $N$ is necessary for reliable communication in the network. Hence, the sufficiency criterion for $N$ given by the union bound in Eqn. (1) is indeed optimal up to a constant factor.

While this scaling problem has been solved partially in the past for cascades of homogeneous DMCs by Niesen et al. in [4], it has also been pointed out in the same work that the tools developed there apply neither to non-homogeneous cascades nor to cascades of continuous-input channels (as is the case in the current paper). In contrast, the results developed here are applicable to continuous-input AWGN links where the links can be non-identical.

1For any $f(n) > 0$ and $g(n) > 0$, $f(n) \in o(g(n)) \iff \lim_{n \to \infty} \frac{f(n)}{g(n)} = 0$, $f(n) \in \Theta(g(n)) \iff \exists c > 0 \text{ s.t. } \lim_{n \to \infty} \frac{f(n)}{g(n)} = c$. 

This work has been supported by the Australian Research Council under the ARC Discovery Grant D90986089.
II. NOTATIONS AND DEFINITIONS

The set of all real numbers is denoted by \( \mathbb{R} \) and the set of all natural numbers by \( \mathbb{N} \). Natural logarithms are assumed in the notations, unless the base is specified. The notation \( \| \cdot \| \) represents \( L^2 \) norm throughout.

We employ the following terminologies in this paper. Let \( \mathcal{W} \triangleq \{ 1, 2, 3, \ldots, 2^{NR} \} \), called the message alphabet. Let \( P_0 > 0 \) be the input power constraint for transmission.

Definition 1: A rate-\( R \) length-\( N \) code \( \mathcal{C} \) with a power constraint of \( P_0 \) is an ordering of \( M = 2^{NR} \) elements from \( \mathbb{R}^N \), called code words that satisfies
\[
\mathcal{C} = (\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \ldots, \mathbf{x}_M) \text{ s.t. } \forall w \in \mathcal{W}, \frac{1}{N} \| \mathbf{x}_w \|^2 \leq P_0.
\]

Definition 2: A rate-\( R \) length-\( N \) decision rule \( \mathcal{R} \) is an ordering of \( M = 2^{NR} \) sub-sets of \( \mathcal{W} \), called decision regions, spanning \( \mathbb{R}^N \) and pairwise disjoint:
\[
\mathcal{R} = (\mathcal{R}_1, \mathcal{R}_2, \ldots, \mathcal{R}_{M}) \text{ s.t. } \bigcup_{w \in \mathcal{R}_i} \mathcal{R}_i = \mathcal{W}, \text{ and } \mathcal{R}_i \cap \mathcal{R}_j = \emptyset.
\]

Definition 3: The encoding function \( EN_C : \mathcal{W} \rightarrow \mathbb{R}^N \) for a code \( \mathcal{C} \) is defined by:
\[
EN_C(w) = \mathbf{x}_w,
\]
where \( \mathbf{x}_w \) is the \( w \)-th code word in \( \mathcal{C} \).

Definition 4: The decoding function \( DE_C : \mathbb{R}^N \rightarrow \mathcal{W} \) for a decision rule \( \mathcal{R} \) is defined by:
\[
DE_C(y) = \bigcup_{w \in \mathcal{R}_i} w \text{ s.t. } \mathbf{y} = \mathbf{x}_w,
\]
where \( i \) is the indicator function and \( \mathcal{R}_w \) is the \( w \)-th subset in \( \mathcal{R} \).

III. NETWORK MODEL

The line network model to be considered is described in Fig. 1. There are \( n+1 \) nodes in the network identified by the indices \( \{ 0, 1, 2, \ldots, n \} \). The \( n \) hops in the network are each associated with noise variances \( \sigma_i^2, 1 \leq i \leq n \). For encoding, nodes \( 0, 1, \ldots, n-1 \) choose \( \mathcal{C}_0, \mathcal{C}_1, \cdots, \mathcal{C}_{n-1} \) respectively to transmit, each code being rate-\( R \) length-\( N \) with a power constraint of \( P_0 \). For decoding, nodes \( n, 1, \ldots, n \) choose rate-\( R \) length-\( N \) decision rules \( \mathcal{R}_n, \mathcal{R}_2, \ldots, \mathcal{R}_n \) for reception. From here on, we write \( EN_C_i \) and \( DE_C_i \) in place of \( EN_C_{\mathcal{C}_i} \) and \( DE_C_{\mathcal{C}_i} \) respectively, for simplicity. Node 0 generates a random message \( W \in \mathcal{W} \) with probability distribution \( p_W(w) \) and intends to convey the same to node \( n \) through the cascade of noisy links in a multihop fashion. Each of the \( n-1 \) intermediate nodes estimates the message (as sent by the node in the previous hop) from its own noisy observation, re-encodes the decoded message, and transmits the resulting codeword to the next hop. The codeword transmitted by node \( i \), for any \( 0 \leq i \leq n-1 \) is given by
\[
\mathbf{X}_i = EN_{C_i}(\hat{W}_i),
\]
where \( \hat{W}_i \) is the estimate of the message at node \( i \) after decoding (Note that \( \hat{W}_0 = W \) in this notation). The observation received by node \( i \), for any \( 1 \leq i \leq n \) is given by \( Y_i \), which follows a conditional density function that depends on the codeword \( \mathbf{X}_{i-1} \) sent by the previous node:
\[
p_{Y_i|X_{i-1}}(y|x) = \frac{1}{(2\pi\sigma_i^2)^{n/2}} e^{-\frac{1}{2\sigma_i^2}(y-x)^2}.
\]

The above density function follows from the assumptions of AWGN noise and memoryless-ness in the channel. The message \( \hat{W}_i \) decoded by node \( i \) is given by
\[
\hat{W}_i = DE_{C_i}(Y_i).
\]

Note that the random variable \( \hat{W}_n \) represents the message decoded by the final destination, as per the above notation.

IV. AN UPPER BOUND ON THE RELIABILITY OF THE NETWORK

The key result presented here is summarized by the following theorem and its corollary:

Theorem 1: In a line network consisting of a cascade of \( n \) AWGN links, let for \( m \leq n \) of the links the noise variances satisfy \( \sigma_i^2 \geq \sigma_0^2 > 0 \). Then, for any \( m \) choice of codes \( \mathcal{C}_0, \mathcal{C}_1, \cdots, \mathcal{C}_{n-1} \) and decision rules \( \mathcal{R}_1, \mathcal{R}_2, \cdots, \mathcal{R}_n \) with rate \( R \) length \( N \), and for any \( \epsilon > 0 \), the following holds for sufficiently large \( m \):
\[
T(W; \hat{W}_n) \leq 2^{NR} \left( 1 - \frac{m}{\binom{N+1}{2}} \right) \exp \left( -N E(S) \right) \left( \frac{1}{2} + 1 \right)^m,
\]
where
\[
E(S) = \text{exp} \left( \text{cosh}^{-1} \left( \frac{S}{2} \right) \right) + \text{cosh}^{-1} \left( \frac{S}{2} + 1 \right).
\]

The corollary to the above theorem leads to the upper bound on the reliability vs. block-length scaling as claimed in the introductory section:

Corollary 1: Let \( R > 0 \), \( \sigma_0 > 0 \), and \( 1 \geq r > 0 \) be independent of \( n \). In a line network of \( n \) links, let for all of the hops the noise variance be at least \( \sigma_0^2 > 0 \). Then, for any \( N(n) \in o(\log n) \), \( \lim_{n \to \infty} T(W; \hat{W}_n) = 0 \).

Proof of Theorem 1: At any hop \( i \), the process of channel encoding, noisy reception, followed by decoding induces the conditional probabilities \( p_{W} | Y_{i}, k \rangle, \forall j, k, \in \mathcal{W} \). For every hop \( i \), let \( \mathbf{P}_i \) be the \( M \times M \) row-stochastic matrix whose entry in row \( j \) and column \( k \) is \( p_{W_j | Y_{i-k}} \). Note that the \( j \)-th row in \( \mathbf{P}_i \) gives the conditional probability mass function on the estimate of message \( W \) at hop \( i \) (i.e., \( \hat{W}_i \)) given that the message sent by hop \( i-1 \) was \( j \). Let
\[
\mathbf{P} = \prod_{i=1}^{n} \mathbf{P}_i.
\]

Then, \( \mathbf{P} \) clearly represents the row-stochastic probability transition matrix between the original message \( W \) and the message decoded at the final destination, \( \hat{W}_n \). The transition matrix \( \mathbf{P} \)
along with \( P_W \), the probability mass function of the original message \( W \) together induce a joint distribution between \( W \) and \( \hat{W}_n \). Our goal is to find an upper bound on \( \mathcal{L}(W; \hat{W}_n) \), with the constraints as given in the statement of Theorem 1.

For any \( M \times M \) row-stochastic matrix \( Q = \{Q_{jk}\} \), let us consider the following measures of deviation:

\[
\delta(Q) \triangleq \max_{j, j' \in k} \max_{k} (Q_{jk} - Q_{j'k}) (10),
\]

\[
\lambda(Q) \triangleq 1 - \min_{j, j' \in k} \min_{k=1}^{M} (Q_{jk}, Q_{j'k}). (11)
\]

Both the above deviations measure the degree to which the rows of \( Q \) differ. The measure \( \lambda(Q) \) is known as Dobrushin’s coefficient of ergodicity and plays a role in the convergence of non-homogeneous stochastic processes [5]. Moreover, for any stochastic matrix \( Q \),

\[
0 \leq \lambda(Q) \leq 1. (12)
\]

Now consider the total variational distance between the joint distribution of \( W \) and \( \hat{W}_n \) and the product of the respective marginal distributions:

\[
\tau(W; \hat{W}_n) \triangleq \sum_{w_1, \hat{w}_n \in \mathcal{F}} |p_W(w_1)p_{\hat{W}_n}(\hat{w}) - p_W(w_1)\hat{W}_n(\hat{w})|.
\]

In the above expression, substituting \( p_W(w_1)p_{\hat{W}_n}(\hat{w}|w_1) \) for \( p_W(w_1)p_{\hat{W}_n}(\hat{w}) \), \( \sum_{w_2 \in \mathcal{F}} p_W(w_1) p_{\hat{W}_n}(\hat{w}|w_2) p_W(w_2) \) for \( p_W(w_1) \hat{W}_n(\hat{w}) \) and by using the triangle inequality, one obtains the following bound:

\[
\tau(W; \hat{W}_n) \leq \sum_{w_1, \hat{w}_n \in \mathcal{F}} p_W(w_1) \sum_{w_1} p_W(w_2) \delta(P) = M\delta(P) = 2^{N} M \lambda(P). (13)
\]

Recalling the definition of \( P \) in our case, and from Theorem 2 in [6] (equivalently, Lemma 2 in [7]), we have:

\[
\delta(P) = \delta\left( \prod_{i=1}^{n} P_i \right) \leq \prod_{i=1}^{n} \lambda(P_i) \leq \prod_{i, i \geq \sigma_0} \lambda(P_i). (14)
\]

The second inequality in the above follows by applying Eqn. (12) for those hops for which \( \sigma_i < \sigma_0 \). Note that as per the statement of the theorem, we have at least \( m \) terms in the product in the last expression above. Now consider \( \lambda(P_i) \) for any hop \( i \) such that \( \sigma_i \geq \sigma_0 \). Suppose \( P_i \) has \( L \) distinct columns with indices \( k_1, k_2, \ldots, k_L \) such that

\[
\forall j, P_{j k_1} = p_{W_1|W_n}(k_1|j) \geq p_1
\]

\[
\vdots
\]

\[
\forall j, P_{j k_L} = p_{W_1|W_n}(k_L|j) \geq p_L. (15)
\]

Then from the definition in Eqn. (11), it follows that

\[
1 - \lambda(P_i) \geq \sum_{i=1}^{L} p_i. (17)
\]

We now show that the conditions given by Eqn. (15)-(16) hold true in our case, so that we can apply Eqn. (17) to our bound. Let \( \alpha > 0 \). Consider one particular hop \( i \) satisfying \( \sigma_i \geq \sigma_0 \). Define the spherical regions

\[
S_i = \{ y \in \mathbb{R}^N : \|y\| \leq \sqrt{NP_0} \}
\]

\[
S_{\alpha i} = \{ y \in \mathbb{R}^N : \|y\| \leq \alpha \sqrt{NP_0} \}
\]

Clearly, any code word in \( S_{\alpha i} \) (transmitted by the previous hop) has to be in \( S_1 \). Next, observe that \( S_{\alpha i} \) has to contain decision regions, say \( L \) in number, spanning \( S_{\alpha i} \) entirely. Let us designate them as \( R_{k_1}, R_{k_2}, \ldots, R_{k_L} \). Also define for each \( 1 \leq \ell \leq L \), \( V_{\ell} = R_{k_{\ell}} \cap S_{\alpha i} \). Hence, we have:

\[
\bigcup_{\ell=1}^{L} V_{\ell} = S_{\alpha i}, \quad \text{and } \forall i, j \neq i, V_{\ell_{i}} \cap V_{\ell_{j}} = \emptyset. (18)
\]

Let \( \hat{W}_{i-1} = j \) be the message as decoded by the previous hop. Hence, the code word \( x_i \) from \( \mathcal{C}_{i-1} \) was transmitted by the node \( i - 1 \). The probability that this was decoded as message \( k_{\ell} \) at hop \( i \) is given by:

\[
p_{W_1|W_n}(k_{\ell}|j) = \int_{y \in S_{\alpha i}} p_{Y|X_n}(y|x_j) \, dy \geq \int_{y \in V_{\ell}} p_{Y|X_n}(y|x_j) \, dy \geq \int_{y \in V_{\ell}} e^{-\frac{\|y-x_j\|^2}{2\sigma_i^2}} \, dy \geq \int_{y \in V_{\ell}} e^{-\frac{(1+1)e^{2\sigma_i^2}}} \, dy \geq e^{-\frac{(1+1)e^{2\sigma_i^2}}{2\sigma_i^2}} |V_{\ell}|. (19)
\]
where $|V_i|$ denotes the $N$-dimensional volume of $V_i$. In the above series of inequalities, step (a) follows from Eqn. (7), (b) from the triangle inequality, and (c) from the fact that any $y \in V_i$ must satisfy $\|y\| \leq \alpha \sqrt{N} P_0$, since $V_i \subseteq S_0$, and from the fact that $x_j$, being a code word in $V_j$, naturally satisfies the power constraint criterion given by $\|x_j\| \leq \sqrt{N} P_0$. Note that the lower bound given by Eqn. (19) is independent of the message $j$ decoded by the previous hop. Hence, the conditions given by Eqns. (15)-(16) are satisfied for

$$p_t = \frac{1}{(2\pi \sigma^2)^{3/2}} e^{-\frac{(\|x\|^2 + \frac{\Gamma}{2} x_0^2)}{2\sigma^2}} |V_i|.$$ (20)

Hence, the bound given by Eqn. (17) holds true. In our case, it gives:

$$1 - \lambda(P_t) \geq \sum_{l=1}^{L} p_l = \frac{1}{(2\pi \sigma^2)^{3/2}} e^{-\frac{(\|x\|^2 + \frac{\Gamma}{2} x_0^2)}{2\sigma^2}} \sum_{l=1}^{L} |V_i| = \frac{1}{(2\pi \sigma^2)^{3/2}} e^{-\frac{(\|x\|^2 + \frac{\Gamma}{2} x_0^2)}{2\sigma^2}} \left(\frac{\pi}{\Gamma(1/2+1)} \right)^{N} (\alpha \sqrt{N} P_0)^{N}$$ (21)

The last inequality follows from the fact that $V_i$ are mutually disjoint and span the entire $N$-dimensional sphere $S_0$ (Eqn. (18)). The volume of $S_0$ is computed as:

$$|V_i| = \pi^{\frac{3}{2}} \Gamma \left(\frac{1}{2} + 1\right) \left(\frac{\sigma}{\alpha \sqrt{N} P_0}\right)^N.$$ (22)

The ideas in the above argument are outlined in Figs 2(a) and 2(b).

Fig. 2: Geometrical argument used for bounding $\lambda(P_t)$.

Next, note that the bound given by Eqn. (21) holds true for any $\alpha > 0$. Hence, we can maximize the right hand side of Eqn. (21) over all $\alpha > 0$ to obtain

$$1 - \lambda(P_t) \geq \left(\frac{\pi}{\Gamma(1/2+1)} \right)^{N} e^{-\frac{\Gamma}{2} x_0^2} \left(\frac{\pi}{\Gamma(1/2+1)} \right)^{N} (\alpha \sqrt{N} P_0)^{N}$$ (23)

where the function $E'(S)$ is as given in the statement of the theorem. Noting further that $E(S)$ is a non-decreasing function in $S$, we will have for hops satisfying $\sigma_t \geq \sigma_0$,

$$\lambda(P_t) \leq 1 - \left(\frac{\pi}{\Gamma(1/2+1)} \right)^{N} e^{-\frac{\Gamma}{2} x_0^2} \left(\frac{\pi}{\Gamma(1/2+1)} \right)^{N} (\alpha \sqrt{N} P_0)^{N}.$$ (24)

Since at least $m$ hops satisfy the minimum noise variance criterion $\sigma_t \geq \sigma_0$, we can now combine Eqn. (24) with Eqn. (14) to obtain

$$\delta(P) \leq \left(1 - \left(\frac{\pi}{\Gamma(1/2+1)} \right)^{N} e^{-\frac{\Gamma}{2} x_0^2} \left(\frac{\pi}{\Gamma(1/2+1)} \right)^{N} (\alpha \sqrt{N} P_0)^{N} \right)^m.$$ (25)

Applying the above to Eqn. (13), we will have

$$\tau(W;W_n) \leq 2^{NR} \left(1 - \left(\frac{\pi}{\Gamma(1/2+1)} \right)^{N} e^{-\frac{\Gamma}{2} x_0^2} \left(\frac{\pi}{\Gamma(1/2+1)} \right)^{N} (\alpha \sqrt{N} P_0)^{N} \right)^m.$$ (26)

We can finally bound $I(W;W_n)$ using Lemma 2.7 of Chapter 1 in [8] by:

$$I(W;W_n) \leq \tau(W;W_n) \log 2^{NR} \tau(W;W_n).$$ (27)

The bound given by the statement of the theorem then follows from combining the above with Eqn. (26) and by observing that for sufficiently large $m$, $\tau(W;W_n) \leq e^{-1}$, that $-x \log x$ is non-decreasing for $x \leq e^{-1}$, and finally from the fact that for any $\epsilon > 0$, $x^\epsilon \geq \log x$ for sufficiently large $x$.

Proof of Corollary 1: For the corollary, we have $m = nr$. Moreover, $\Gamma(1/2 + 1) \leq \left(\frac{\pi}{\Gamma(1/2+1)} \right)^{N}$. Hence, the bound given by Theorem 1 reduces to:

$$I(W;W_n) \leq 2^{NR} \left(1 - e^{-\frac{\Gamma}{2} x_0^2} \left(\frac{\pi}{\Gamma(1/2+1)} \right)^{N} (\alpha \sqrt{N} P_0)^{N} \right)^{nr(1-\epsilon)}$$ (28)

$$\leq 2^{NR} e^{-nr(1-\epsilon)} e^{-\frac{\Gamma}{2} x_0^2} \left(\frac{\pi}{\Gamma(1/2+1)} \right)^{N} (\alpha \sqrt{N} P_0)^{N}$$ (29)

$$= e^{NR \log 2 - e^{-\frac{\Gamma}{2} x_0^2} \left(\frac{\pi}{\Gamma(1/2+1)} \right)^{N} (\alpha \sqrt{N} P_0)^{N}}.$$ (30)

The last expression diminishes to 0 with $n \to \infty$ if $N(n) = N(n) \in o(\log n)$. Hence, we will have $I(W;W_n) \to 0$ for any $N \in o(\log n)$.

REFERENCES

Secure Multiplex Coding Over Interference Channel with Confidential Messages

Xiaolin Li
Dept. of Electrical and Computer Engineering
Hong Kong University of Science and Technology
darwinlx1@ust.hk

Ryutaroh Matsumoto
Dept. of Communications and Integrated Systems
Tokyo Institute of Technology, 152–8550 Japan, and Dept.
of Mathematical Sciences, Aalborg University, Denmark.
ryutaroh@it.ss.titech.ac.jp

Abstract—In this paper, an inner bound on the capacity region of two-user interference channels with two confidential messages has been proposed. With secure multiplex coding, we show that the Han-Kobayashi region can be achieved with strong security requirement. The equivocation rate for a collection of secret messages has also been evaluated, when the length of the message is finite or the information rate is high, our result provides a good approximation for bounding the worst case equivocation rate.

Index Terms—Information theoretic security, capacity region, interference channel, secure multiplex coding, strong security.

I. INTRODUCTION

In [12] the authors proposed the celebrated Han-Kobayashi region which provided the best inner bound on the channel capacity of the interference channel known to now. In the coding scheme proposed in that paper, the information from each transmitter was divided into two parts, the first part was for only one receiver (we say this part of the information is sent over the “private channel”), and the other part could be decoded only by both receivers (we say this part of the information is sent over the “common channel”). A natural question raises: what is the secrecy transmission rate if only confidential messages are sent? In [2], the authors proposed an inner bound of secure transmission over interference channel by modifying the coding scheme in [11], and information is only sent over the “private channel”, which is a natural solution. But in this paper, we show somewhat surprisingly that even if we transmit over the “common channel”, confidentiality can also be guaranteed, thus we propose a larger achievable security rate region.

Also in [2], outer and inner bounds have been provided, but are under the weak secrecy requirement [3], which requires that the mutual information divided by the length of the codeword goes to zero as the codeword length goes to infinity. But this requirement is not strong enough for some applications [8] [9], because even if this rate goes to zero asymptotically, vital information bits can still be easily leaked to an illegitimate receiver. Moreover, secrecy is achieved by adding dummy random bits into the transmitted signal, which inevitably decreases the information rate.

The authors in [2] did not evaluate the equivocation rate when the information rates of the secret messages are large or the length of the message is finite. This means that their results are only valid for the cases where secrecy can be asymptotically achieved, but if the secrecy requirement is not achieved, they are not able to evaluate how much information may be leaked out.

In [4], the authors proposed the secure multiplex coding scheme for wiretap channels, the goal of which is to remove the rate loss incurred by the random dummy message. In [5] and [7], the authors applied the secure multiplex coding in different scenarios: broadcast channels with a common message and secure network coding. They showed that secure multiplex coding can not only remove the information rate loss, but can also achieve strong security within the capacity region.

In this paper, the model of interference channel with confidential messages as in [2] is considered. By applying the technique of secure multiplex coding, we propose an inner bound that can achieve the Han-Kobayashi region with the strong security requirement. Moreover, we give the dominating term approximation for a lower bound on the equivocation rate with finite message length.

This paper is organized as the following: in Section II, the system model and preliminaries shall be introduced. In Section III, we present an inner bound on the secure capacity of the interference channel. Section IV concludes the paper.

II. SYSTEM MODEL AND PRELIMINARIES

A. System Model

We adopt the same channel model as in [2]. Consider a discrete memoryless interference channel with finite input alphabets $X_1$, $X_2$, finite output alphabets $Y_1$, $Y_2$, and the channel transition probability distribution $P_{Y_1,Y_2|X_1,X_2}$. Two transmitters wish to send independent, confidential messages to their respective receivers.

The definition of the capacity region for the interference channel with secure multiplex coding is given as follows:

Definition 1: The rate tuple $(R_{1,1}, \ldots, R_{1,T_1}, R_{2,1}, \ldots, R_{2,T_2})$ and the equivocation rate tuple $\{(R_{1,1}, \ldots, R_{2,T_2}) | 0 \neq I_1 \subseteq \{1, \ldots, T_1\}, 0 \neq I_2 \subseteq \{1, \ldots, T_2\}\}$ are said to be achievable for the secure multiplex coding with $T_1$ secret messages for sender 1 and $T_2$ messages for sender 2, if there exists a sequence of stochastic encoders for sender 1 denoted as $\zeta_1^n : \mathcal{X}_1^n \times \cdots \times \mathcal{X}_1^n \rightarrow \mathcal{Y}_1^n$, and for sender 2 denoted as $\zeta_2^n : \mathcal{X}_2^n \times \cdots \times \mathcal{X}_2^n \rightarrow \mathcal{Y}_2^n$, and for receiver 1 deterministic...
decoder $\varphi^n_1: \mathcal{Y}^n \to C^n_{1,1} \times \cdots \times C^n_{1,T_1}$, and for receiver 2
deterministic decoder $\varphi^n_2: \mathcal{Y}^n \to C^n_{2,1} \times \cdots \times C^n_{2,T_2}$ such that

$$\lim_{n \to \infty} \Pr\{|C^n_{1,i} \neq C^n_{1,j}\} = 0,$$

or

$$\lim_{n \to \infty} I(C^n_{2,i}; Y^n_2) = 0 \quad \text{if} \quad R_{1,i}, X_1 \in I_1,$$

for $i = 1, \ldots, T_1$ and $j = 1, \ldots, T_2$, where $C^n_{1,i}$ and $C^n_{2,j}$ represent the
$i$-th secret message from sender 1 and the $j$-th secret message from sender 2 respectively. All of
$C^n_{1,i}$ and $C^n_{2,j}$ have uniform distribution on $\mathcal{C}^{n}_{1,i}$ and $\mathcal{C}^{n}_{2,j}$ and are statistically independent. Both of $C^n_{1,i}$ and $C^n_{2,j}$ are collections of random variables: $C^n_{1,i} = \{C^n_{1,i} | i \in I_1 \}$ and $C^n_{2,j} = \{C^n_{2,j} | j \in I_2 \}$. The received signals by the two receivers are denoted as $Y^n_1$ and $Y^n_2$, with the transmitted signals $C^n_{1,i}$ and $C^n_{2,j}$, and the channel transition probability $P_{Y^n_1, Y^n_2 | X^n_1, X^n_2}$. The capacity region of the secure multiplex coding is the closure of the achievable rate tuples.

**Remark 2:** Note that (2) and (3) reflect the requirement of strong secrecy in [3].

The main idea behind the multiplex coding is that instead of making the mutual information between $C^n_{1,i}$ and $Y^n_1$ to be zero, we now only need to ensure $I(C^n_{1,i}, Y^n_2)$ vanishes, which means each multiplex channel is secure. Since other messages $C^n_{1,i}$ and $C^n_{1,i+1}$ are independent with $C^n_{1,i}$, they acted as noise and provide protection for $C^n_{1,i}$.

**B. Preliminaries**

Throughout the whole paper we use natural log.

The definition of interference channel can be found in [1], in the following we introduce the Han-Kobayashi region:

**Theorem 3:** [11] Let $P^n_1$ be the set of probability distribution $P^n_1(\cdot)$ that factor as

$$P^n(u, w_1, w_2, v_1, v_2) = p(u)p(v_1, w_1|u)p(v_2, w_2|u)$$

Let $R_{HK}(P^n_1)$ be the set of nonnegative rate-tuples $(R_1, R_2)$ that satisfy

$$R_1 \leq I(V_1; Y_1|W_2U)$$

$$R_1 \leq I(V_1; Y_1 | W_2W_1U) + I(V_2W_1; Y_2|W_2U)$$

$$R_1 \leq I(V_2; Y_2 | W_2W_1U) + I(V_1W_2; Y_1|W_1U)$$

$$R_1 + R_2 \leq I(V_1W_2; Y_1|W_2) + I(V_2; Y_2 | W_2U)$$

$$R_1 + R_2 \leq I(V_1W_2; Y_1 | W_2U) + I(V_2W_1; Y_2|W_1U)$$

$$R_1 + R_2 \leq I(V_1W_2; Y_1 | W_1U) + I(V_2W_1; Y_2|W_2U) + I(V_1Y_2|W_1U) + I(V_2Y_1|W_2U)$$

$$R_1 + R_2 \leq I(V_2W_1; Y_1 | W_2U) + I(V_2W_1; Y_2|W_2U) + I(V_1Y_2|W_1U)$$

Then we have

$$R_{HK} = \cup_{P^n_1 \in P^n_1} R_{HK}(P^n_1)$$

is an achievable rate region for the discrete memoryless interference channel.

**III. Inner Bound on the Secure Multiplex Coding with Strong Secrecy Requirement**

Denote the total rate of the sender by $t \leq R_t = \sum_{i=1}^{T_1} R_{i} \leq I(V_1; Y_1|U)$ (here $t = 1$ or 2, and we adopt this notation throughout the paper). An inner bound is proposed as the following:

**Theorem 4:** Let $P_2^n$ be the set of probability distribution $P_2^n(\cdot)$ that factor as

$$P^n(u, w_1, w_2, v_1, v_2, x_1, x_2, y_1, y_2)$$

$$= p(u)p(w_1, v_1, w_2, v_2, x_1, x_2|u)p(y_1, y_2|x_1, x_2)$$

$$= p(u)p(w_1, v_1|x_1)p(v_1, w_2, v_2|x_2)p(x_1, x_2|v_2,v_2)$$

$$+ P(y_1, y_2|x_1, x_2)$$

In the above, $x_1$, $x_2$, and $y_1$, $y_2$ are the inputs and outputs of the interference channel respectively.

And $P_{in}(P_2^n)$ be the set of nonnegative rate-tuples and $(R_1, R_2, R_{1,i}, R_{2,j})$ satisfy

$$R_{1,i} = R_{1,1,j} + I(V_1; Y_1|U, V_2)$$

$$R_{2,j} = R_{2,2,j} + I(V_2; Y_2|U, V_1)$$

$$(R_1, R_2) \in R_{HK}(P_2^n)$$

$$0 \leq R_{1,1,j} \leq \sum_{i \in I_1} R_{1,i}$$

$$0 \leq R_{2,2,j} \leq \sum_{j \in I_2} R_{2,j}$$

Note in the above we abuse the notation a little by writing $R_{HK}(P_2^n)$. We can write this because if $P^n(u, w_1, w_2, v_1, v_2, x_1, x_2, y_1, y_2) \in P_2^n$, then the marginal distribution $P^n(u, w_1, w_2, v_1, v_2, x_1, x_2, y_1, y_2) \in P_2^n$.

An inner bound for the interference channels with secure multiplex coding is
\[ R_{in} = \cup_{P_2 \in \mathcal{F}_2} R_{in}(P_2) \]

\textbf{Proof:}

\textbf{Part 1: Random Coding Scheme}

Before presenting the random coding scheme, some notations are introduced: let \((c_{t,1}^1, \ldots, c_{t,T_t}^1) \in \mathcal{C}_{t,T_t}^1 \) be the secret messages for transmitter \( t \), and denote \( \mathcal{C}_t^0 = \prod_{i=1}^{T_t+1} C_{t,T_t+1}^i \), where \( C_{t,T_t+1}^i \) is the alphabet of randomness used by the stochastic encoder, and \( n \) denotes the code length. Let \( \mathcal{F}_t^n \) be the set of all linear bijective maps from \( C_t^0 \) to itself.

We modify the random coding scheme proposed in [11], and apply the secure multiplex coding techniques. The new scheme is described in detail as follows:

1. **Codebook Generation:** Sender \( t \) and receiver \( t \) fix and agree on the choice of a bijective function \( f_t^n \in \mathcal{F}_t^n \). Given \( T_t \) secret messages \((-\text{private channel})\) \((c_{t,1}^1, \ldots, c_{t,T_t}^1) \in \mathcal{C}_{t,T_t}^1 \), uniformly choose \( c_{t,T_t+1}^1 \in C_{t,T_t+1}^1 \), let \( \alpha_t = (f_t^n)^{-1}(c_{t,1}^1, \ldots, c_{t,T_t+1}^1) \). Here the message \( c_{t,T_t+1}^1 \) is used by the stochastic encoder to increase the randomness in the secret message. In order to use multiplex coding, we write

\[ C_t^0 = (E_t^n, B_t^n) = (f_t^n)^{-1}(\{c_{t,1}^1, \ldots, c_{t,T_t+1}^1\}) \]

Here \( f_t^n \) belongs to the family of linear bijective maps \( \mathcal{F}_t^n \), and this is achieved by matrix multiplication. Applying \((f_t^n)^{-1}\) on the secret messages can be achieved by matrix multiplication:

\[ C_t^n = (L_t^n)^{-1} [c_{t,1}^n, \ldots, c_{t,T_t+1}^n]^T. \]

Note that if the length of \( C_t^n \) is \( k_{t,n} \), then \( L_t^n \) is a nonsingular matrix of size \( k_{t,n} \times T_t \) with \( L_t^n = \sum_{l_t=1}^{T_t+1} k_{t,l_t} \). Randomly generate a sequence \( u \) with probability \( P(u) = \prod_{i=1}^{n} P(u_i) \), and assume that both transmitters and receivers know the time-sharing sequence \( u \).

For transmitter \( t \), generate \( 2^{nS_i} \) independent sequences \( S_t \) is the information rate over the “common channel” \( w_t \), each with probability \( P(w_t|u) = \prod_{i=1}^{n} P(w_{t_i}|u_i) \). Then generate \( 2^{nT_t} \) \((R_{in} = S_t + T_t, \text{and } T_t \text{ is the rate of information over “private channel”})\) independent sequences \( v_t \), each with probability \( P(v_t|w_t,u) = \prod_{i=1}^{n} P(v_{t_i}|w_{t_i},u_i) \).

2. **Encoding:** Encode \( v_t \) with encoder \( t1 \) and \( t2 \) (here \( t = 1 \) or \( 2 \), refer to Fig. 1), according to the codebook generated in the previous step and obtain the codeword \( v_{t,n} \). Then the transmitters generate the channel input sequences based on respective mappings \( P_{X_t|V_t}, P_{X_{t2}|V_{t2}} \).

The structure of the encoder is illustrated in Fig. 1. The codebook for encoder \( ij \) is denoted as \( \Lambda_{ij} \in \Lambda_{ij} \) \((i, j = 1, 2)\), for the simplicity of notations, let \( \Lambda = (\Lambda_{11}, \Lambda_{12}, \Lambda_{21}, \Lambda_{22}) \).

3. **Decoding:** Without loss of generality, we consider for receiver 1. Let \( A_{in}^{(n)}(W_1, V_1, W_2, Y_1, U) \) denote the set of jointly typical sequences defined in [13]. Since receiver 1 is supposed to know the time sharing sequence \( U^n \), after receiving \( Y_{1,n} \), the receiver will try to find \( W_1^n, W_{21}^n, W_{22}^n \) such that \((W_1^n, V_1^n, W_{21}^n, Y_{1,n}^n) \in A_{in}^{(n)}(W_1, V_1, W_2, Y_1, U) \). When such choice exists and is unique then the decoding is successful; otherwise declare error.

\textbf{Part 2: Evaluation of Equivocation Rate}

If we compare our scheme with the original one in [11], it can be observed that the decoding error probability in our scheme is at least as good as the original one. Hence we only need to show the existence of the tuple \((u, \lambda, f_{1}, f_{2})\) such that the strong security requirement can be fulfilled. Without loss of generality, we just need to consider the information leaked to receiver 2 from sender 1. In [6], it has been proved that if \( F_{1}^n \) is an uniform random variable on \( \mathcal{F}_1^n \) and \( \alpha_{1,2} \) is the projection from \( C_1^n \) to \( \prod_{i \in I} C_i^n \), then \( \alpha_{1,2} \circ F_{1}^n \) is a family of two-universal hashing functions [10]. The projection is simply \( \alpha_{1,2} C_1^n = \{ C_1^n \mid i \in I \} \). With a little abuse of notations, we also write \( C_{1,2}^n = (F_1^n)^{-1}(C_1^n, \ldots, C_{T_1+1}^n) \), by the uniformness of the distribution it can be seen \( C_1^n \) and \( F_1^n \) are statistically independent.

In the following, we evaluate the mutual information \( I(\alpha_{1,2}(F_1^n(C_1^n)); Y_{21}^n|F_{1}^n, \Lambda, U^n) \) and \( \rho \) is a real constant with \( 0 < \rho < 1 \). For the limitation of the pages, we omit the details which can be found in [13]. With some derivations,

\[ E_{t,n,\lambda,\rho} \exp \left( \rho I(C_{1,2}; Y_{21}^n|F_{1}^n = f_1^n, \Lambda = \lambda, U^n = u) \right) \]

\[ \leq 1 + \exp \left( n\rho(R_2 - R_1 + I(V_1; Y_2|U_2) + \epsilon) \right), \]  

where \( \epsilon(\rho) \to 0 \) \((\rho \to 0)\), and \( R_2 = \sum_{i \in I} R_{1i} \).

From (27), if \( R_2 - R_1 + I(V_1; Y_2|U_2) < 0 \), we can always choose large enough \( n \), such that

\[ I(C_{1,2}; Y_{21}^n|F_{1}^n, \Lambda, U^n) \leq \epsilon_n \]  

Hence we can see that the strong security is achieved.

In case the strong secrecy can not be achieved or \( n \) is finite, by almost the same argument in [7], there exists at least one tuple \((f_1^n, \lambda, u)\) such that

\[ I(C_{1,2}; Y_{21}^n|F_{1}^n, \Lambda, U^n) < 2^{T+2} \epsilon_n \]

\[ \exp(\rho I(C_{1,2}; Y_{21}^n|F_{1}^n = f_1^n, \Lambda = \lambda, U^n = u)) \]

\[ \leq 2^{T+2} \left[ 1 + \exp \left( n\rho(R_2 - R_1 + I(V_1; Y_2|U_2) + \epsilon) \right) \right]. \]  

such that
Decoding error probability \( \leq 2^{T+2}\delta_n \).

In the above expressions, \( \epsilon(\rho) \) is a constant that only depends on \( \rho \), and \( \lim_{\rho \to 0} \epsilon(\rho) = 0 \).

By Eq. (29) we can see

\[
I(C_1; X; Y_1^n | F_1^n = f_1^n, \Lambda = \lambda, U^n = u))
\leq 1 + \log(2^{T+2}) \frac{n}{n\rho} + R_2 - R_p + I(V_1; Y_2 | U V_2) + \epsilon(\rho).
\]

(30)

for \( R_2 - R_p + I(V_1; Z | U) + \epsilon(\rho) \geq 0 \). By Eq. (30) we can see that the equivocation rate \( H(C_1; X; Y_1^n | F_1^n = f_1^n, \Lambda = \lambda)/n \) becomes larger than the required value \( R_1, I, \epsilon \) for sufficiently large \( n \). This completes the analysis of the equivocation rates and the mutual information for all \( \emptyset \neq I \subseteq \{1, \ldots, T_1\} \).

**Remark 5:** This inner bound of secret capacity over interference channel given above shows that the whole Han-Kobayashi region can be achieved. Moreover from (27) and (28), it can be observed that strong security can be achieved. Note that (28) – (30) also provides an upper bound for the leaked information, which is not analyzed in [2].

### IV. Gaussian Interference Channel and Numerical Results

In this section we use the same model and notations of Gaussian interference channel as in Section III part D in [1]. Then we compare the inner bound we proposed with that in [1]. For the sake of "fair" comparison, in our inner bound we only use a "trivial" multiplex coding, namely we let \( T_1 = T_2 = 1 \), this is equivalent to use dummy message to achieve secrecy. We can see in Fig. 2 our inner bound (denoted as "Secure-Han-Kobayashi region") is strictly larger than the one proposed in [2].

### V. Conclusions

In this paper an inner bound that achieves Han-Kobayashi region for secure multiplex coding over interference channel has been proposed. We have also presented a random coding scheme that achieves the inner bound. We have substituted the weak secrecy requirement by the strong one, and removed the information rate loss caused by the dummy message. Moreover we evaluated the equivocation rate for a collection of secret messages.

### VI. Acknowledgement

This work was partly supported by the AoE Grant E-02/08 from the University Grants Committee of the Hong Kong Special Administration Region, China, and also by the MEXT Grant-in-Aid for Young Scientists (B) No. 22760267, Grant-in-Aid for Scientific Research (A) No. 23246071, and the Vellum Foundation through their VELUX Visiting Professor Programme 2011–2012.

### References


Polymer Expansions for Cycle LDPC Codes

Nicolas Macris and Marc Vuffray
LTHC, IC, EPFL,
CH-1015 Lausanne, Switzerland
nicolas.macris@epfl.ch, marc.vuffray@epfl.ch

Abstract—We prove that the Bethe expression for the conditional input-output entropy of cycle LDPC codes on binary symmetric channels above the MAP threshold is exact in the large block length limit. The analysis relies on methods from statistical physics. The finite size corrections to the Bethe expression are expressed through a polymer expansion which is controlled thanks to expander and counting arguments.

I. INTRODUCTION

A few years ago Cherktov and Chernyak [1] devised a loop series which represents the partition function of a general vertex model as the product of the Bethe mean field expression and a residual partition function over a system of loops. In this representation all quantities are entirely expressible in terms of Belief Propagation (BP) marginals or messages. However it has not been clear so far if this representation leads to a controlled series expansions for the log-partition, in other words the free energy. If this is the case it should hopefully allow to control the difference between the true free energy and the Bethe free energy.

The loop expansion has a potential interest in coding theory since Low-Density-Parity-Check (LDPC) and Low-Density-Generator-Matrix (LDGM) codes on general binary-input memoryless symmetric (BMS) channels fit in the framework of (generalized) vertex models. In this context free energy is just another name for conditional input-output Shannon entropy. For these models it is believed that the Bethe formula for the conditional entropy/free energy is exact. However there is no general proof, except for the cases of the binary erasure channel [2], LDGM codes for high noise, and in special situations for LDPC codes at low noise [3].

We consider cycle LDPC codes for high noise (above the MAP threshold) on the binary symmetric channel (BSC). We study probability distributions which can be factorized as a sum over words the free energy. If this is the case it should hopefully controlled series expansions for the log-partition

II. LOOP AND POLYMER REPRESENTATIONS

Let \( \Gamma = (V,E) \) be a graph with vertices \( a \in V \) of regular degree \( d \) and edges \( ab \in E \). The symbol \( \partial a \) denotes the set of \( d \) neighbors of \( a \). In vertex models the degrees of freedom are spins \( \sigma_{ab} \in \{-1,+1\} \) attached to each edge. At each function node \( a \in V \) we attach a non-negative function \( f_a(\sigma_{\partial a}) \) depending only on neighboring variables \( \sigma_{\partial a} \equiv (\sigma_{ab})_{b \in \partial a} \). We study probability distributions which can be factorized as

\[
\mu_V(\vec{\sigma}) = \frac{1}{Z_{\Gamma}} \prod_{a \in V} f_a(\sigma_{\partial a}) , \quad Z_{\Gamma} = \sum_{\vec{\sigma}} \prod_{\varnothing \in \Gamma} f_{\varnothing}(\vec{\sigma}_{\varnothing}) ,
\]

and their associated free energy \( f_a(\vec{\eta}) \equiv \frac{1}{n} \ln Z_{\Gamma} \).

For each edge \( ab \in E \) we introduce two directed “messages” \( \eta_{a \rightarrow b} \) and \( \eta_{b \rightarrow a} \). For the moment these variables are arbitrary and are collectively denoted by \( \vec{\eta} \). One has the identity [1]

\[
f_a = \frac{1}{n} \ln Z_{\text{Bethe}}(\vec{\eta}) + \frac{1}{n} \ln Z_{\text{corr}}(\vec{\eta}) .
\]

The first term is the Bethe free energy functional,

\[
\ln Z_{\text{Bethe}}(\vec{\eta}) = \sum_{a \in V} \ln \left( \sum_{\sigma_{\partial a}} f_a(\sigma_{\partial a}) \prod_{b \in \partial a} e^{\eta_{b \rightarrow a} - \eta_{a \rightarrow b}} \right) - \sum_{ab \in E} \ln \left( 2 \cosh (\eta_{a \rightarrow b} + \eta_{b \rightarrow a}) \right) .
\]

The “partition function” in the second term can be expressed as a sum over all subgraphs (not necessarily connected) \( g \subset \Gamma \)

\[
Z_{\text{corr}}(\vec{\eta}) = \sum_{g \subset \Gamma} K(g)
\]

and \( K(g) = \prod_{a \in g} K_a \)

with

\[
K_a = \sum_{\sigma_{\partial a}} p_a(\sigma_{\partial a}) \prod_{b \in \partial a \setminus g} \sigma_{ab} e^{-\sigma_{ab} (\eta_{b \rightarrow a} + \eta_{a \rightarrow b})} \]

\[
p_a(\sigma_{\partial a}) = \frac{f_a(\sigma_{\partial a}) \prod_{b \in \partial a \setminus g} e^{\eta_{b \rightarrow a} - \eta_{a \rightarrow b}}}{\sum_{\sigma_{\partial a}} f_a(\sigma_{\partial a}) \prod_{b \in \partial a \setminus g} e^{\eta_{b \rightarrow a} - \eta_{a \rightarrow b}}} .
\]

It is well known that the stationary points of (3) satisfy the BP fixed point equations,

\[
\eta_{a \rightarrow b} = \frac{\sum_{\sigma_{\partial a}} \sigma_{ac} f_c(\sigma_{\partial c}) \prod_{b \in \partial a \setminus g} e^{\eta_{b \rightarrow c} - \eta_{c \rightarrow b} + \eta_{a \rightarrow b} - \sigma_{ab}}}{\sum_{\sigma_{\partial a}} f_a(\sigma_{\partial a}) \prod_{b \in \partial a \setminus g} e^{\eta_{b \rightarrow a} - \sigma_{ab}}} .
\]

Remarkably, for any solution of (5), \( K(g) = 0 \) if \( g \) contains a degree one node. Thus if \( \vec{\eta} \) is a fixed point of the BP equations then \( Z_{\text{corr}}(\vec{\eta}) \) is given by the sum in (4) over \( g \subset \Gamma \) with no degree one nodes. Such graphs are called loops (see figure 1).

One can recognize that \( Z_{\text{corr}} \) can be interpreted as the partition function of a system of polymers. A loop \( g \subset \Gamma \) can be decomposed into its connected parts in a unique way as...
illustrated on figure 1. Connected loops are called polymers and are generically denoted by the letter $\gamma$. The important point is that by definition the polymers do not intersect. For each polymer $\gamma$ we define a weight (also called activity), $K(\gamma) = \prod_{a \in \gamma} K_a$. Let $g = \bigcup_{i=1}^M \gamma_i$. Since the $\gamma_i$ are disjoint, $\prod_{a \in g} K_a = \prod_{i=1}^M K(\gamma_i)$. Thus equation (4) can be cast in the form

$$Z_{\text{corr}}(\vec{\eta}) = \sum_{n \geq 0} \frac{1}{n!} \sum_{\gamma_1, \ldots, \gamma_M} \prod_{i=1}^M K(\gamma_i) \prod_{i<j} |\gamma_i \cap \gamma_j = \emptyset|.$$ \hspace{1cm} (6)

In this sum each $\gamma_i$ runs over all connected subgraphs with no dangling edges of the underlying graph $\Gamma$. The sum over the number of polymers $M$ has a finite number of terms because the polymers cannot intersect.

In the next paragraphs $\Gamma$ is a random $d$-regular graph. We denote by $P$ and $E$ the relevant probability and expectation over this ensemble.

III. POLYMER EXPANSION

We wish to compute the correction to the Bethe free energy in (2), namely

$$f_{\text{corr}}(\vec{\eta}) = \frac{1}{n} \ln Z_{\text{corr}}(\vec{\eta})$$

when $\vec{\eta}$ is a BP fixed point. Using (6) the logarithm can be expanded as a power series in $K(\gamma_i)$’s. This yields the polymer (or Mayer) expansion [4]

$$f_{\text{corr}}(\vec{\eta}) = \frac{1}{n} \sum_{M=1}^{+\infty} \frac{1}{M!} \sum_{\gamma_1, \ldots, \gamma_M} \prod_{i=1}^M K(\gamma_i) \times \sum_{\{\gamma_i \cap \gamma_j \neq \emptyset\}} \prod_{G \subseteq GM \setminus \{(i,j)\} \in G} \{ -\prod (\gamma_i \cap \gamma_j = \emptyset) \}. \hspace{1cm} (7)$$

The third sum is over the set $GM$ of all connected graphs with $M$ vertices labeled by $\gamma_1, \ldots, \gamma_M$, and at most one edge between each pair of vertices. The product of indicator functions is over edges $(i,j) \in G$. It constrains the set of polymers $\gamma_1, \ldots, \gamma_M$ to intersect according to the structure of $G$. In this expansion one sums over an infinite number of terms so it is important to address the question of convergence. A criterion which ensures the convergence of the expansion uniformly in system size $n$ (and thus ensures convergence in the infinite size limit) is

$$\sum_{t=0}^{+\infty} \frac{1}{n^t} \sup_{a \in V} \sum_{\gamma \ni a} |\gamma| \cdot |K(\gamma)| < 1 \hspace{1cm} (8)$$

To illustrate the use of the polymer expansion in a simple case, consider a vertex model at high temperature defined by

$$f_a(\sigma_{\partial a}) = \frac{1}{2}(1 + \tanh J_a \sum_{b \in \partial a} \sigma_{ab} e^{\frac{h_{ab} - \sigma_{ab}}{2}})$$

where $J_a$ and $h_{ab}$ are $\in \mathbb{R}$ with $\sup_{a \in V} J_a \equiv J << 1$ and $\sup_{a \in \partial a} h_{ab} < h < +\infty$. For $J$ is small enough the BP (5) equations have a unique fixed point solution [6]. We call $\vec{\eta}_{a}$ this fixed point. The subscript $n$ indicates (with some abuse of notation) that this fixed point depends on the finite instance, that is, the graph $\Gamma$, and $h_{ab}$. For the activities of the polymers, computed at the fixed point, we have the bounds $|K(\gamma)| \leq (2J)^{|\gamma|}$. Moreover the number of polymers $\gamma \ni a$ is (for each $a$) at most $\exp|a|/c_d$ with $c_d \geq 0$ a numerical constant depending only on $d$. Using also that the smallest polymer must have $|\gamma| \geq 3$, it is then easily shown that the left hand side of (8) is $O(J^n) << 1$. By standard methods [4] one can then estimate the sum over $M$ in (7) term by term, which yields

$$|f_{\text{corr}}(\vec{\eta}_{a})| \leq (1 + O(J^3)) \frac{1}{n} \sum_{a \in V} \sum_{\gamma \ni a} (2J)^{|\gamma|} < 1.$$ \hspace{1cm} (9)

Proposition 3.1: For $J < J_0(h)$ small enough, we have

$$\lim_{n \to +\infty} E[f_{\text{corr}}(\vec{\eta}_{a})] = 0.$$ \hspace{1cm} Proof idea: From (9) $\mathbb{E}[|f_{\text{corr}}(\vec{\eta}_{a})|] \leq (1 + O(J^3)) \mathbb{E}[\sum_{\gamma \ni a} (2J)^{|\gamma|}]$. Here $o$ is any specified node in the graph. In order to conclude it suffices to use the fact that on a random $d$-regular graph, with probability $1 - o(1)$, polymers have a size $|\gamma| \geq a_d \ln n$ ($a_d \geq 0$ a positive numerical constant).

IV. CYCLE LDPC CODES OVER THE BSC

Random $d$-regular graphs are equivalent to the LDPC($2,d$) ensemble of cycle codes. Code bits $x_{ab} = 0.1$ are attached to the edges $ab \in E$. In the spin language bits are $\sigma_{ab} = \pm 1$ and the parity check constraints are $\prod_{b \in \partial a} \sigma_{ab} = 1$. For definiteness we assume transmission over the BSC($p$), $p \in [0,\frac{1}{2}]$. Without loss of generality one can assume that the transmitted word is $(1,\ldots,1)$ so that MAP decoding is based on the posterior distribution (1) with

$$f_a(\sigma_{\partial a}) = \frac{1}{2}(1 + \prod_{b \in \partial a} \sigma_{ab}) \prod_{b \in \partial a} e^{\frac{h_{ab} - \sigma_{ab}}{2}}.$$ \hspace{1cm} (10)

Here $h_{ab}$ is the half-log-likelihood for the bit $\sigma_{ab} = \pm 1$, based on the channel output. The Shannon conditional input-output entropy and free energy are essentially equivalent, and related by the simple formula

$$\frac{1}{n} H(\vec{X}|\vec{Y}) = E_{\vec{X}}[f_{\vec{a}}(\vec{\eta})] - \frac{1 - 2p}{2} \ln \frac{1 - p}{p} \hspace{1cm} (11)$$
where $\mathbb{E}_q$ is the average over channel outputs (or the log-
likelihood vector).

We interested in the high noise regime where $p$ is close to
1/2. Therefore we seek solutions of the BP equations such that
$
\sup_{u \in E} |h_{ab}| \leq h$ where $h > 0$ is a fixed small number.
We assume that for $h$ small enough there exists a fixed point
of the BP equations for each finite instance. We denote it $\bar{\eta}_n$
as before. Note that assuming its unicity is not needed.

Proposition 4.1: Assuming the existence of a fixed point
$\bar{\eta}_n$ of the BP equations for $h$ small enough, we have
$\lim_{n \to +\infty} \mathbb{E}[\frac{1}{n} \ln Z_{\text{corr}}(\bar{\eta}_n)] = 0$.

In view of (2), (11) the proposition implies that the average
conditional entropy is given by the average of the Bethe
expression computed at the fixed point (for $|p - \frac{1}{2}| \ll 1$).

In order to prove the proposition we will use the identity

$$\ln Z_{\text{corr}}(\bar{\eta}) = \ln Z_p(\bar{\eta}) + \ln \left\{ 1 + \sum_{\gamma} \frac{K(\gamma)}{Z_p(\bar{\eta})} \right\}$$

(12)

where

$$Z_p(\bar{\eta} | \gamma) = \frac{1}{M!} \sum_{\gamma_1, \ldots, \gamma_M} \prod_{i=1}^M K(\gamma_i) \prod_{i < j} \mathbb{I}(\gamma_i \cap \gamma_j = 0)$$

and $Z_p(\bar{\eta}) \equiv Z_p(\bar{\eta}|\emptyset)$. This identity is derived by splitting the
sum over $\gamma_1, \ldots, \gamma_M$: in (6), into a sum where all polymers are small ($\mathbb{V}(\gamma_i) < n/2$), and a sum where there exists at least
one large polymer $(\exists i, |\gamma_i| \geq n/2)$; and by noting that when
there exists a large polymer it has to be unique.

We will need three lemmas.

Lemma 4.2: For $h$ small enough we have
$\lim_{n \to +\infty} \mathbb{E}[\frac{1}{n} \ln Z_p(\bar{\eta}_n)] = 0$.

Sketch of Proof: It is possible to estimate the activities
computed at the fixed point,

$$|K(\gamma)| \leq (1 - \alpha d \frac{d-2}{2} h^2)^{n_d(\gamma)} \prod_{i=2}^{d-1} (\alpha_i h^{d-i})^{n_i(\gamma)}.$$  

(14)

Here $0 < \alpha_d < 1$, and $\alpha_1 > 1$, $i = 2, \ldots, d - 1$ are fixed
numerical constants (that we can take close to 1). The $n_i(\gamma)$
denotes the number of nodes of degree $i$ in the polymer $\gamma$.

Estimate (14) is essentially optimal for $h$ small, as can be
checked by Taylor expanding $K(\gamma)$ in powers of $h_{ab}$.
Hard constraints manifest themselves in the factor $(1 - \alpha_d d \frac{d-2}{2} h^2)^{n_d(\gamma)}$
which is not small enough to compensate the entropic term
$e^{cd(\gamma)}$ in the convergence criterion. However for polymers of
size $|\gamma| \leq \frac{n}{2}$ we can use expander arguments to circumvent
this problem. Let $e(\gamma)$ the set of edges in $E$ connecting $g$
to $\Gamma \setminus g$.

We say that $\Gamma$ is an expander if for all $g \subset \Gamma$ with
$|g| \leq \frac{n}{2}$ we have $|e(\gamma)| \geq \kappa |\gamma|$. For all $d \geq 3$ [8]

$$P(\Gamma \text{ is an expander with } \kappa = 0.18 |d| = 1 - o_n(1)$$

(15)

Now note that for polymers $e(\gamma) \leq \sum_{i=2}^{d-1} (d - i) n_i(\gamma) \leq d \sum_{i=2}^{d-1} n_i(\gamma)$. Therefore we deduce thanks to (15) that
with high probability $\sum_{i=2}^{d-1} n_i(\gamma) \geq 0.18 |\gamma|$ and $K(\gamma) \leq (2h)^{0.18 |\gamma|}$ for $|\gamma| < \frac{n}{2}$ This is sufficient to control the
convergence criterion, and achieve the proof of this lemma
by methods similarly to the high temperature case.

Lemma 4.3: Fix $\epsilon > 0$. Then

$$P[|\gamma| \in \Gamma : e^{\epsilon n_{2}} \leq \frac{Z_p(\bar{\eta} | \gamma)}{Z_p(\bar{\eta})} \leq e^{\epsilon n_{2}}) \geq 1 - \frac{1}{\epsilon^2}.$$

(16)

This inequality is a fortiori valid for $g$’s replaced by $\gamma$’s in the sum.

Sketch of Proof: We denote by $K_n$ the complete graph
with $n$ vertices. By Markov’s inequality,

$$P \left[ \sum_{g \subset \Gamma} |K(g)| \geq \delta \right] \leq \frac{1}{\delta} \sum_{g \subset K_n} \mathbb{E}[|K(g)| | g \subset \Gamma]$$

(17)

Consider graphs $g$ with $n_i(g)$, $i = 2, \ldots, d$ fixed. Mackay [9]
provides a bound for the probability $P[g \subset \Gamma]$ of finding
a particular subgraph into a regular graph $\Gamma$. Namely for
$\frac{1}{2} \sum_{i=2}^{d} n_i(g) + 2d^2 \leq \frac{w}{4}$

$$P[g \subset \Gamma] \leq \frac{\prod_{i=2}^{d} \left( \frac{n_i(g)}{n_i(g)} \right)^{n_i(g) - n_i(g)} }{2^{d} \sum_{i=2}^{d} n_i(g)^{n_i(g)} \prod_{i=2}^{d} i^{n_i(g)}}$$

(18)

The number of subgraphs of $K_n$ with given $n_i(g)$ is

$$\frac{n!}{(n - \sum_{i=2}^{d} n_i(g))! \prod_{i=2}^{d} n_i(g)!} \times \frac{\prod_{i=2}^{d} n_i(g)!}{\sum_{i=2}^{d} n_i(g)!}$$

(19)

Replacing (18) in (17), using (19), setting $a_i = \frac{n_i}{n}$, and
performing an asymptotic calculation for $n$ large, we show (here $x \equiv (x_2, \ldots, x_d)$ and $\Delta \equiv \{x_2^2 \leq \sum_{i=2}^{d} x_i \leq 1\}$)

$$P \left[ \sum_{g \subset \Gamma} |K(g)| \geq \delta \right] \leq \frac{\prod_{i=2}^{d} x_i \log \left( n \left( 1 - \alpha D \frac{d}{2} h^2 \right)^{\sum_{i=2}^{d} x_i - 1} \right) }{\sum_{i=2}^{d} x_i \log \left( n \left( 1 - \alpha D \frac{d}{2} h^2 \right)^{-1} \right)}$$

(20)

$^3$Here $[m] = m(m - 1) \ldots (m - i + 1)$.
The large $n$ behavior of the integral asymptotic is computed by $f_n(\bar{x})$, and $g_n(\bar{x})$ gives sub-dominant contributions that do not concern us here. We have

$$f_n(\bar{x}) = \frac{1}{2} \sum_{i=2}^{d} i x_i \ln \frac{1}{2} \left( \sum_{i=2}^{d} i x_i \right) - \sum_{i=2}^{d} x_i \ln x_i (20')$$

$$(1 - \sum_{i=2}^{d} x_i) \ln(1 - \sum_{i=2}^{d} x_i) - \left( \frac{r}{2} - 2 r^2 \frac{\ln(\frac{\frac{r}{2}}{2})}{n} \right) + \left( \frac{r}{2} - \sum_{i=2}^{d} i x_i - 2 r^2 \frac{\ln(\frac{\frac{r}{2}}{2})}{n} \right) - \ln(\frac{\frac{r}{2}}{2} - 2 r^2 \frac{\ln(\frac{\frac{r}{2}}{2})}{n}) (21)$$

For $h$ small enough, in the domain $\Delta$, the exponent in (20) is

$$\frac{1}{n} \ln \left( 1 + \sum_{\gamma \in \Gamma} K(\gamma) \frac{Z_p(\bar{\gamma} | \gamma)}{Z_p(\bar{\gamma})} \right) \leq C''$$

(23)

Now suppose for a moment that there exist a positive constant independent of $n$ such that

$$\frac{1}{n} \ln \left( 1 + \sum_{\gamma \in \Gamma} K(\gamma) \frac{Z_p(\bar{\gamma} | \gamma)}{Z_p(\bar{\gamma})} \right) \leq C''$$

Then $B \leq C'' P[I_c]$. Setting $\zeta = \delta e^{2\alpha c}$, the above arguments imply

$$E \left[ \frac{1}{n} \ln \left( 1 + \sum_{\gamma \in \Gamma} K(\gamma) \frac{Z_p(\bar{\gamma} | \gamma)}{Z_p(\bar{\gamma})} \right) \right] \equiv A + B \leq \frac{1}{n} \ln(1 - \delta e^{2\alpha c}) + C e^{-\alpha c h^2} + 1 + o_n(1).$$

We are free to choose $\delta = e^{-\alpha c h^2}$ and $\epsilon = \alpha c h^2$ (lemmas 4.3, 4.4 hold) and this choice $A + B = o_n(1)$, which proves (22).

It remains to justify (23). From the convergence of the polymer expansion we deduce that $\frac{1}{n} \ln Z_p(\bar{\gamma}^n) = \text{bounded uniformly in } n$. From (1), (10) we easily show that $\frac{1}{n} \ln Z_p = \text{bounded uniformly in } n$. In the high noise regime the BP messages are bounded so that from (3) we deduce that $\frac{1}{n} \ln Z_p(\bar{\gamma}^n) = \text{bounded uniformly in } n$. Finally the triangle inequality implies $\frac{1}{n} \ln Z_p(\bar{\gamma}^n) - \ln Z_p(\bar{\gamma}^n)$ is bounded uniformly in $n$. This is precisely the statement (23).

V. CONCLUSION

The approach is quite general and can hopefully be generalized to standard irregular LDPC codes with bounded degrees and binary-input memoryless output-symmetric channels with bounded log-likelihood variables. This will be the subject of future work.

ACKNOWLEDGMENT

M.V acknowledges supported by the Swiss National Foundation for Scientific Research, Grant no 2000-121903. N.M benefited from discussions with M. Chertkov and R. Urbanke.

REFERENCES

Factoring linear trellises

David Conti
Claude Shannon Institute and
School of Mathematical Sciences
University College Dublin, Ireland
Email: david.conti@ucdconnect.ie

Nigel Boston
Departments of Mathematics and ECE
University of Wisconsin, USA
Email: boston@math.wisc.edu

Abstract—Koetter/Vardy proved in [9] the remarkable result that any linear trellis can be factored into elementary factors of a linear trellis are uniquely determined, extending a known result for minimal trellises ([4], [8], [11]). In so doing, we give a graphical method to compute all the spans and their multiplicities. We show how also to determine all the possible edge-labelings of the factors of a linear trellis, and give exact conditions for their uniqueness. These results can help to compute and classify all trellises for a given code.

I. INTRODUCTION

Linear trellises are amongst the most important graph representations of linear codes, both for theoretical and practical reasons. Towards the end of last millennium, due to the observation of striking low complexity achieved by nonconventional trellises ([11]), the interest expanded to the whole class of tail-biting trellises (of which conventional trellises can be seen as a particular case). As a consequence, in the recent years, linear tail-biting trellises has been the subject of major research within trellis theory ([9], [8], [4], [5], [10], [7]). The most important achievement is probably the factorization theorem proven in [9], which states that every linear tail-biting trellis is a product of elementary trellises. This fundamental theorem opened the road to other central works concerning minimal linear trellis representations of codes ([8], [4]).

In this paper we investigate further linear trellis factorizations and give graphical/combinatorial methods to compute such factorizations. We first prove that if we forget about edge-labels then unique factorization holds, which means that all the spans of factors and their multiplicities are uniquely determined. Our proof yields at the same time a method for computing all the spans and multiplicities. We show also how to determine all the possible edge-labelings of the factors of a linear trellis, and give exact conditions for their uniqueness. These results can help to compute and classify all trellises for a given code.

A. Basics on Trellises

All trellises considered will be over a fixed finite field \( \mathbb{F} \equiv \mathbb{F}_q \) and have a fixed length \( n \). Also, we want to do modular arithmetic on the coordinate indices of \( \mathbb{F}^n \), so \( \mathbb{Z}_n \equiv \mathbb{Z}/n\mathbb{Z} \) will be the index set of coordinates. A trellis (over \( \mathbb{F} \), and of length \( n \)) is a directed graph \( T = (V, E) \) together with a partition \( V = \bigcup_{i \in \mathbb{Z}_n} V_i \) indexed over \( \mathbb{Z}_n \), such that the edges are \( \mathbb{F} \)-labeled and can only go from \( V_i \) to \( V_{i+1} \), so that \( E \) has also a partition \( E = \bigcup_{i \in \mathbb{Z}_n} E_i \), where \( E_i \subseteq V_i \times \mathbb{F} \times V_{i+1} \). For formal reasons we also allow multiple edges in a trellis, i.e. each edge \( e \in E \) also has a multiplicity \( m(e) \geq 1 \). A trellis is conventional if \( |V_0| = 1 \).

Two trellises \( T = (V, E) \) and \( T' = (V', E') \) are isomorphic if there exists a bijection \( f : V \rightarrow V' \) such that \( e = (v, a, w) \in E \) if and only if \( f(v), a, f(w) \in E' \), \( m(e) = m(f(e)) \) for all \( e \in E \), and \( f(V_0) = V'_0 \). If by forgetting their labels \( T \) and \( T' \) are isomorphic as directed multigraphs, then we say that \( T \) and \( T' \) are structurally isomorphic again, we require \( V_0 \) to be sent to \( V'_0 \) and write \( T \cong T' \).

By a cycle of a trellis \( T \) we mean a closed directed path in \( T \) of length \( n \) starting and ending at \( V_0 \). The subset \( C(T) := \{ \text{edge-label sequences of cycles of } T \} \subseteq \mathbb{F}^n \) is the code represented by \( T \). A trellis is reduced if every edge and every vertex belongs to a cycle. A trellis is linear if it is reduced, the multiplicity function \( m : E \rightarrow \mathbb{N} \) on each edge \( E_i \) is a constant of the form \( q^j \) for some \( j \geq 0 \), and all \( V_i \)‘s have an \( \mathbb{F} \)-vector space structure such that \( E_i \) is an \( \mathbb{F} \)-subspace of \( V_i \times \mathbb{F} \times V_{i+1} \) for all \( i \). If \( T \) and \( T' \) are isomorphic then \( T \) is linear if and only if \( T' \) is linear. Also, if \( T \) is linear then so is \( C(T) \). In this paper we will consider only linear trellises, so, to simplify the terminology, from now on by a trellis we will always mean a linear trellis.

We will denote by \( T \) the set of trellises up to isomorphism, and by \( \mathcal{T} \) the set of unlabeled trellises, i.e. trellises up to structural isomorphism. Clearly \( T \) can be identified with the subset of all trellises having all edge-labels equal to 0, so, we see \( T \subseteq \mathcal{T} \). We have a projection map \( T \rightarrow \mathcal{T} \), which to each trellis \( T \) associates its underlying unlabeled trellis \( \mathcal{T} \) (equivalently, putting all edge-labels of \( T \) equal to 0).

For \( 0 \leq h \leq n \) and \( i \in \mathbb{Z}_n \), \( \{i, i+h\} \subseteq \mathbb{Z}_n \) is a span of length \( h \) of \( v \in \mathbb{F}^n \) if \( \text{supp}(v) \subseteq [i, i+h] \) and \( \{i, i+h\} \). If \( h < n \) we say that the span \( \{i, i+h\} \) is proper, and that it starts at \( i \) and ends at \( j = i+h \).
The degenerate span \( Z_n \) is a span of any \( v \in F^n \). Now, let \( s \) be a span of \( v \in F^n \). Let \( V_t := F \) for all \( t \in s \) and else \( V_t := 0 \). Choose \( v_t \in V_t \setminus \{0\} \) for all \( t \in s \), while for all \( t \notin s \) put \( v_t := 0 \). Let then \( E_t := F(v_t, v_{t+1}) \), i.e. \( E_t \) is the subspace of \( V_t \times F \times V_{t+1} \) generated by the vector \((v_t, v_t, v_{t+1})\). We also put \( m(e) := 1 \) for all \( e \in E \), except in the case \( v_0 = 0 \) (i.e. \( e \) is a fixed vertex). Not only does this depend on the choice of the \( v_t \)'s. It is clearly a (linear) trellis, and it satisfies \( v_0 = \lambda v_0 \) for \( \lambda \neq 0 \). This gives the elementary trellis \( v_0 \) (up to trellis isomorphism, it doesn’t depend on the choice of the \( v_t \)'s). This also is its identity, the spans (along with their multiplicities) appearing in the unique factorization holds, that is, if \( T_1 \otimes T_2 \otimes \ldots \otimes T_r = T'_1 \otimes T'_2 \otimes \ldots \otimes T'_r \), with \( T_i, T'_i \in \mathbb{T}_{E_{i}} \), then \( r = r' \) and, up to order, \( T_i = T'_i \) for all \( i \). In other words, the spans (along with their multiplicities) appearing in a factorization of a trellis \( T \) are uniquely determined.

It is easy to see that the multiplicity of the degenerate span \( Z_n \) is uniquely determined and is equal to the number of connected components of \( T \), so, the real problem is understanding what happens with proper spans. In what follows we will tackle this problem by a graph-theoretical approach, which yields also a method to compute the structural factorization.

Before going on to prove Theorem 2, we also inform the reader that we were recently told by Heide Gluesing-Luerssen that her PhD student Elizabeth Weaver has independently obtained uniqueness of spans of factors in the particular case of one-to-one trellises.

### A. Graph-theoretical approach

The graph-theoretical approach involves studying the earliest intersections of paths starting along different edges from a fixed vertex. Not only does this enable to prove unique factorization in \((\mathbb{T}, \otimes)\), but from the same intersection data one is also able to determine precisely all the spans of the factors.

Now, let us give some notation. Given a multiset \( S \), write \( m(x, S) \) for the multiplicity of \( x \) in \( S \) (in particular \( m(x, S) > 0 \) if and only if \( x \in S \)). If \( T \) is a trellis and \( e = (v, a, v') \) is an edge of \( T \), then \( h(e) := v' \) is the head of \( e \), and \( t(e) := v \) is its tail. A path \( p \equiv p_0 p_1 \ldots p_r \) in \( T \) is a sequence of edges \( p_0, p_1, \ldots, p_r \) in \( T \) such that \( h(p_0) = t(p_{r+1}) \), \( i = 0, \ldots, r-1 \). Now, let \( e \neq e' \) be two different edges of \( T \) such that \( t(e) = t(e') \). Define \( l(e, e') \) to be the smallest \( r \geq 0 \) such there exist two directed paths \( p = p_0 \ldots p_r \) and \( p' = p'_0 \ldots p'_r \) in \( T \) satisfying \( p_0 = e, p'_0 = e' \), and \( h(p_i) = h(p'_i) \). If there exist no directed paths satisfying those conditions then we put \( l(e, e') = \infty \). Define then the multiset \( I(e) := \{l(e, e') | e' \neq e, t(e') = t(e)\} \).

**Example 1.** Consider the unlabeled trellis

\[ e \rightarrow c \rightarrow e' \]

Then \( I(e) = \{\{1\}\} \), \( I(e') = \{\{2\}\} \), and \( I(e'') = \{\{1\}, \{1\}\} \).

Now, let \( T \) be a trellis and let \( e, e' \) be two edges with same tail. A priori, to compute \( l(e, e') \) one needs to compute the set of all possible couple of paths \( p, p' \) starting along
Let $e, e'$ and look for the earliest possible intersection. But in fact, by linearity (we are only considering trellises with linear structure) one can fix $p$ and let only $p'$ vary:

**Observation 1.** Let $T$ be a trellis and let $e, e'$ be two edges such that $t(e) = t(e')$. Fix a path $p$ such that $p_0 = e$. Then $l(e, e') = \min \{ r \mid \exists p' = p'_0 \ldots p'_r$ such that $p'_0 = e', h(p'_r) = h(p_r) \}$.

The highly symmetrical structure of (linear) trellises is further reflected in the following fundamental lemma:

**Lemma 1.** Let $T$ be a trellis of length $n$. Then:

- $l(e, e') \leq n - 1$ for any edges $e, e'$
- $I(e) = I(e')$ if $t(e), t(e') \in V_i$ for some $i$

In sight of this result, for a trellis $T$ and $i \in \mathbb{Z}_n$ it is legitimate to define $I_i(T) := I(e)$, where $e$ is any edge such that $t(e) \in V_i$.

The next lemma tells us that $I_i(T)$ is determined only by those factors of $T$ whose spans start at $i$.

**Lemma 2.** Let $T$ be a trellis, and let $T' \in \mathbb{T}_{El}$ be an elementary trellis with span not starting at $i$ or degenerate span. Then $I_i(T \otimes T') = I_i(T)$.

The above lemma is crucial for the following theorem, which is the key result:

**Theorem 3.** Let $T = T_1 \otimes \ldots \otimes T_r$, with $T_1, \ldots, T_r \in \mathbb{T}_{El}$. Fix $i \in \mathbb{Z}_n$, and let $L_i(T)$ be the multiset of span lengths of those $T_j$'s with (proper) span starting at $i$. Then for $l = 0, \ldots, n - 1$

$$\log_q \left( 1 + \sum_{j=0}^{l} m(j, I_i(T)) \right) = \sum_{j=1}^{l} m(0, L_i(T))$$

The above equations can be recursively solved for $m(j, L_i(T)), j = 0, \ldots, n - 1$, and the solution is unique. Therefore, since the left-hand side depends only on $T$, we conclude that Theorem 2 holds. Moreover, by computing all $I_i(T)$'s we are able to determine all the (proper) spans and their multiplicities in any factorization of $T$.

**Example 2.** Let $T$ be the unlabeled connected trellis

This trellis is $\mathbb{F}_2$-linear, its linear structure given by the shown $\mathbb{F}_2$-labels of vertices. Then one easily computes

- $I_0(T) = I(e_0) = \emptyset$
- $I_1(T) = I(e_1) = \{ 2 \}$
- $I_2(T) = I(e_2) = \emptyset$
- $I_3(T) = I(e_3) = \{ 3, 4, 4 \}$

- $I_4(T) = I(e_4) = \emptyset$

So, by Theorem 3, we get that $L_0(T) = L_2(T) = L_4(T) = \emptyset$, $L_1(T) = \{ \{ 3 \} \}$, $L_3(T) = \{ \{ 4, 5 \} \}$. Therefore $T = [3] \otimes [3, 1] \otimes [3, 2]$, as one can check.

**III. Factorization in $T$**

We have already pointed out that in $(\mathbb{T}, \otimes)$ unique factorization doesn’t hold, since the labels are not necessarily uniquely determined. Nevertheless, we give a method to find a legitimate labeling of a structural factorization of a trellis. We will also deduce precise conditions for a trellis $T$ under which unique factorization in $(\mathbb{T}, \otimes)$ holds.

Let $T \in \mathbb{T}$, and let $S(T)$ be the span multiset of $T$, which by Theorem 2 is uniquely determined. If $(i, j) \in S(T)$, i.e. $m((i, j), S(T)) \geq 1$, we say that $(i, j)$ is a span of $T$. Also, we put $s := [i, j]$ for a proper span $s = (i, j)$, and $\mathbb{Z}_n = \mathbb{Z}$.

By linearity there exists a zero vertex $z_i \in V_i$ for all $i$. Let $(i, j)$ be a proper span of $T$, and let $C_{i,j}(T)$ denote the code of all label-sequences of paths starting at $z_i$ and ending at $z_j$.

This is a code of length equal to the span length of $(i, j)$, but it is naturally a code in $\mathbb{F}^n$ by setting the coordinates outside the span $(i, j)$ equal to 0. It is not hard to see that it is linear, since $T$ is so. Also, for the degenerate span $\mathbb{Z}_n$ we put $C_{i,j}(T) := (C(T))$. Then we have the following:

**Theorem 4.** Let $T \in \mathbb{T}$, and let $s$ be a span of $T$ of multiplicity $r = m(s, S(T))$. Then $v_1[s] \otimes \ldots \otimes v_r[s]$ divides $T$ if and only if

$$Fv_1 + \ldots + Fv_r + \sum_{\nu \in S(T) \mid \nu \subseteq s} C_{\nu}(T) = C_{s}(T)$$

The following corollary extends the well known result that if there are no containments between different atomic spans of a code then the associated minimal conventional trellis factorizes uniquely, since all atomic generators are uniquely determined (up to scalar multiplication).

**Corollary 1.** Let $T = v_1[i_1, j_1] \otimes \ldots \otimes v_r[i_r, j_r]$. Then $v_1, \ldots, v_r$ are uniquely determined up to scalar multiplication and ordering (i.e. the factorization of $T$ is unique) if and only if there are no containments between different spans of $T$ and all their multiplicities are equal to 1.

**Example 3.** Label the edges of $T$ from example 2 as follows (by using dashed lines for 0’s and full lines for 1’s):

Thus labeled, $T$ is again $\mathbb{F}_2$-linear. Then one gets:

- $C_{1,3}(T) = \{ 00000, 01010 \}$
\begin{itemize}
  \item \(C_{3,1}(T) = \{00000, 01011\}\)
  \item \(C_{3,2}(T) = \{00000, 01011\}\)
\end{itemize}

Therefore by Theorem 4 and its corollary \( T \) has two (and only two) distinct factorizations,

\[
T = 01010\{1, 3\} \otimes 01011\{3, 1\} \otimes 01011\{3, 2\}
\]

\[
T = 01010\{1, 3\} \otimes 01011\{3, 1\} \otimes 00000\{3, 2\}
\]

Note also that \( T' = 01010\{1, 3\} \otimes 00000\{3, 1\} \otimes 01011\{3, 2\} \)

(depicted below) is a different trellis from \( T \), according to Theorem 4. In fact, in \( T' \) it is possible to go out from \( 0 \in V_3 \)
along two paths with all edge-labels equal to \( 0 \), and that meet at \( V_2 \), while this is not possible in \( T \).

\section*{IV. Applications}

The complexity of trellis-based decoding is directly proportional to the size of the chosen representing trellis, so, to
achieve low complexity it is important to search for the smallest trellis representations of codes. If trellis size is all what one is interested in, then obviously the way labels are arranged on a trellis doesn’t matter (as long as the trellis represents the wanted code), which implies that it is sufficient to classify all the trellis representations up to structural isomorphism. In [8] Koetter and Vardy show that up to structural isomorphism all the minimal trellises for a given code are encoded into a single matrix (characteristic matrix), and show how to efficiently compute that matrix (see also [4]).

On the other hand, the performance of iterative or LP decoding algorithms on a trellis is affected by so-called pseudocodewords, which makes it important to sort trellises also with respect to their pseudocodewords, as one wants to find trellises that yield few bad pseudocodewords ([3], [6]). In [2] we have given an example which shows that by changing labels in a trellis it is possible to change the set of yielded pseudocodewords and yet represent the same code. This means that to sort all the trellis representations of a given code with respect to pseudocodewords it is not sufficient to do a classification of trellises up to structural isomorphism. We need a complete classification of trellises. Theorem 2 and Theorem 4 help in that direction. Indeed they yield an exact method to check whether two trellises are isomorphic or not.

To see this recall that (by Theorem 1) to define a trellis we need to specify a span multiset and a list of vectors that is compatible with that span multiset. Theorem 2 tells us first of all that two different span multisets always yield two different trellises (since they are not even structurally isomorphic!). Once a span multiset (and so by Theorem 2 the unlabeled graph structure of the trellis) is chosen, Theorem 4 tells us the precise relations that hold among all the possible lists of vectors that give the same trellis. More precisely, if the chosen spans are \( s_1, \ldots, s_r \) with respective multiplicities \( m_1, \ldots, m_r \), and \( \{v_{ij}\}_{1 \leq i \leq r, 1 \leq j \leq m_i} \) are list of vectors associated to the spans, then it is easy to see from Theorem 4 that the corresponding trellises are isomorphic if and only if for all \( i = 1, \ldots, r \) the equation

\[
\sum_{h \in \mathbb{F}_{q^h}} \sum_{1 \leq j \leq m_h} F_{thj} = \sum_{h \in \mathbb{F}_{q^h}} \sum_{1 \leq j \leq m_h} F_{thj}
\]

holds.

\begin{remark}
It is easy to show that if a trellis \( T \) for a given code is optimal with respect to iterative or LP decoding (in the sense that it yields few bad pseudocodewords) then it must be one-to-one, i.e. the list of generating vectors of \( T \) must be a basis of the code. So, for iterative or LP decoding purposes, it is actually sufficient to do a complete classification of one-to-one trellises.
\end{remark}

\section*{Acknowledgments}

This work is part of the Ph.D. research of D. Conti supported by the Science Foundation Ireland grant 06/MI/006, and supervised by N. Boston.

\section*{References}

Information Theoretic Authentication and Secrecy Codes in the Splitting Model

Michael Huber
University of Tuebingen
Wilhelm Schickard Institute for Computer Science
Sand 13, D-72076 Tuebingen, Germany
Email: michael.huber@uni-tuebingen.de

Abstract—In the splitting model, information theoretic authentication codes allow non-deterministic encoding, that is, several messages can be used to communicate a particular plaintext. Certain applications require that the aspect of secrecy should hold simultaneously. Ogata–Kurosawa–Stinson–Saido (2004) have constructed optimal splitting authentication codes achieving perfect secrecy for the special case when the number of keys equals the number of messages. In this paper, we establish a construction method for optimal splitting authentication codes with perfect secrecy in the more general case when the number of keys may differ from the number of messages. To the best knowledge, this is the first result of this type.

I. INTRODUCTION

The development of quantum computer resistant cryptographic schemes and security technologies is of crucial importance for maintaining cryptographic long-term security and/or confidentiality of digital data, as classical cryptographic primitives such as RSA, DSA, or ECC would be easily broken by future quantum computing based attacks (e.g., [1], [2]). Application areas where cryptographic long-term security and/or confidentiality is strongly required include archiving official documents, notarial contracts, court records, medical data, state secrets, copyright protection as well as further areas concerning e-government, e-health, e-publication, et cetera.

To this end, one promising approach is the design of information theoretic authentication and secrecy systems (e.g., [3], [4]). The information theoretic, or unconditional, security model does not depend on any complexity assumptions and hence cannot be broken given unlimited computational resources. This guarantees not only resistance against future quantum computing based attacks but also perfect security in the classical world.

This paper considers authentication and secrecy codes in the splitting model. Splitting is of importance, for instance, in the context of authentication with arbitration [5] (i.e., protection against insider attacks in addition to outsider attacks). Ogata–Kurosawa–Stinson–Saido [6] have constructed optimal splitting authentication codes with perfect secrecy for the special case when the number of keys equals the number of messages.

In this work, we develop a construction method for optimal splitting authentication codes with perfect secrecy in the more general case when the number of keys may differ from the number of messages. To the best knowledge, this is the first result of this type. Our simple yet powerful approach is based on the notion of cyclic splitting designs and establishes an efficient method to construct optimal splitting authentication codes with perfect secrecy.

II. THE SPLITTING MODEL

We rely on the information theoretical, or unconditional secure, authentication model developed by Simmons (e.g., [7], [8]). Our notation follows [6], [9], [10]. In this model, three participants are involved: a transmitter, a receiver, and an opponent. The transmitter wants to communicate information to the receiver via a public communications channel. The receiver in return would like to be confident that any received information actually came from the transmitter and not from some opponent (integrity of information). The transmitter and the receiver are assumed to trust each other. An authentication code is sometimes called, for short, an A-code.

Let \( S \) denote a finite set of source states (or plaintexts), \( M \) a finite set of messages (or ciphertexts), and \( E \) a finite set of encoding rules (or keys). Using an encoding rule \( e \in E \), the transmitter encrypts a source state \( s \in S \) to obtain the message \( m = e(s) \) to be sent over the channel. The encoding rule is communicated to the receiver via a secure channel prior to any messages being sent. When it is possible that more than one message can be used to communicate a particular source state \( s \in S \) under the same encoding rule \( e \in E \), then the authentication code is said to have splitting. In this case, a message \( m \in M \) is computed as \( m = e(s, r) \), where \( r \) denotes a random number chosen from some specified finite set \( R \). If we define

\[
e(s) := \{ m \in M : m = e(s, r) \text{ for some } r \in R \}
\]

for each encoding rule \( e \in E \) and each source state \( s \in S \), then splitting means that \( |e(s)| > 1 \) for some \( e \in E \) and some \( s \in S \). In order to ensure that the receiver can decrypt the message being sent, it is required for any \( e \in E \) that \( e(s) \cap e(s') = \emptyset \) if \( s \neq s' \). For a given encoding rule \( e \in E \), let

\[
M(e) := \bigcup_{s \in S} e(s)
\]

denote the set of valid messages. A received message \( m \) will be accepted by the receiver as being authentic if and only if
A splitting authentication code is called \( c \)-splitting if
\[
|e(s)| = c
\]
for every encoding rule \( e \in E \) and every source state \( s \in S \).

We note that an authentication code can be represented algebraically by a \( |E| \times |S| \) encoding matrix with the rows indexed by the encoding rules \( e \in E \), the columns indexed by the source states \( s \in S \), and the entries defined by \( a_{es} := e(s) \).

We address the scenario of a spoofing attack of order \( i \) (cf. [11]): Suppose that an opponent observes \( i \geq 0 \) distinct messages, which are sent through the public channel using the same encoding rule. The opponent then inserts a new message \( m' \) (being distinct from the \( i \) messages already sent), hoping to have it accepted by the receiver as authentic. The cases \( i = 0 \) and \( i = 1 \) are called impersonation game and substitution game, respectively.

For any \( i \), we assume that there is some probability distribution on the set of \( i \)-subsets of source states, so that any set of \( i \) source states has a non-zero probability of occurring.

We address the scenario of a spoofing attack of order \( i \) (cf. [11]): Suppose that an opponent observes \( i \geq 0 \) distinct messages, which are sent through the public channel using the same encoding rule. The opponent then inserts a new message \( m' \) (being distinct from the \( i \) messages already sent), hoping to have it accepted by the receiver as authentic. The cases \( i = 0 \) and \( i = 1 \) are called impersonation game and substitution game, respectively.

For any \( i \), we assume that there is some probability distribution on the set of \( i \)-subsets of source states, so that any set of \( i \) source states has a non-zero probability of occurring.

We address the scenario of a spoofing attack of order \( i \) (cf. [11]): Suppose that an opponent observes \( i \geq 0 \) distinct messages, which are sent through the public channel using the same encoding rule. The opponent then inserts a new message \( m' \) (being distinct from the \( i \) messages already sent), hoping to have it accepted by the receiver as authentic. The cases \( i = 0 \) and \( i = 1 \) are called impersonation game and substitution game, respectively.

For any \( i \), we assume that there is some probability distribution on the set of \( i \)-subsets of source states, so that any set of \( i \) source states has a non-zero probability of occurring.

We address the scenario of a spoofing attack of order \( i \) (cf. [11]): Suppose that an opponent observes \( i \geq 0 \) distinct messages, which are sent through the public channel using the same encoding rule. The opponent then inserts a new message \( m' \) (being distinct from the \( i \) messages already sent), hoping to have it accepted by the receiver as authentic. The cases \( i = 0 \) and \( i = 1 \) are called impersonation game and substitution game, respectively.

For any \( i \), we assume that there is some probability distribution on the set of \( i \)-subsets of source states, so that any set of \( i \) source states has a non-zero probability of occurring.

We address the scenario of a spoofing attack of order \( i \) (cf. [11]): Suppose that an opponent observes \( i \geq 0 \) distinct messages, which are sent through the public channel using the same encoding rule. The opponent then inserts a new message \( m' \) (being distinct from the \( i \) messages already sent), hoping to have it accepted by the receiver as authentic. The cases \( i = 0 \) and \( i = 1 \) are called impersonation game and substitution game, respectively.

For any \( i \), we assume that there is some probability distribution on the set of \( i \)-subsets of source states, so that any set of \( i \) source states has a non-zero probability of occurring.

We address the scenario of a spoofing attack of order \( i \) (cf. [11]): Suppose that an opponent observes \( i \geq 0 \) distinct messages, which are sent through the public channel using the same encoding rule. The opponent then inserts a new message \( m' \) (being distinct from the \( i \) messages already sent), hoping to have it accepted by the receiver as authentic. The cases \( i = 0 \) and \( i = 1 \) are called impersonation game and substitution game, respectively.

For any \( i \), we assume that there is some probability distribution on the set of \( i \)-subsets of source states, so that any set of \( i \) source states has a non-zero probability of occurring.

We address the scenario of a spoofing attack of order \( i \) (cf. [11]): Suppose that an opponent observes \( i \geq 0 \) distinct messages, which are sent through the public channel using the same encoding rule. The opponent then inserts a new message \( m' \) (being distinct from the \( i \) messages already sent), hoping to have it accepted by the receiver as authentic. The cases \( i = 0 \) and \( i = 1 \) are called impersonation game and substitution game, respectively.

For any \( i \), we assume that there is some probability distribution on the set of \( i \)-subsets of source states, so that any set of \( i \) source states has a non-zero probability of occurring.

We address the scenario of a spoofing attack of order \( i \) (cf. [11]): Suppose that an opponent observes \( i \geq 0 \) distinct messages, which are sent through the public channel using the same encoding rule. The opponent then inserts a new message \( m' \) (being distinct from the \( i \) messages already sent), hoping to have it accepted by the receiver as authentic. The cases \( i = 0 \) and \( i = 1 \) are called impersonation game and substitution game, respectively.

For any \( i \), we assume that there is some probability distribution on the set of \( i \)-subsets of source states, so that any set of \( i \) source states has a non-zero probability of occurring.

We address the scenario of a spoofing attack of order \( i \) (cf. [11]): Suppose that an opponent observes \( i \geq 0 \) distinct messages, which are sent through the public channel using the same encoding rule. The opponent then inserts a new message \( m' \) (being distinct from the \( i \) messages already sent), hoping to have it accepted by the receiver as authentic. The cases \( i = 0 \) and \( i = 1 \) are called impersonation game and substitution game, respectively.

For any \( i \), we assume that there is some probability distribution on the set of \( i \)-subsets of source states, so that any set of \( i \) source states has a non-zero probability of occurring.

We address the scenario of a spoofing attack of order \( i \) (cf. [11]): Suppose that an opponent observes \( i \geq 0 \) distinct messages, which are sent through the public channel using the same encoding rule. The opponent then inserts a new message \( m' \) (being distinct from the \( i \) messages already sent), hoping to have it accepted by the receiver as authentic. The cases \( i = 0 \) and \( i = 1 \) are called impersonation game and substitution game, respectively.

For any \( i \), we assume that there is some probability distribution on the set of \( i \)-subsets of source states, so that any set of \( i \) source states has a non-zero probability of occurring.

We address the scenario of a spoofing attack of order \( i \) (cf. [11]): Suppose that an opponent observes \( i \geq 0 \) distinct messages, which are sent through the public channel using the same encoding rule. The opponent then inserts a new message \( m' \) (being distinct from the \( i \) messages already sent), hoping to have it accepted by the receiver as authentic. The cases \( i = 0 \) and \( i = 1 \) are called impersonation game and substitution game, respectively.

For any \( i \), we assume that there is some probability distribution on the set of \( i \)-subsets of source states, so that any set of \( i \) source states has a non-zero probability of occurring.

We address the scenario of a spoofing attack of order \( i \) (cf. [11]): Suppose that an opponent observes \( i \geq 0 \) distinct messages, which are sent through the public channel using the same encoding rule. The opponent then inserts a new message \( m' \) (being distinct from the \( i \) messages already sent), hoping to have it accepted by the receiver as authentic. The cases \( i = 0 \) and \( i = 1 \) are called impersonation game and substitution game, respectively.

For any \( i \), we assume that there is some probability distribution on the set of \( i \)-subsets of source states, so that any set of \( i \) source states has a non-zero probability of occurring.

We address the scenario of a spoofing attack of order \( i \) (cf. [11]): Suppose that an opponent observes \( i \geq 0 \) distinct messages, which are sent through the public channel using the same encoding rule. The opponent then inserts a new message \( m' \) (being distinct from the \( i \) messages already sent), hoping to have it accepted by the receiver as authentic. The cases \( i = 0 \) and \( i = 1 \) are called impersonation game and substitution game, respectively.

For any \( i \), we assume that there is some probability distribution on the set of \( i \)-subsets of source states, so that any set of \( i \) source states has a non-zero probability of occurring.

We address the scenario of a spoofing attack of order \( i \) (cf. [11]): Suppose that an opponent observes \( i \geq 0 \) distinct messages, which are sent through the public channel using the same encoding rule. The opponent then inserts a new message \( m' \) (being distinct from the \( i \) messages already sent), hoping to have it accepted by the receiver as authentic. The cases \( i = 0 \) and \( i = 1 \) are called impersonation game and substitution game, respectively.

IV. **Optimal Splitting Authentication Codes**

We state lower bounds on cheating probabilities for splitting authentication codes (cf. [12], [13]).

**Theorem 1:** In a splitting authentication code, for every \( 0 \leq i \leq t \), the deception probabilities are bounded below by
\[
P_{di} \geq \min_{e \in E} \frac{|M(e)| - i \cdot \max_{s \in S} |e(s)|}{|M| - i}.
\]

A splitting authentication code is called \( t \)-fold secure against spoofing if
\[
P_{d1} = \min_{e \in E} \frac{|M(e)| - i \cdot \max_{s \in S} |e(s)|}{|M| - i}
\]
for all \( 0 \leq i \leq t \).

We indicate a lower bound on the size of encoding rules for splitting authentication codes (see [10], and [14], [15] for the case \( t = 2 \)).

**Theorem 2:** If a splitting authentication code is \((t - 1)\)-fold secure against spoofing, then the number of encoding rules is bounded below by
\[
|E| \geq \prod_{i=0}^{t-1} \frac{|M| - i \cdot \max_{s \in S} |e(s)|}{|M| - i}.
\]

A splitting authentication code is called optimal if the number of encoding rules meets the lower bound with equality.
Corollary 1: In a $c$-splitting authentication code, 
\[ P_d \geq \frac{c(|S| - i)}{|M| - i} \]
for every $0 \leq i \leq t$.

Corollary 2: If a $c$-splitting authentication code is $(t - 1)$-fold secure against spoofing, then
\[ |E| \geq \frac{(|M|)}{c(|S|)} \]

Optimal splitting authentication codes can be characterized in terms of splitting designs (see [10], and [6] for the case $t = 2$) as follows.

Theorem 3: Suppose there is a $t$-$(v, b, l = cu, 1)$ splitting design with $t \geq 2$. Then there is an optimal $c$-splitting authentication code for $u$ equiprobable source states, having $v$ messages and $c(\binom{v}{t})/c^2(\binom{v}{t})$ encoding rules, that is $(t - 1)$-fold secure against spoofing. Conversely, if there is an optimal $c$-splitting authentication code for $u$ source states, having $v$ messages and $c(\binom{v}{t})/c^2(\binom{v}{t})$ encoding rules, that is $(t - 1)$-fold secure against spoofing, then there is a $t$-$(v, b, l = cu, 1)$ splitting design.

V. OPTIMAL SPLITTING AUTHENTICATION CODES WITH PERFECT SECRECY

In what follows, we are interested in optimal splitting authentication codes that simultaneously achieve perfect secrecy. According to Shannon [16], an authentication code is said to have perfect secrecy if
\[ p_B(s|m) = p_B(s) \]
for every source state $s \in S$ and every message $m \in M$, that is, the a posteriori probability that the source state is $s$, given that the message $m$ is observed, is identical to the a priori probability that the source state is $s$.

By introducing the notion of an external difference family (EDF) (which yields a certain type of a splitting design), Ogata–Kurosawa–Stinson–Saido [6, Thm. 3.4] have given a construction scheme for optimal splitting authentication codes with perfect secrecy in the special case when the number of keys equals the number of messages.

Theorem 4: Suppose there exists a $(v, c, 1)$-EDF over an Abelian group of order $v$, then there is an optimal $c$-splitting authentication code for $u$ equiprobable source states, having $v$ messages and $c$ encoding rules, that is one-fold secure against spoofing and simultaneously achieves perfect secrecy.

Example 1: An optimal 2-splitting authentication code for $u = 2$ equiprobable source states, having $v = 9$ messages and $b = 9$ encoding rules, that is one-fold secure against spoofing and achieves perfect secrecy can be constructed from a $2$-$(9, 9, 4 = 2 \times 2, 1)$ splitting design. Each encoding rule is used with probability $1/9$. An encoding matrix is given in Table 1.

In the following, we develop a construction method for obtaining optimal splitting authentication codes with perfect secrecy in the more general case when the number of keys may differ from the number of messages:

1. We first introduce the notion of a cyclic splitting design. Let $D = (X, B)$ be a $2$-$(v, b, l = cu, A)$ splitting design, and let $\sigma$ be a permutation on $X$. For a block $B_i = \{B_{i,1}, \ldots, B_{i,u}\} \in B$ given as in (ii) of Definition 1, define $B_i^\sigma := \{B_i^{\sigma_1}, \ldots, B_i^{\sigma_u}\}$, satisfying
\[ B_i^\sigma = B_i^1 \cup \cdots \cup B_i^u \]
with $|B_i^\sigma| = |B_i| = c$ and $|B_i^\sigma| = l = cu$. If $B^\sigma := \{B_i^\sigma : B_i \in B, 1 \leq i \leq b\} = B$, then $\sigma$ is called an automorphism of $D$. If there exists an automorphism $\sigma$ of order $v$, then $D$ is called cyclic. In this case, the point-set $X$ can be identified with $\mathbb{Z}_v$, the set of integers modulo $v$, and $\sigma$ can be represented by $\sigma : j \rightarrow j + 1$ (mod $v$). For a block $B_i = \{B_{i,1}, \ldots, B_{i,u}\}$, the set
\[ B_i + j := \{B_{i,1} + j (\text{mod } v), \ldots, B_{i,u} + j (\text{mod } v)\} \]
for $j \in \mathbb{Z}_v$ is called a translate of $B_i$, and the set of all distinct translates of $B_i$ is called the orbit containing $B_i$. If the length of an orbit is $v$, then the orbit is said to be full, otherwise short. A block chosen arbitrarily from an orbit is called a base block (or starter block).

For a cyclic $2$-$(v, b, l = cu, 1)$ splitting design to exist, a necessary condition is $v \equiv 1$ or $l (\text{mod } u(u - 1)c^2)$. When $v \equiv 1$ (mod $u(u - 1)c^2$) all orbits are full.

2. Let us assume that there exists a cyclic $2$-$(v, b, l = cu, 1)$ splitting design without short orbit. Then, by Theorem 3, there is an optimal $c$-splitting authentication code for $u$ equiprobable source states, having $v$ messages and $c(\binom{v}{t})/c^2(\binom{v}{t})$ encoding rules, that is one-fold secure against spoofing. Furthermore, when considering the corresponding $b \times u$ encoding matrix, it follows by constructional reasons from the underlying cyclic splitting design without short orbit that the code simultaneously achieves perfect secrecy under the assumption that the encoding rules are used with equal probability.

Hence, we have proved the following theorem.

<table>
<thead>
<tr>
<th>$s_1$</th>
<th>$s_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>c1</td>
<td>{1.2}</td>
</tr>
<tr>
<td>c2</td>
<td>{2.3}</td>
</tr>
<tr>
<td>c3</td>
<td>{3.4}</td>
</tr>
<tr>
<td>c4</td>
<td>{4.5}</td>
</tr>
<tr>
<td>c5</td>
<td>{5.6}</td>
</tr>
<tr>
<td>c6</td>
<td>{6.7}</td>
</tr>
<tr>
<td>c7</td>
<td>{7.8}</td>
</tr>
<tr>
<td>c8</td>
<td>{8.9}</td>
</tr>
<tr>
<td>c9</td>
<td>{9.1}</td>
</tr>
</tbody>
</table>

TABLE 1

SPLITTING AUTHENTICATION CODE WITH PERFECT SECRECY FROM A $2$-$(9, 9, 4 = 2 \times 2, 1)$ SPLITTING DESIGN.
Theorem 5: Suppose there is a cyclic 2-(v, b, l = cu, 1) splitting design without short orbit (that is, it holds that
\[ v \equiv 1 \mod u(u - 1)c^2 \]. Then there is an optimal c-splitting authentication code for \( u \) equiprobable source states, having
\( v \) messages and \( \binom{v}{c}/[v^2c(c-1)] \) encoding rules, that is one-fold secure against spoofing and simultaneously achieves perfect
secrecy.

Relying on some recent constructions of splitting designs (cf. [17, Sect. 3.2]), we give exemplarily a series of optimal
splitting authentication codes with perfect secrecy.

Example 2: (i) An optimal 2-splitting authentication code for \( u = 2 \) equiprobable source states, having
\( v = 17 \) messages and \( b = 34 \) encoding rules, that is one-fold secure against spoofing and achieves perfect secrecy
can be constructed from a cyclic 2-(17, 34, 4 = 2 \times 2, 1)
splitting design with base blocks \( \{\{1, 2\}, \{3, 5\}\} \) and
\( \{\{1, 2\}, \{11, 13\}\} \). Each encoding rule is used with
probability 1/34. An encoding matrix is given in Table

(ii) As generalization of (i), an optimal c-splitting authentication
code for \( u = 2 \) equiprobable source states, having
\( v = 2c^2 + 1 \) messages and \( b = (2c^2 - 1 + 1)n \)
encoding rules, that is one-fold secure against spoofing and
achieves perfect secrecy can be constructed from a
cyclic 2-(2c^2 + 1, 2c^2 - 1 + 1, 2c^2 - 2 - c + c + 1, 2c^2 h - (2c^2 - c) + c + 1, \ldots, 2c^2 h - (2c^2 - c) +
c(c - 1) + 1) \} \) for all \( 1 \leq h \leq n \).

(iii) Further examples of splitting authentication codes with
perfect secrecy, also for \( u > 2 \), can be obtained in the
same way from various further constructions of splitting
designs in [17, Sect. 3.2].

ACKNOWLEDGMENT

The author gratefully acknowledges support by the Deutsche
Forschungsgemeinschaft (DFG) via a Heisenberg grant
(Hu954/4) and a Heinz Maier-Leibnitz Prize grant (Hu954/5).

REFERENCES

Cryptography – CRYPTO 1999, ed. by M. J. Werner, Lecture Notes in
[4] M. Huber, Combinatorial Designs for Authentication and Secrecy Codes,
Foundations and Trends® in Communications and Information Theory,
codes with arbitration,” Designs, Codes and Cryptography, vol. 22,
designs and their applications to authentication codes and secret
porary Cryptology: The Science of Information Integrity, ed. by G. J.
Anti-Structure Problems

Ram Zamir
Department of Electrical Engineering-Systems
Tel Aviv University, Israel
zamir@eng.tau.ac.il

Abstract—The recent success of structured solutions for a class of information-theoretic network problems, calls for exploring their limits. We show that sum-product channels resist a solution by structured (as well as random) codes. We conclude that the structured approach fails whenever the channel operations do not commute (or for general functional channels, when the channel function is non decomposable).

Key words: sum-product channels, distributed coding, functional source coding, functional Gelfand-Pinsker problem, non-decomposable functions, commutativity, associativity.

I. INTRODUCTION

Structured codes can be effective, and significantly better than random codes, for various multiuser problems. Prominent examples include the well known Korner-Marton (KM) "modulo-two sum" problem [1], as well as more recent setups such as the "dirty" multiple-access channel (MAC) [2], the noisy linear network (along with the compute & forward relaying technique) [3], and more [4]. The effectiveness of structured codes, in particular linear or lattice codes, is due to a good match between their linear structure and the additive nature of the source or channel involved.

In the Korner-Marton problem, for example, the two components \((X, Y)\) of a doubly-symmetric binary source are encoded separately. The joint decoder is not interested in a full reconstruction of \(X\) and \(Y\), which are viewed as "helper sources"; rather the decoder is interested in their modulo-two sum \(X + Y\) (or Xor). Writing the statistical relation between \(X\) and \(Y\) as a modulo-additive noise channel

\[
Y = X + Z \tag{1}
\]

we can recast the problem as that of lossless reconstruction of the noise \(Z\) from separate encodings of \(X\) and \(Y\).

As shown by Korner and Marton, a linear structured coding scheme, which sends the syndromes of \(X^n\) and \(Y^n\) with respect to a suitable linear binary code, achieves the minimum possible rate of \(H(Z)\) - the entropy of \(Z\) - per each encoder. In contrast, a conventional random coding scheme cannot do better than to encode at a sum rate equal to the joint entropy of \(X\) and \(Y\). This corresponds to the Slepian-Wolf solution [5], i.e., to a lossless reconstruction of both \(X\) and \(Y\) at the decoder. The resulting sum rate can be therefore significantly higher than \(2H(Z)\) for highly correlated sources.

The binary KM problem can be generalized to a \(q\)-ary field, in which case a linear \(q\)-ary code replaces the linear binary code in the KM solution [6]. And it also has a quadratic-Gaussian version [7].

A dual example with a similar characteristics is that of the "doubly dirty" MAC. This channel extends Costa’s “writing on a dirty paper” problem [8], [9] to a MAC; i.e., an additive-noise channel with two inputs \(X_1\) and \(X_2\) and an output \(Y\) given by

\[
Y = X_1 + X_2 + S_1 + S_2 + \text{noise} \tag{2}
\]

where \(S_1\) and \(S_2\) are two interferences, each known as “side information” to one of the encoders. Addition in (2) is over some group in the discrete channel case, or the usual addition in the continuous case. The problem is made interesting by imposing input constraints upon \(X_1\) and \(X_2\), thus the encoders cannot simply subtract the interferences.

Similarly to the Korner-Marton problem, a linear/lattice pre-coding scheme (which subtracts the interference “modulo the code”) achieves the capacity region of this channel [10], [2].

And in contrast, the rates achieved by a more conventional random binning scheme vanish in the limit of strong interference signals.

This sharp discrepancy is due to the distributive nature of the side-information; if the knowledge of \(S_1\) and \(S_2\) were centralized - i.e., they were both known to one encoder or to the joint decoder, then random binning could be effective and (nearly) achieve capacity; see [2].

Sometimes structured codes are inferior to random codes. This situation occurs when the linear structure of the code causes ambiguity at the decoder; for example, the symmetric-rates point of the (clean) MAC capacity region, or of the Slepian-Wolf rate region.

In this short note we focus on another, perhaps obvious weakness of structured codes: they are sensitive to the structure of the channel. Specifically, we show that if the additive channel in (1) or in (2) is replaced by one involving both addition and multiplication, then structured codes - and in fact, any other coding scheme - are not effective.

II. SUM-PRODUCT KORNER-MARTON

Consider a generalization of the KM problem (1), where the statistical relation between the component sources is given by

\[
I_{X+Y} = I_{X} + I_{Y} \tag{3}
\]

In the discrete noiseless case the linear coding scheme is exactly optimal, while in the continuous case it is asymptotically optimal in the continuous high SNR case.

This problem can be resolved by using two different (linearly independent) linear codes [11].
\( X \rightarrow \text{enc} \xrightarrow{M} \text{dec} \stackrel{\uparrow}{\rightarrow} \hat{Z} = F(X, Y) \)

Fig. 1. Functional source coding with side information at the decoder.

the channel
\[ Y = A + B' \times B'' + C \quad (3) \]
where \( A, B', B'' \) and \( C \) are statistically independent, and \( B', B'' \neq 0 \) with probability one. All variables in (3) belong to a finite field \( F_q \) of size \( q \), and the + and \( \times \) are the sum and product operations over \( F_q \). Here \( A \) and \( Y \) are viewed as the "helper sources", \( C \) as the desired source, and \( B' \) and \( B'' \) as the "channel states". The classical KM problem (1) corresponds to the case where the channel states are deterministic; specifically, \( q = 2 \), \( A = X \) is uniform over \( \{0, 1\} \), \( B' = B'' = 1 \), and \( C = Z \).

In the centralized case, the equivalent channel state \( B = B' \times B'' \) is either known to the joint decoder (i.e., one encoder observes \( A \), the other encoder observes \( Y \), and the decoder has access to \( B \)), or to both encoders (i.e., one encoder observes \( (A, B) \), and the other encoder observes \( (Y, B) \)). It is not hard to show that in this case the compression rate is \( H(Z) \) per each encoder, independent of the state distribution, as in the classical KM problem.\(^3\)

Our focus is, however, on the de-centralized state case, where each of the channel states \( B' \) and \( B'' \) is available to a different encoder. The performance in this case can be bounded by the simplified setup shown in Fig. 1, where one of the helper sources is available (un-coded) as "side information" at the decoder. That is, there is only one encoder which observes \( X = (A, B) \), while
\[ Y = A + B \times C \]
is available at the decoder, who wishes to reconstruct \( Z = C \).

This latter problem is a special case of functional source coding \([6]\), where a function \( Z = F(X, Y) \) needs to be reconstructed from separate coded versions of \( X \) and \( Y \). The setup of Fig. 1 corresponds to the case where \( Y \) is encoded as "side information" to the decoder (or it is encoded at a rate greater than or equal to \( h(Y) \)), and where
\[
\begin{align*}
X &= (A, B), \quad Y = A + B \times C, \quad Z = C \\
&\text{and} \quad F(X, Y) = (Y - A)/B. \quad (4)
\end{align*}
\]

A precise definition of functional source coding with side information at the decoder is as follows. The encoding function is \( f : F_q^2 \rightarrow \mathcal{M} \), where the size of the message space \( \mathcal{M} \) is \( 2^nR \), with \( n \) being the code block length and \( R \) being the coding rate. The decoding function is \( g : \mathcal{M} \times F_q^n \rightarrow F_q^n \). The probability of error \( P_e \) is the probability that \( g(M, Y^R) \) is not equal to the vector \( Z^R \), where \( Z_i = F(X_i, Y_i), \quad i = 1 \ldots n \), and where \( M = f(X^N) \) is the encoded message. For a given memoryless double source \((X_1, Y_1), (X_2, Y_2), \ldots \) and a function \( F(\ldots) \), a rate \( R \) is said to be "achievable" if we can make \( P_e \) as small as desired for some functions \( f \) and \( g \), and large enough \( n \). Finally, \( R^* \) denotes the minimum achievable rate.

Clearly, the minimum achievable rate \( R^* \) satisfies
\[ H(X|Y) \geq R^* \geq H(F(X,Y)|Y) \quad (5) \]
where the LHS corresponds to the case where the decoder fully reconstructs \( X \) before computing \( F(X,Y) \), while the RHS corresponds to the case where the encoder also has access to \( Y \), so it can first compute \( F(X,Y) \) and then compress it. In the sum-product case (4), if \( A \) is uniform over \( F_q \), then the bounds (5) become
\[ H(B) + H(C) \geq R^* \geq H(C). \quad (6) \]
Note that in the classical KM problem \( B = 1 \), i.e., \( H(B) = 0 \); thus the bounds coincide, and the coding rate is merely the entropy of the desired variable \( C \).

Han and Kobayashi \([6]\) give necessary and sufficient conditions for the LHS of (5) to be tight.\(^4\) These conditions are satisfied in the sum-product case.

\textbf{Lemma 1.} In the sum-product (functional source coding) problem (4), \( R^* = H(X|Y) \). Thus, if \( A \) is uniform over \( F_q \), then \( R^* = H(B) + H(C) \).

\textit{Proof:} Follows since two different lines in \( F_q \) intersect in at most one point, implying the condition in [6, lem.1]. \textrm{\(\blacksquare\)}

This result implies that the minimum coding rate \( R^* \) is in general larger than the entropy of the desired variable \( C \), which is the rate in the classical KM setting (1). In fact, the "extra" rate can be as large as \( \log(q-1) \), for \( B \) which is uniform over \( F_q \setminus 0 \).

As a corollary from Lemma 1, it follows that for uniform channel states \( B' \) and \( B'' \) in the distributed coding setup of (3), the rate of each encoder is at least \( \log(q-1) + H(C) \). The interpretation is that the introduction of the multiplicative state variables breaks the structure of the classical KM problem; the states \( B' \) and \( B'' \) must be fully conveyed to the decoder before the linear structure of the channel can be utilized (by means of a linear "syndrome" coding) to encode the desired source \( C \).

\section{III. The Sum-Product Dirty MAC}
Consider next a modification of the dirty MAC problem (2), in which the channel output is given by
\[ Y = A' + A'' + B \times C \quad (7) \]
\(^3\)Regarding the former case \((B \) available at the decoder\), note that a random parity-check matrix \( H \) is "good" with high probability for the classical KM problem (1) (i.e., \( Z^n \) can be reliably decoded from the syndromes \( HX^n \) and \( HY^n \)); hence \( H(B^n) \) is "good" with high probability for the generalized KM problem (3). In the latter case, the encoders simply divide their observations by \( B \), hence get back to the classical KM problem.

\(^4\)They in fact consider a more general case where both \( X \) and \( Y \) are encoded.
where as in (3) all variables belong to a finite field $F_q$ of size $q$, and the $+$ and $\times$ are the sum and product operations over $F_q$. The inputs of this MAC are $A'$ and $A''$ (corresponding to $X_1$ and $X_2$ in (2)), while $B$ and $C$ are the channel state variables (corresponding to $S_1$ and $S_2$ in (2)). There is no additional noise, nor input constraints.

As in the sum-product KM, the centralized state case is easy: if both state variables $B$ and $C$ are known to one encoder, or are known to the joint decoder, then the product $B \times C$ can be simply subtracted; hence the sum capacity is $\log (q)$, as if the channel was noiseless.

The interesting setup is, again, the de-centralized state case. That is, each encoder has access to only one of the channel states, while the decoder is completely ignorant of the states. The capacity in this case is bounded from above by that of the single-user channel shown in Fig. 2, with

$$Y = A + B \times C.$$  \hfill (8)

Here there is a single encoder that has access to one of the states ($S_1 = B$), while the decoder has access to the second state ($S_2 = C$), where $C$ is independent of both the input $X = A$ and $B$.

A precise definition of encoding and decoding over such a channel is as follows. The encoding function is $f : M \times F_q^B \rightarrow F_q^y$, and the decoding function is $g : F_q^y \times F_q^m \rightarrow M$, where the size of the message space $M$ is $2^{R_q}$, $R$ being the coding rate. The error probability $P_e$ is the probability that $g(\mathbf{y}^n, S_2^n) \neq M$, where $\mathbf{y}^n$ depends on $\mathbf{x}^n$, $\mathbf{S}_1^n$ and $\mathbf{S}_2^n$, and where $\mathbf{y}^n = f(M, \mathbf{S}_1^n)$ for $M \in M$. A rate $R$ is said to be “achievable” if we can make $P_e$ as small as desired for some functions $f$ and $g$, and large enough $n$. Finally, the capacity $C$ is the highest achievable rate.

The sum-product channel (8) is, in fact, a deterministic channel, where the output $Y$ is a function of the input $X$, and the two states $S_1$ and $S_2$:

$$Y = f(X, S_1, S_2).$$  \hfill (9)

There is no additional noise in the channel, beyond the randomness of the two (known) states $S_1$ and $S_2$.

The setup of (9) is an instance of the Gelfand-Pinsker problem [9], i.e., a channel with non-causal side information at the encoder. Hence, it has a single letter solution of the form

$$C = \max I(U; Y, S_2) - I(U; S_1)$$  \hfill (10)

where the maximization is over a suitable set of auxiliary random variables $U$, and functions $X = X(U, S_1)$.

The structure of the function $f$ in (9) plays a key role in determining the capacity $C$. A favorable case is when $f$ has a composite form, where the dependence on the encoder variables $(X, S_1)$ is separate from the decoder state $S_2$.

**Lemma 2.** If the function $f : F_q^X \times F_q^X \times F_q^X \rightarrow F_q$ can be decomposed into $f(a, b, c) = f'(a, b) \cdot g(c)$, where $f'$ is invertible with respect to the first argument (i.e., the equation $y = f'(t, c)$ has a solution $t$ for every $y$ and $c$), then (10) is optimized by $U = G(X, S_1)$. If also $g$ is invertible with respect to the first argument, then the capacity is

$$C = \log (q)$$

and it is achieved by an input $p(x|s_1)$ that makes $G(X, s_1)$ uniform over $F_q$ for all values of $s_1$.

**Proof:** The first part follows from [13, sec. III.F], and the invertibility of $f$. See also [14].

The sum-product channel (8) clearly does not satisfy the first condition of the lemma, as addition and multiplication do not commute. In fact, this channel is much worse. To assess its capacity, we shall first establish a relation to a “minimum entropy” problem.

**Lemma 3.** The capacity of a deterministic two-state channel of the form

$$Y = X + F(S_1, S_2)$$  \hfill (11)

where $+$ denotes addition in $F_q$ and where $S_1$ and $S_2$ are available at the encoder and the decoder, respectively, is given by

$$C = \log (q) - \inf \frac{1}{n} H \left( g(S_1^n) + F(S_1^n, S_2^n) | S_2^n \right)$$  \hfill (12)

where the second term is the average conditional entropy given $S_2^n$, and where the infimum is over all code block lengths $n$, and functions $g : F_q^X \rightarrow F_q^n$.

**Proof:** Easy and will be omitted.

Although (12) is not a single-letter expression, it is sometimes easier for analysis than the Gelfand-Pinsker solution (10). Specifically, for the sum-product channel (8) we have:

**Theorem 1.** (Shany-Zamir [15]) For the case where $Y = X + S_1 \times S_2$, the minimum average conditional entropy in (12) is bounded by

$$\log \left( \frac{q}{2} \right) \leq H_{\min} \leq \log \left( \frac{q}{\frac{q}{2} - 1/q} \right).$$

The upper bound is achieved (for all $n$) by a quadratic per-letter function $g(s) = s^2$.

As a corollary from this theorem, we conclude that the capacity of the sum-product channel (8) is at most one bit.

$^5$A continuous version of this setup may be thought of as a channel with a fading interference [12].
for all $q$. This is quite disappointing when compared to the capacity of $\log(q)$, which is achievable in the centralized-state case. The same statement is true also for the sum-product dirty MAC (7); that is, the rate of each user is at most one bit.\footnote{Perhaps even the stronger statement - that the sum rate is at most one bit - is true.}

IV. DISCUSSION

The essence of the examples given in this paper is that the order of performing the sum and product operations matters; and in fact, they are very “different”. One aspect of this difference - which is related to the sum-product KM problem - is that the expression

$$a + b \times c$$

cannot be decomposed into the form: function $f$ (function $(a, b), c$) (not even approximately). A second aspect - related to the sum-product dirty MAC - is that it is impossible to find a function of $a = a(b)$ such that (13) would be only a function of $c$ (not even approximately).

In contrast, these two requirements are easily fulfilled if the expression in (13) is a pure sum $a + b + c$ (by the associativity of summation), or a pure product $a \times b \times c$ (by the associativity of multiplication).\footnote{Note that pure multiplicative versions of the generalized KM and DMAC problems can be solved using linear codes over a “logarithmic” domain.}

It would be interesting to explore further (and perhaps quantify) the information-theoretic aspects of function decomposition. Note that this question is almost “distribution free” (i.e., nearly independent of the probability distributions of sources and channels). A different aspect of “anti structure”, which is due to a “bad” noise distribution, can be found in [16].

ACKNOWLEDGMENT

I thank Yaron Shany for many interesting discussions about the sum-product channel. Thanks are also due to Aaron Wagner for an interesting discussion about the sum-product KM problems, and to Prakash Iswar and Sandeep Pradhan for pointing out the relation to the work of Han and Kobayashi.

REFERENCES

Real-Time Coding of Markov Sources over Erasure Channels: When is Binning Optimal?

Ashish Khisti and Farrokh Etezadi
University of Toronto
10 King’s College Road
Toronto, ON, Canada
Email: {akhisti, fetezadi}@comm.utoronto.ca

Mitchell Trott
HP Labs
1501 Page Mill Road
Palo Alto, California
Email: mitchell.trott@hp.com

Abstract—We study sequential coding of a Markov source process under error propagation constraints. The channel can erase up to $B$ packets in a single burst, but reveals all other packets to the destination. The destination is required to reproduce all the (vector) source sequences sequentially, except those that occur in a window of length $B+W$ following the start of the erasure burst. Our earlier work establishes upper and lower bounds on the compression rate as a function of $B$ and $W$. In this work we show that for the class of symmetric sources, if we restrict to a memoryless encoding function, then a binning based scheme is optimal. Our converse involves a drawing connection between the sequential coding problem and a multiuser source coding problem called Zig-Zag source coding with side information.

I. INTRODUCTION

A tradeoff between compression efficiency and error resilience is fundamental to any video compression system. In live video coding, an encoder observes a sequence of correlated video frames and produces a compressed bit-stream that is transmitted to the destination. If the underlying channel is an ideal bit-pipe, it is well known that predictive coding [1] achieves the optimum compression rate. Unfortunately in many emerging video distribution networks, such as peer-to-peer systems and mobile systems, packet losses are unavoidable. Predictive coding is highly sensitive to such packet losses and can lead to a significant amount of error propagation. Various techniques are used to practice prevent such losses. Commonly used video coding techniques use a group of picture (GOP) architecture, where intra-frames are periodically inserted to limit the effect of error propagation. Forward error correction codes can also be applied to compressed bit-streams to recover from missing packets [2], [3]. Modifications to predictive coding, such as leaky-DPCM [4], [5], have been proposed in the literature to deal with packet losses. The robustness of distributed video coding techniques in presence of packet losses has been studied in e.g., [6], [7].

Information theoretic analysis of video coding has received significant attention in recent times, see e.g., [8]–[10] and the references therein. These works focus primarily on the source coding aspects of video. The source process is a sequence of vectors, each of which is spatially i.i.d. and temporally correlated. Each source vector is sequentially compressed into a bit stream. The destination is required to recover the source vectors in a sequential manner as well. However all of these works assume an ideal channel with no packet losses. To our knowledge even the effect of a single isolated packet loss is not fully understood [11].

In an earlier work [12] we build upon [8], [9] and introduce an information theoretic framework to characterize the tradeoff between error propagation and compression rate. An encoder is revealed source vectors in a sequential manner and compresses them sequentially into channel packets that are then transmitted over a channel. An information theoretic notion of error propagation is defined and upper and lower bounds are obtained on the compression rate. The lower bound is based on a careful analysis of information flow during the decoding process whereas the upper bound is based on a binning technique. For a special class of sources, a new technique, prospliant coding is proposed, and shown to be optimal. However the optimal compression rate remains an open problem for a large class of sources including the binary symmetric Markov source.

In this paper we consider a class of symmetric Markov sources. For this class the minimum compression rate has not yet been characterized. Our main result in this paper is that if we restrict to the class of memoryless encoders, then the binning based scheme proposed in [12] is optimal. The converse is established by drawing a connection to a multiuser source coding problem called zig-zag source coding network [13]–[15].

II. PROBLEM STATEMENT

A. Source Model

We consider a semi-infinite stationary vector source process $\{s^t_n\}_{n \geq 0}$ whose symbols (defined over some finite alphabet $\mathcal{S}$) are drawn independently across the spatial dimension and from a first-order Markov chain across the temporal dimension, i.e., for each $t \geq 1$,

$$
\Pr( s^t_n = s^t_j | s^t_{n-1} = s^t_{j-1} ) = \prod_{j=1}^{n} p_{s^t_j | s^t_{j-1}}, \quad \forall t \geq 1.
$$

(1)

We assume that the prior distribution $p_{s^t_0}(\cdot)$ and $p_{s^t_0}(\cdot)$ are selected such that the underlying random variables $\{s^t_n\}_{n \geq 0}$ constitute a time-invariant and a first-order stationary Markov...
chain. Of particular interest in this paper is the class of symmetric sources where the underlying Markov chain is also reversible i.e., the random variables satisfy $p(s_i | s_{i-1}, s_{i-2}, \ldots, s_0) = p(s_{i-1} | s_{i-2}, \ldots, s_0)$, where the equality is in the sense of distribution [16]. Of particular interest to us is the following property satisfied for each $t \geq 1$.

$$p_{s_{t+1}, s_t}(s_{t+1}, s_t) = p_{s_{t-1}, s_t}(s_{t-1}, s_t), \quad \forall s_t, s_{t+1} \in S$$

(2)

i.e., we can “exchange” the source pair $(s^t_i, s^t_j)$ with $(s^t_{i-1}, s^t_j)$ without affecting the joint distribution. An important class of sources that are symmetric are the binary sources: $s^t_i = s^t_{i+1} \oplus z^t_i$, where $\{z^t_i\}_{i \geq 1}$ is an i.i.d. binary source process (in both temporal and spatial dimensions) with the marginal distribution $Pr(z^t_i = 0) = p$, the marginal distribution $Pr(s^t_i = 0) = Pr(s^t_{i+1} = 1) = \frac{1}{2}$ and $\oplus$ denotes modulo-2 addition.

### B. Rate-Recovery Function

A rate-$R$ causal encoder maps the sequence $\{s^t_i\}_{i \geq 0}$ to an index $f^t_i \in [1, 2^nR]$ according to some function

$$f^t_i = g^t_i(s^t_0, \ldots, s^t_i)$$

(3)

for each $i \geq 0$. A memoryless encoder satisfies $g^t_i(s^t_0, \ldots, s^t_i) = g^t_i(s^t_i)$ i.e., the encoder does not use the knowledge of the past sequences.

The channel introduces an erasure burst of size $B$, i.e. for some particular $j \geq 0$, it introduces an erasure burst such that $g^t_i = \ast$ for $i \in \{j, j+1, \ldots, j+B-1\}$ and $g^t_i = f^t_i$ otherwise. Upon observing the sequence $\{g^t_j\}_{j \geq 0}$ the decoder is required to perfectly recover all the source sequences using decoding functions

$$\hat{s}^t_i = g^t_i(g^t_0, g^t_1, \ldots, g^t_i), \quad i \notin \{j, \ldots, j+B-W-1\}.$$  

(4)

It is however not required to produce the source sequences in the window of length $B+W$ following the start of an erasure burst. We call this period the error propagation window. The setup is shown in Fig. 1.

A rate $R(B, W)$ is feasible if there exists a sequence of encoding and decoding functions and a sequence $s_u$ that approaches zero as $n \to \infty$ such that $Pr(s^t_i \neq \hat{s}^t_i) \leq s_u$ for all $i \notin \{j, \ldots, j+B-W-1\}$. We seek the minimum feasible rate $R(B, W)$ which we define to be the rate-recovery function. The following upper and lower bounds have been established in [12].

**Theorem 1 ([12]):** For any stationary first-order Markov source process the rate-recovery function satisfies

$$R^-(B, W) \leq R(B, W) \leq R^+(B, W)$$

where

$$R^-(B, W) = H(s_1 | s_0) + \frac{1}{W+1} I(s^t_B; s^t_{W+B+1} | s^t_0).$$

(5)

$$R^+(B, W) = H(s_1 | s_0) + \frac{1}{W+1} I(s^t_B; s^t_{B+W} | s^t_0)$$

(6)

Notice that the upper and lower bound coincide for $W = 0$ and $W \to \infty$, yielding the rate-recovery function in these cases. The upper bound is obtained via a memoryless binning based scheme. At each time the encoding function $f^t_i$ in (3) is obtained as the bin-index of an independent Slepian-Wolf codebook [17]. The rate expression for $R^+(B, W)$, which is equivalent to [12]

$$R^+(B, W) = \frac{1}{W+1} H(s^t_B + 1, \ldots, s^t_{W+B+1} | s^t_0)$$

(7)

guarantees that the decoder can recover $s^t_{j+B+W}$ following an erasure burst between $[j, j+B-1]$ using the $W+1$ bin indices $f^t_{j+B}, \ldots, f^t_{j+B+W}$ and the source sequence $s^t_{j-1}$ before the erasure.

In [12] some counter-examples are provided where the lower bound $R^-(B, W)$ (c.f. (5)) is tight and binning based upper bound $R^+(B, W)$ (c.f. (6)) is not optimal in general. Nevertheless such examples require a special structure and do not include many natural source models such as the binary symmetric sources. The optimal rate-recovery function for the class of symmetric sources remains open. In this paper we establish the optimality of binning based scheme if one restricts to the class of memoryless encoders.

**Theorem 2:** For the class of symmetric sources that satisfy (2) the rate-recovery function, restricted to the class of
memoryless encoders, is given by
\[ R(B, W) = \frac{1}{W+1} H(s_{B+1}, s_{B+2}, \ldots, s_{B+W+1} | s_0). \]  
(8)

Note that the achievability follows immediately from (7). Thus it only remains to show that the lower bound (5) needs to be improved. We have only been able to obtain this improvement for the class of memoryless encoders. For the general encoder structure (3) this remains an open problem. At first glance one may expect that the binning based scheme is always optimal for the class of memoryless encoders. This is however not true. Interestingly the prospicient encoders in [12] that improve upon the binning based lower bound are also memoryless. Our proof involves an interesting connection a multi-terminal source coding problem called zig-zag source coding [13]–[15]. In particular we develop a simple approach to lower bound the sum-rate of a zig-zag source coding network with symmetric sources that may of independent interest.

### III. PROOF OF THEOREM 2

The special case when \( W = 0 \) follows directly from (5). We only need to consider the case when \( W \geq 1 \). For simplicity in exposition we consider the case when \( W = 1 \). Then we need to show that
\[ R(1, W) = 1 \]
(9)
The proof for general \( W \geq 1 \) follows along similar lines and will be sketched briefly.

Assume that an erasure-burst spans time indices \( j - B, \ldots, j - 1 \). The decoder must recover
\[ s_{j+1}^B = \hat{g}_{j+1}(f_j, f_{j+1}). \]
(10)
From Fano’s inequality, we have,
\[ H(j, f_j, f_{j+1}) \leq n \alpha. \]
(11)
Furthermore if there is no erasure until time \( j \) then
\[ s_j^B = \hat{g}_j(f_j), \]
(12)
must hold. Hence from Fano’s Inequality,
\[ H(s_j^B | f_j) \leq n \alpha. \]
(13)
Our aim is to combine (11) and (13) to establish the following lower bound on the sum-rate
\[ R_j + R_{j+1} \geq H(s_{j+1} | s_j) + H(s_j | s_{j-1}). \]
(14)
The lower bound then follows since
\[ R \geq \max(R_j, R_{j+1}) \]
(15)
\[ R_j \geq \frac{1}{2} (H(s_j | s_{j-1}) + H(s_{j-1} | s_{j-2})) \]
(16)
\[ R_{j+1} \geq \frac{1}{2} (H(s_{j+1} | s_j) + H(s_j | s_{j-1})) \]
(17)
\[ = \frac{1}{2} H(s_{j+1}, s_j | s_{j-1}) = \frac{1}{2} H(s_{j+1}, s_{j+2} | s_0) \]
(18)
thus establishing (9).

To establish (14) we make a connection to a multi-terminal source coding problem in Fig. 2.

### A. Zig-Zag Source Coding

Consider the source coding problem with side information illustrated in Fig. 2(a). In this setup there are four source sequences drawn i.i.d. from a joint distribution \( p(s_j, s_{j-1}, s_{j-2}, s_{j-3}) \). The two encoders \( j \) and \( j+1 \) are revealed source sequences \( s_j^B \) and \( s_{j+1}^B \) and the two decoders \( j \) and \( j+1 \) are revealed sources \( s_j^B \) and \( s_{j+1}^B \). The encoders operate independently and compress the source sequences to \( f_j \) and \( f_{j+1} \) at rates \( R_j \) and \( R_{j+1} \) respectively. Decoder \( j \) has access to \( (f_j, s_j^B) \) while decoder \( j+1 \) has access to \( (f_{j+1}, s_{j+1}^B) \) and are interested in reproducing,
\[ s_j^B = \hat{g}_j(f_j, s_j), \]
(20)
\[ s_{j+1}^B = \hat{g}_{j+1}(f_{j+1}, s_{j+1}^B) \]
(21)
respectively such that \( \Pr(s_j^B \neq s_j^B) \leq \epsilon_n \) for \( i = j, j+1 \). When \( s_j^B \) is a constant sequence, the problem has been studied in [13], [15]. A complete single letter characterization involving an auxiliary random variable is obtained. Fortunately in the present case of symmetric sources a simple lower bound can be obtained using the following observation.

**Lemma 1**: The set of all achievable rate-pairs \( (R_j, R_{j+1}) \) for the problem in Fig. 2(a) is identical to the set of all achievable rate-pairs for the problem in Fig. 2(b) where the side information sequence \( s_j^B \) at decoder 1 is replaced by the side information sequence \( s_{j+1}^B \).

The proof of Lemma 1 follows by observing that the capacity region for the problem in Fig. 2(a) depends on the joint distribution \( p(s_j, s_{j-1}, s_{j-2}, s_{j-3}) \) only via the marginal distributions \( p(s_j | s_{j-1}) \) and \( p(s_{j-1} | s_{j-2}) \). When the source is symmetric the distributions \( p(s_j, s_{j-1}) \) and \( p(s_{j-1}, s_{j-2}) \) are identical. The formal proof will be omitted.

Thus it suffices to lower bound the achievable sum rate for the problem in Fig. 2(b). First upon applying the Slepian-Wolf lower bound to encoder \( j+1 \)
\[ nR_{j+1} \geq H(s_{j+1} | s_j^B, f_j) - n \alpha \]
(22)
and to bound \( R_j \)
\[ nR_j \geq H(f_j) = I(f_j; s_j^B, s_{j-1}^B) \]
(23)
\[ \geq H(s_j^B | s_{j-1}^B) - H(s_j^B | s_{j-1}^B, f_j) \]
(24)
\[ = H(s_j^B | s_{j-1}^B) - H(s_j^B | s_{j-1}^B, f_j) - n \alpha \]
(25)
\[ = H(s_j^B | s_{j-1}^B) - H(s_j^B | s_{j-1}^B, f_j) - n \alpha \]
(26)
where (23) follows by applying Fano’s inequality to since \( s_j^B \) can be recovered from \( s_{j+1}^B \) and hence \( H(s_j^B | s_{j-1}^B, f_j) \leq n \alpha \) holds and (24) follows from the Markov relation \( s_j^B \rightarrow s_j^B \rightarrow (f_j, s_{j-1}^B) \). Observe that (14) follows by summing (22) and (24).
B. Connection between Streaming and Zig-Zag Coding Problems

It remains to show that the lower bound on the Zig-Zag coding problem also constitutes a lower bound on the original problem.

Lemma 2: Suppose that the encoding function $f_j = \mathcal{F}_j(s_j^j)$ is memoryless. Suppose that there exist decoding functions $\hat{s}_j^j = \mathcal{G}_j(\hat{f}_j^j)$ and $\hat{s}_j^{n-1} = \mathcal{G}_{j+1}(f_{j+1}^{j+1}, f_j^{j+1})$ such that $\Pr(\hat{s}_j^j \neq s_j^j)$ and $\Pr(\hat{s}_j^{n-1} \neq s_j^{n-1})$ both vanish to zero as $n \to \infty$. Then

\[
H(s_j^j | s_{j-1}^j, f_j) \leq n h_n
\]

(25)

and

\[
H(s_j^{n-1} | s_{j-B+1}^j, f_j, f_{j+1}^j) \leq n h_n
\]

(26)

also hold.

We omit the proof due to space constraint. The conditions in (25) and (26) show that any rate that is achievable in the original problem is also achieved in the Zig-Zag source network. Hence a lower bound to the source network also constitutes a lower bound to the original problem.

C. Extension to Arbitrary $W > 1$

Finally we comment on the extension of the above approach to $W = 2$. We now consider three encoders $t \in \{j, j+1, j+2\}$. Encoder $t$ observes a source sources $s_t^t$ and compresses it into an index $f_t \in \{1, 2, ..., B\}$. The corresponding decoders are revealed $s_{j-1}^j$ for $t \in \{j, j+1\}$ and the decoder $j + 2$ is revealed $s_{j-B+1}^j$. By an argument analogous to Lemma 1 the rate region is equivalent to the case when decoders $j$ and $j+1$ are instead revealed $s_{j+1}^j$ and $s_{j+2}^j$ respectively. For this new setup it is easy to show that decoder $j + 2$ must reconstruct $(s_j^j, s_{j+1}^j, s_{j+2}^j)$ given $(s_j^j, f_j, f_{j+1}, f_{j+2})$. The sum rate must therefore satisfy $R_j + R_{j+1} + R_{j+2} \geq \frac{1}{W} \sum_{i=1}^{W} H(s_{j+i}^j | s_{j-i+1}^j, s_{j-i+2}^j, s_{j-B+1}^j)$. Using an extension of Lemma 2 we can show that the proposed lower bound also continues to hold for the original streaming problem. This completes the proof. The extension to any arbitrary $W > 1$ is completely analogous.

References


SuperNyquist Rateless Coding for Intersymbol Interference Channels

Uri Erez
Tel Aviv University, Ramat Aviv, Israel
Email: uri@eng.tau.ac.il

Gregory W. Wornell
Dept. EECS, MIT, Cambridge, MA
Email: gww@mit.edu

II. SYSTEM AND CHANNEL MODEL
We consider a linear dispersive Gaussian channel for which the complex baseband channel output takes the form

\[ g(t) = h(t) * x(t) + z(t), \]

where \( z(t) \) is additive white Gaussian noise (AWGN) with one-sided power spectral density \( N_0 \), and where \( x(t) \) is the input, which is subject to a power constraint \( \mathbb{E} \{ |x(t)|^2 \} \leq P \) and bandwidth constraint \( W \). The associated white-input capacity of the channel is

\[ C_{bw} = \int_{-W/2}^{W/2} \log \left( 1 + \frac{P|h(f)|^2}{N_0W} \right) df. \]

We consider pulse-amplitude modulation, whereby

\[ x(t) = \sum_n s[n] g(t - nT), \]

where \( T \) is the symbol duration and \( T_0 = 1/W \) is the Nyquist sampling time. The associated “over-signaling” ratio is thus \( L = T_0/T \). After matched filtering and sampling at the symbol rate, the equivalent discrete-time channel is

\[ g[n] = k[n] * s[n] + z[n], \]

where \( k[n] = k(nT), \) where \( k(t) = h^*(−t) * h(t) * g(−t)^* \) \( g(t), \) and where

\[ S_{zz}(e^{2\pi f}) = \frac{N_0}{2} K(e^{2\pi f}) \]

\[ = \frac{N_0}{2T} \sum_i |H(f/T + i/T)|^2 |G(f/T + i/T)|^2. \]

The pulse shape is required to be limited to system bandwidth \( W \), i.e., \( g(t) \) satisfies \( G(f) = 0 \) for \( |f| > W/2 \). To simplify our development, we largely restrict our attention to the case

\[ g(t) = \sin(t/T_0), \] with \( \sin(u) \triangleq \sin(\pi u)/\pi u. \]

Taking the symbols \( s[n] \) to be independent identically-distributed (i.i.d.) circularly symmetric complex Gaussian with power \( P/L \) results in a (proper) Gaussian random input signal...
x(t) with power P. It follows that the capacity of the discrete-time channel (3) is
\[ C_{[b/\text{SNQ symbol}]} = \int_{-1/2T}^{1/2T} \log \left( 1 + \frac{P|H(f)|^2 G(f)^2}{N_0} \right) df \]
\[ = \frac{T}{T_0} \int_{-1/2}^{1/2} \log \left( 1 + \frac{P}{N_0} \right) df, \] (5)
where the last equality follows from the fact that \( g(t) \) is bandlimited.

Note that for sinc modulation (4), \( x(t) \) has a flat power spectrum over the bandwidth \( W \), and the modulation achieves the white-input capacity (1) for any \( L \), i.e., (5) specializes to
\[ C_{[b/\text{SNQ symbol}]} = \frac{1}{T_0} \int_{-1/2}^{1/2} \log \left( 1 + \frac{P}{N_0} \right) df, \]
\[ = \frac{T}{T_0} \int_{-1/2}^{1/2} \log \left( 1 + \frac{P}{N_0} \right) df, \]
where the second equality holds for ideal sinc modulation.

Consider now packetized transmission where the packet size is large but otherwise plays no role in the analysis. We consider a simplified model where the channel response experienced throughout transmission of the \( m \)th packet, \( m = \ldots, M \), is linear time-invariant (LTI) but the impulse response, which we denote by \( h_m(t) \), may vary from packet to packet. The channel input-output relation for the transmission of the \( m \)th packet is therefore
\[ y_m[n] = s_m[n] * h_m[n] + z_m[n], \] (7)
where \( k_m[n] = k_m(nT) \) and \( h_m(t) = h_m(-t) = g^*(t) + g(t) \). Assuming discrete-time white-input transmission for all packets, it follows from (6), that the mutual information (in b/\text{SNQ symbol}) corresponding to each packet is
\[ C_{[m/\text{SNQ symbol}]} = \int_{-1/2T}^{1/2T} \log \left( 1 + \frac{P|H(f)|^2 G(f)^2}{N_0} \right) df. \]
\[ = \frac{T}{T_0} \int_{-1/2}^{1/2} \log \left( 1 + \frac{P}{N_0} \right) df, \]
where the second equality holds for ideal sinc modulation.

Upon receiving a set \( S \subseteq \{1, \ldots, M\} \) of packets, the aggregate mutual information is thus
\[ C(S) = \sum_{m \in S} C_m. \] (8)

Our aim is to design a low complexity coding and modulation scheme that (simultaneously) approaches \( C(S) \) for all sets \( S \subseteq \{1, \ldots, M\} \) without requiring the transmitter to have knowledge of the capacities \( C_m \). Rather, for any given chosen target rate \( R \), and no knowledge of the channel, transmission should be successful whenever \( C(S) > R \) holds for the received set of packets \( S \).

We proceed to describe the proposed rateless SNQ construction. All the signals \( s_m[n] \) are obtained from a single coded stream \( s[n] \) according to
\[ s_m[n] = v_m[n] s[n], \] (9)
where \( v_m[n] \) are sequences to be specified. The transmitted signal corresponding to packet \( m \) is thus
\[ x_m(t) = \sum_i s[n] v_m[n] g(t - iT). \]

Provided we choose the sequences \( v_m[n] \) so that the transmitted signals \( x_m(t) \) are statistically independent and the \( s_m[n] \) are white circularly-symmetric complex Gaussian processes, the mutual information corresponding to each packet remains \( C_m \) and furthermore the aggregate mutual information from the receipt of multiple packets is the sum of the individual ones.

A simple means to achieve this is by taking \( v_m[n] = e^{-j2\pi mn/L}. \) Accordingly, we define
\[ x_m[n] \triangleq x_m(nT) = \sum_i s[i] e^{-j2\pi mn/L} g[n - i], \] (10)
where \( g[n] = g(nT) = \text{sinc}(n/L) \), with \( g(t) \) as in (4). Using (10), we see that the transmit signals "shifted-back in frequency" in this case are
\[ \tilde{x}_m[n] \triangleq e^{j2\pi mn/L} x_m[n] = \sum_i s[i] g_m[n - i], \]
where \( g_m[n] = e^{-j2\pi mn/L} g[n]. \)

Clearly, requiring that the signals \( \{x_m(t)\} \) be mutually independent is equivalent to requiring that the associated discrete-time signals \( \{x_m[n]\} \) be. Furthermore, the latter holds if and only if \( \{\tilde{x}_m[n]\} \) are mutually independent. Therefore, it suffices to verify the last condition. Since the signals \( \tilde{x}_m[n] \) are jointly Gaussian and stationary, they are independent if their cross-spectra
\[ S_{\tilde{x}_m, \tilde{x}_n}(f) = S_{\tilde{s}, \tilde{s}}(e^{j2\pi f} g_m(f)) G_m(e^{j2\pi f} f) G^*_m(e^{j2\pi f} f) \]
\[ = \frac{1}{T^2} S_{\tilde{s}, \tilde{s}}(e^{j2\pi f}) \left( \frac{f + m_1/L}{T} \ mod \ 1 \right) \left( \frac{f + m_2/L}{T} \ mod \ 1 \right) \]
vanish. Since \( G(f/T) \) occupies no more than \( 1/L \) of the SNQ frequency band, it follows that there is no overlap between the frequency responses \( G((f + \mu/L)/T \ mod \ 1/T) \) for different values of \( \mu \), and hence \( S_{\tilde{x}_m, \tilde{x}_n}(e^{j2\pi f}) \) indeed vanishes for \( m_1 \neq m_2 \).

A. Receiver Architecture
A low-complexity receiver architecture suffices to approach the associated information-theoretic limits. In particular, specializing (7) to the case (9) with our choice \( v_m[n] = e^{-j2\pi mn/L} \), the equivalent "shifted back" channel model is
\[ \tilde{y}_m[n] \triangleq \tilde{y}_m[n] e^{j2\pi mn/L} = \tilde{h}_m[n] * s[n] + \tilde{z}_m[n], \] (11)
where \( \tilde{k}_m[n] = k_m[n] e^{j2\pi mn/L} \). Since these channels do not overlap in frequency, they may be added without loss, resulting in the effective scalar ISI channel

\[
\tilde{y}[n] = \sum_{m \in S} \tilde{k}_m[n] e^{j2\pi mn/L} = s[n] \star \left( \sum_{m \in S} \tilde{k}_m[n] \right) + \sum_{m \in S} \tilde{z}_m[n].
\]

For such ISI channels, the unbiased MMSE decision-feedback equalizer (DFE) is an information-lossless receiver structure \([3, 4]\). In particular, to approach capacity, one can use Guess-Vanarasi interleaving \([3]\) and a single (fixed-rate) base code designed for an AWGN channel. In essence, every symbol is replaced by a different codeword and thus the DFE decision device acts on codewords rather than symbols.

IV. MIMO-SNQ: Extending SNQ to MIMO Systems

A straightforward extension of the preceding architecture to a multi-input multi-output (MIMO) system, which we term MIMO-SNQ, is as follows. The particular channel model of interest is

\[
y_m(t) = H_m(t) * x_m(t) + z_m(t),
\]

where there are \( N_t \) transmit and \( N_r \) receive elements. In turn, with input of the form \( x_m(t) = \sum_n x_m[n] g(t - nT) \), the associated discrete-time channel, after applying a matrix matched filter, is

\[
y_m[n] = K_m[n] x_m[n] + z_m[n],
\]

where \( K_m[n] = K_m(nT) \) with \( K_m(t) = H_m^\dagger(-t) * H_m(t) \) for which MIMO-SNQ achieves zero capacity channel since a vector of all 1's is orthogonal to \( K_m[n] \).

We employ a single stream transmission architecture based on the application of time-varying DFT beamforming to a scalar signal \( s[n] \). Specifically, we assume that the transmitted signal corresponding to packet \( m \) is formed as \( x_m[n] = s[n] v_m[n] \), where \( v_m[n] = v[n] e^{-j2\pi mn/L} \) with

\[
v[n] = \begin{bmatrix} 1 & e^{-j2\pi n/N_1} & \cdots & e^{-j2\pi (N_1-1)n/N_1} \end{bmatrix}^T.
\]

The effective received signal for packet \( m \) is, after frequency shifting \([cf. (11)]\),

\[
y_m[n] = y_m[n] e^{j2\pi mn/L} = \sum_l K_m[l] v[n-l] s[n-l] + z_m[n],
\]

where \( \tilde{K}_m[n] = K_m[n] e^{j2\pi mn/L} \). Note that the effective channel \( (12) \) is a periodically varying MIMO-ISI channel with period \( N_t \). We refer to each of the \( N_t \) induced substreams as “phases.” As in the SISO case, we may employ a DFE at the receiver, but due to the time-varying nature of the effective channel, for each phase a different set of \( N_t \) feedforward filters is applied to the channel output vector sequence. Thus, the equalizer is also periodic with period \( N_t \).

Note the covariance matrix of the transmitted vector for our SNQ modulation is white. We conclude that for this modulation, the transmitted signal is white over all degrees of freedom as long as the oversampling rate satisfies \( L \geq N_t M \). However, this doesn’t guarantee capacity can be achieved. In particular, we associate with each of the \( N_t \) “phases” a signal-to-interference-plus-noise ratio (SINR) value corresponding to the associated DFE slicer input. Equivalently, we may associate with each such phase a corresponding capacity. Hence, while the sum of the per-phase capacities equals the white-input capacity of the MIMO channel, the per-phase capacities are in general not equal. Moreover, since the variation is unknown to the transmitter, in a Guess-Vanarasi transmission architecture, a fixed code rate is used, and thus the achievable rate is determined by the minimum of the per-phase capacities.

It is worth emphasizing that this SINR variation across phases is analogous to the SINR variation across streams in a V-BLAST system, in which independently coded streams are sent over the antennas \([5]\). For this reason, V-BLAST serves as a useful benchmark with which to compare the performance of SNQ modulation.

A. Parallel Channels

In some cases, MIMO-SNQ is strictly capacity achieving. For example, consider the special case of \( N \) parallel ISi channels. This model is essentially equivalent to using SNQ modulation for transmission over a block-varying ISI channel as considered in Section III, with the \( N \) parallel channels replacing the \( L \) consecutive blocks of the SISO ISI channel. As we have shown that SNQ modulation is an optimal scheme in such a scenario, it follows that MIMO-SNQ is optimal for the case of parallel channels.

B. Channels Without Temporal ISI

As another class of channels of interest, consider the special case in which there is no temporal ISI and only inter-channel interference (ICI) is present, i.e., \( H_m(t) = H_m \).

While for diagonal \( H_m \), MIMO-SNQ is capacity achieving, there exist other \( H_m \) for which MIMO-SNQ achieves zero rate. For example, if \( H_m \) is the (rank-one) matrix of all 1’s, there will exist an SNQ Nyquist substream that experiences a zero-capacity channel since a vector of all 1’s is orthogonal to \( v[n] \) for \( n \neq N_1 \), all \( l \). Hence, MIMO-SNQ achieves zero rate, while V-BLAST achieves a strictly positive rate. However, for all but such pathological \( H_m \), MIMO-SNQ supports a rate that grows with SNR. By contrast, it is well known that for all rank-one channel matrices V-BLAST performance is interference-limited, i.e., is bounded with increasing SNR.

More generally, when the channel matrix \( H_m \) is drawn from a random ensemble, its performance is on average never worse that V-BLAST, and has significant advantages, particularly when keeping in mind that in V-BLAST an ordering is forced in the detection process, while MIMO-SNQ requires no such ordering since the scheme is inherently more symmetric.

We consider the average throughput for an ensemble of \( H_m \) with i.i.d. circularly symmetric complex Gaussian entries. The resulting average throughput of MIMO-SNQ is depicted in Fig. 1, along with that for both fixed- and optimized-decoding-order V-BLAST. As the plot reflects, the performance
of MIMO-SNQ modulation lies in between the two and approaches the latter at high SNR.

We can also relate MIMO-SNQ performance to that of D-BLAST [6]. In particular, as is well known, D-BLAST can achieve capacity, but to do so requires a base code designed for time-varying channels. In that sense, MIMO-SNQ can also achieve capacity provided practical such base codes exist. However, when we require that a communication architecture has the property that the base code sees an AWGN channel, Fig. 1 reflects that MIMO-SNQ can perform as well as V-BLAST with an optimized decoding order. In contrast, when the same constraint is imposed on D-BLAST, the result is V-BLAST with a fixed decoding order.

\section*{C. Spatio-Temporal ISI Channels}

When there is also temporal ISI, MIMO-SNQ is even more attractive, as we next illustrate. We now consider a random MIMO channel model where the Nyquist-rate equivalent discrete-time matrix channel impulse response \( K_{\text{eq}}[n] \) is of finite length and each Nyquist-rate tap is drawn i.i.d. over spatial and time dimensions according to a circularly-symmetric complex Gaussian distribution. Fig. 2 depicts the expected (averaged over the ensemble) capacity of MIMO-SNQ for different channel lengths. We observe that the gap-to-capacity decreases as the channel length grows confirming that SNQ modulation is able to exploit the temporal diversity afforded by the channel.

Moreover, such behavior is not specific to such i.i.d. ensembles. Indeed, Table I describes the performance of MIMO-SNQ for a typical \( 2 \times 2 \) underwater acoustic communication channel realization from the recent KAM-11 experiment.\(^1\) Performance was numerically evaluated for an oversignaling rate of \( L = 2 \). In this case, the equivalent discrete-time (Nyquist-rate) baseband channel impulse responses are 100 taps long. As the table reflects, MIMO-SNQ is effectively capacity achieving for this channel, with a gap to capacity of less than 0.5 dB.

\begin{table}[h]
\centering
\caption{MIMO-SNQ Spectral Efficiency (b/s/Hz) on a Sample \( 2 \times 2 \) Underwater Acoustic Channel of Length 100 Taps}
\begin{tabular}{|c|c|c|c|c|c|c|c|}
\hline
SNR (dB) & 0 & 2 & 4 & 6 & 8 & 10 & 12 & 14 \\
\hline
\hline
Capacity & 0.95 & 1.31 & 1.76 & 2.30 & 2.94 & 3.68 & 4.51 & 5.41 \\
SNQ & 0.86 & 1.20 & 1.63 & 2.16 & 2.80 & 3.53 & 4.37 & 5.29 \\
\hline
\end{tabular}
\end{table}

\begin{thebibliography}{9}
\end{thebibliography}

\(^1\)The authors thank Qing He for providing this sample channel.
Successive Compute-and-Forward

Bobak Nazer
Boston University
ECE Department
Boston, MA 02215, USA
Email: bobak@bu.edu

Abstract—In prior work, we proposed the compute-and-forward framework for sending linear combinations of messages to relays. In this note, we extend the notion of successive interference cancellation to the compute-and-forward setting. We find that once a relay has decoded a linear combination, it can mix it with its channel output to create a new effective channel output. The resulting effective channel can be tuned so that it is more suitable for decoding a second linear combination than the original channel.

I. INTRODUCTION

The classical approach to communication over a wireless relay network treats interference between transmitters as a nuisance to be avoided. Typically, each relay observes a noisy linear combination of the transmitted codewords and attempts to decode one (or more) of them while treating the others as additional noise. Recent efforts have revealed that interference can in fact be exploited if we are willing to expand the set of decoding possibilities to include linear combinations of codewords. One natural approach, sometimes referred to as compute-and-forward, is to employ a lattice codebook so that integer combinations of codewords are themselves codewords [1]–[5]. Relays are then free to select integer coefficients that match the channel coefficients as closely as possible, thus reducing the effective noise and increasing the achievable rates.

Under the classical approach, a relay can employ successive interference cancellation to remove decoded codewords from its channel observation. This decreases the effective noise encountered in the next decoding step. In this paper, we devise an analogous technique for the compute-and-forward framework. After decoding a linear combination, a relay can combine it with its channel observation to obtain a new effective channel that is even better for decoding the next linear combination. For ease of exposition, we will focus on the case where each relay wants to recover just two linear combinations.

Owing to space limitations, we do not attempt a full survey of the literature. We refer interested readers to [2] for additional references pertaining to compute-and-forward and to [6], [7] for surveys of the closely related topic of physical-layer network coding.

II. PROBLEM STATEMENT

Our setting is nearly identical to that of [2] and we reproduce some of the key definitions below. For ease of exposition, we will limit ourselves to real-valued channels and symmetric rates. We will denote addition and summation over \( \mathbb{R} \) with + and \( \sum \), respectively, and use \( \oplus \) and \( \boxplus \) to denote the same operation over \( \mathbb{F}_p \).

Each transmitter (indexed by \( \ell = 1, \ldots, L \)) has a length-\( k \) message that is drawn independently and uniformly over a prime-sized finite field, \( w_\ell \in \mathbb{F}_p^k \). An encoder, \( E_\ell : \mathbb{F}_p^k \rightarrow \mathbb{F}_p^n \), then maps the message into a length-\( n \) codeword, \( x_\ell = E(w_\ell) \), which must satisfy the usual power constraint \( \|x_\ell\|^2 \leq nP \). The message rate is \( R = (k/n) \log p \).

Each relay (indexed by \( m = 1, \ldots, M \)) observes a noisy linear combination of the codewords,

\[
y_m = \sum_{\ell=1}^{L} h_{m\ell} x_\ell + z_m ,
\]

where the \( h_{m\ell} \in \mathbb{R} \) are the channel coefficients and \( z_m \sim \mathcal{N}(0, I) \) is i.i.d. Gaussian noise. Let \( h_m = [h_{m1} \cdots h_{mL}]^T \) denote the vector of channel coefficients. The goal is for each relay to recover two linear combinations of the messages of the form

\[
\begin{align*}
\mathbf{u}^{(1)}_m &= \bigoplus_{\ell=1}^{L} q_{m\ell}^{(1)} \mathbf{w}_\ell , \\
\mathbf{u}^{(2)}_m &= \bigoplus_{\ell=1}^{L} q_{m\ell}^{(2)} \mathbf{w}_\ell
\end{align*}
\]

where the \( q_{m\ell}^{(1)}, q_{m\ell}^{(2)} \in \mathbb{F}_p \) are finite field coefficients. To this end, each relay is equipped with a decoder, \( D : \mathbb{F}_p^n \rightarrow \mathbb{F}_p^L \times \mathbb{F}_p^k \), that produces estimates \( \hat{\mathbf{u}}^{(1)}_m \) and \( \hat{\mathbf{u}}^{(2)}_m \) of its desired linear combinations. We will say that the average probability of error is at most \( \epsilon \) if

\[
\mathbb{P}\left( \bigcup_m \{ \hat{\mathbf{u}}^{(1)}_m \neq \mathbf{u}^{(1)}_m \} \cup \{ \hat{\mathbf{u}}^{(2)}_m \neq \mathbf{u}^{(2)}_m \} \right) < \epsilon .
\]

To map between the real-valued linear combination provided by the channel and the desired finite field linear combinations, we will need a bit of additional nomenclature. Specifically, we will refer to \( u^{(1)}_m \) as the linear combination with coefficient vector \( \mathbf{a}_m = [a_{m1} \cdots a_{mL}]^T \in \mathbb{Z}^L \) if its finite field coefficients satisfy

\[
q^{(1)}_{m\ell} = [a_{m\ell}] \mod p .
\]

This is a slight abuse of notation. More formally, we should explicitly define a mapping between \( \mathbb{F}_p \) and \( \{0, 1, \ldots, p - 1\} \). See [2, Definition 6] for more details.
Similarly, we will refer to \( u^{(2)}_m \) as the linear combination with coefficient vector \( b_m = [b_{m1}, \ldots, b_{mL}]^T \in \mathbb{Z}^L \) if
\[
q^{(2)}_m = [b_{m\ell}] \mod p .
\]  
(5)

We will say that the computation rate region \( R(h_m, a_m, b_m) \) is achievable if, for any \( \epsilon > 0 \) and \( m \) large enough, there exist encoders and decoders, such that all relays can recover their desired linear combinations with average probability of error \( \epsilon \) so long as
\[
R < \min_m R(h_m, a_m, b_m) .
\]  
(6)

Note that the relays are free to choose which linear combinations to decode so long as (6) is satisfied.

### III. Nested Lattice Codes

One key requirement of our scheme is that all integer combinations of codewords must be afforded protection against noise. Nested lattice codes are a natural fit for this purpose. A lattice \( \Lambda \) is a discrete subgroup of \( \mathbb{R}^n \) with the property that if \( t_1, t_2 \in \Lambda \) then \( t_1 + t_2 \in \Lambda \). By construction, all of our lattices will contain the zero vector. A pair of lattices \( \Lambda, \Lambda_{\text{FINE}} \) is nested if \( \Lambda \subset \Lambda_{\text{FINE}} \).

A lattice quantizer is a function, \( Q_{\Lambda} : \mathbb{R}^n \to \Lambda \), that maps vectors to the nearest lattice point in Euclidean distance,
\[
Q_{\Lambda}(x) = \arg \min \|x - t\| .
\]  
(7)

The fundamental Voronoi region is the subset of points in \( \mathbb{R}^n \) that quantize to the zero vector, \( V = \{x : Q_{\Lambda}(x) = 0\} \). The modulo operation returns the quantization error with respect to the lattice,
\[
[x] \mod \Lambda = x - Q_{\Lambda}(x) ,
\]  
(8)

and satisfies the distributive law,
\[
[a[x] \mod \Lambda + b[y] \mod \Lambda] \mod \Lambda = [ax + by] \mod \Lambda ,
\]  

for any \( a, b \in \mathbb{Z} \).

A nested lattice code \( \mathcal{C} \) is created by taking the set of fine lattice points that fall within the fundamental Voronoi region of the coarse lattice, \( \mathcal{C} = \Lambda_{\text{FINE}} \cap V \). Erez and Zamir have shown that their exist nested lattice codes that can approach the capacity of a point-to-point Gaussian channel [8].

### IV. Compute-AND-Forward

In [2], we proposed the compute-and-forward framework as a way of communicating linear combinations of messages. Our focus was on the case where each relay decodes a single linear combination with coefficient vector \( a_m \). Define
\[
R_{CF}(h, a) \triangleq \frac{1}{2} \log^+ \left( \left( \|a_m\|^2 - \frac{\langle h_m, a_m \rangle^2 P}{1 + P\|h_m\|^2} \right)^{-1} \right)
\]
where \( \log^+(x) \triangleq \max(\log(x), 0) \).

**Theorem 1** ([2, Theorem 2]): For any set of channel vectors \( h_m \in \mathbb{R}^L \) and coefficient vectors \( a_m \in \mathbb{Z}^L \), the following computation rate region is achievable:
\[
R(h_m, a_m) = R_{CF}(h_m, a_m) .
\]  
(9)

We now provide a brief overview of the basic compute-and-forward encoding and decoding functions which will be useful in the proof of our main result. Using Construction A [8], [9], we select a pair of nested lattices \( \Lambda \subset \Lambda_{\text{FINE}} \) that can approach the capacity of a point-to-point Gaussian channel. It can be shown that there is a one-to-one map \( \phi \) between \( \mathbb{R}^L \) and the nested lattice code \( \mathcal{C} \) that preserves linearity (see [2, Lemma 5]). Using this mapping, the encoder chooses a lattice point \( t_\ell = \phi(w_\ell) \). It then applies a dither \( d_\ell \) that is drawn independent and uniformly over \( \mathcal{V} \) and transmits the result,
\[
x_\ell = [t_\ell - d_\ell] \mod \Lambda .
\]  
(10)

Relay \( m \) observes \( y_m \) and has access to every dither\(^2\). It scales its observation by the minimum mean-squared error (MMSE) coefficient
\[
\alpha_m = \frac{\langle h_m, a_m \rangle}{1 + P\|h_m\|^2}
\]  
(11)

and removes the dithers according to the desired coefficients \( a_m \ell \). Afterwards, it quantizes the result onto the fine lattice and takes the modulus with respect to the coarse lattice,
\[
\hat{\nu}_m^{(1)} = \left[ Q_{\Lambda_{\text{FINE}}} (a_m y_m + \sum_{\ell=1}^L a_m \ell d_\ell) \right] \mod \Lambda .
\]  
(12)

It can be shown that, with high probability, this is equal to
\[
\nu_m^{(1)} = \left[ \sum_{\ell=1}^L a_m \ell t_\ell \right] \mod \Lambda
\]  
(13)

so long as
\[
R < \min \frac{1}{2} \log^+ \left( \frac{P}{\alpha_m^2 + P\|a_m h_m - a_m \|^2} \right) .
\]  
(14)

Finally, the relay applies the inverse map to get its estimate \( \hat{u}_m^{(1)} = \phi^{-1}(\hat{\nu}_m^{(1)}) \). Assuming that \( \hat{\nu}_m^{(1)} = \nu_m^{(1)} \), it can be shown that \( \hat{u}_m^{(1)} = u_m^{(1)} \) (see [2, Lemma 6]).

### V. Successive Compute-And-Forward

Successive interference cancellation is a powerful technique for decoding several messages at a single receiver. Assume that, given the channel observation \( y_m \), a relay has correctly decoded \( x_i \). It can now completely remove the effect of \( x_i \) from its observation,
\[
y_m - h_m x_i = \sum_{\ell \neq i} h_m \ell x_\ell + z_m ,
\]  
(15)

which reduces the interference and makes it easier to decode the next codeword.

As it turns out, we can employ a similar technique when decoding several linear combinations. Assuming the relay has decoded \( \sum_{\ell} a_m \ell x_\ell \), it can create a new effective channel
\[
y_m + \gamma_m \sum_{\ell=1}^L a_m \ell x_\ell = \sum_{\ell=1}^L (h_m \ell + \gamma_m a_m \ell) x_\ell + z_m .
\]  
(16)

\(^2\)These dithers can be replaced with deterministic sequences.
By adjusting the effective channel coefficients, we can make it easier for the relay to decode its second linear combination, and thus increase the computation rate region. Note that unlike successive interference cancellation, it is not always optimal to subtract the recovered linear combination. Below, we develop a successive computation scheme that follows the concept outlined above. We begin by showing that we can always recover the real sum of codewords if we have access to the modulo sum and the dithers.

Remark 1: In [2, Theorem 12], we described a limited version of successive computation. The key drawback is that this scheme only allows for integer-valued $\gamma_m$, owing to the fact that it works directly with the modulo sum of codewords.

As part of the compute-and-forward scheme, the relay recovers an estimate $\hat{v}_m^{(1)}$ of the modulo linear combination of codewords $v_m^{(1)}$ from (34). The lemma below shows that this modulo sum can be used to recover the real sum $\sum_\ell a_m \xi_\ell$ that is needed for successive computation.

Lemma 1: The relay can make an estimate $\hat{s}_m$ of the real sum of codewords

$$
\hat{s}_m = \sum_{\ell=1}^L a_m \xi_\ell
$$

with vanishing probability of error, $\lim_{m \to \infty} P(\hat{s}_m \neq s_m) = 0$, so long as $R < R(h_m, a_m)$.

Proof: Since $R < R(h_m, a_m)$, we can use Theorem 1 to make an estimate $\hat{v}_m^{(1)}$ that is equal to $v_m^{(1)}$ with high probability. For the remainder of the proof, we will assume that this estimate is correct. First, the relay dithers this linear combination and takes the modulus with respect to $\Lambda$. This gives it access to a modulo combination of the dithered lattice points,

$$
\left[\hat{v}_m^{(1)} - \sum_{\ell=1}^L a_m \xi_\ell \right] \mod \Lambda
$$

$$
= \left[\sum_{\ell=1}^L a_m \xi_\ell \right] \mod \Lambda - \sum_{\ell=1}^L a_m \xi_\ell \mod \Lambda
$$

$$
= \sum_{\ell=1}^L a_m (\xi_\ell - \xi_\ell) \mod \Lambda = \left[\sum_{\ell=1}^L a_m \xi_\ell \right] \mod \Lambda.
$$

It then subtracts this quantity from $a_m y_m$.

$$
r_m = a_m y_m - \left[\sum_{\ell=1}^L a_m \xi_\ell \right] \mod \Lambda
$$

$$
= \sum_{\ell=1}^L a_m h_m \xi_\ell + a_m z_m - \sum_{\ell=1}^L a_m \xi_\ell + Q(\sum_{\ell=1}^L a_m \xi_\ell)
$$

$$
= Q(\sum_{\ell=1}^L a_m \xi_\ell) + a_m z_m + \sum_{\ell=1}^L (a_m h_m - a_m) \xi_\ell,
$$

to get a quantized version of the desired sum $s_m$ plus some effective noise with variance $\alpha_m^2 + P||\alpha_m h_m - a_m||^2$. To remove this noise, it applies the coarse lattice quantizer. This operation will be successful with high probability so long as the second moment of $\Lambda$ exceeds the effective noise variance, i.e., $P > \alpha_m^2 + P||\alpha_m h_m - a_m||^2$. Assuming that $R(h_m, a_m) > 0$, this condition holds and we have that

$$
Q_A(r_m) = Q_A\left(\sum_{\ell=1}^L a_m \xi_\ell \mod \Lambda\right)
$$

with high probability. Finally, since the relay knows the quantized sum as well as its quantization error, it can infer the desired real sum. Assuming that (21) holds, we have that

$$
\hat{s}_m = Q_A(r_m) + \sum_{\ell=1}^L a_m \xi_\ell \mod \Lambda
$$

$$
= \sum_{\ell=1}^L a_m \xi_\ell = s_m.
$$

Using the real sum of the codewords, we can construct a successive compute-and-forward scheme. Define

$$
R_{SCF}(h, a, b) \triangleq \frac{1}{2} \log^2 \left(\frac{P(\|b\|^2 - \|a\|^2)^2}{1 + P(\|h\|^2 - \|a\|^2)^2}\right)^{-1}
$$

Theorem 2: For any set of channel vectors $h_m \in \mathbb{R}^L$ and coefficient vectors $a_m, b_m \in \mathbb{Z}^L$, the following computation rate region is achievable:

$$
R(h_m, a_m, b_m) = \max(R_{AB}, R_{BA})
$$

$$
R_{AB} = \min(R_{SCF}(h_m, a_m), R_{SCF}(h_m, a_m, b_m))
$$

$$
R_{BA} = \min(R_{SCF}(h_m, b_m), R_{SCF}(h_m, b_m, a_m)).
$$

Proof: Fix an $\epsilon > 0$. The expressions $R_{AB}$ and $R_{BA}$ correspond to the two possible decoding orders. We will prove that $R_{AB}$ is achievable by first decoding the linear combination with coefficient vector $a_m$ and then that with $b_m$. The proof of $R_{BA}$ follows identically by exchanging the role of $a_m$ and $b_m$.

We employ the same encoding framework as in Theorem 1. Relay $m$ uses the same decoding framework to make an estimate $\hat{u}_m^{(1)}$ of $u_m^{(1)}$. For $n$ large enough, this estimate is incorrect with probability at most $\epsilon/3$ if

$$
R < \min_m R_{SCF}(h_m, a_m).
$$

As a byproduct of successful decoding, the relay will obtain a correct estimate $\hat{v}_m^{(1)}$ of $v_m^{(1)}$. Using Lemma 1, it makes an estimate $\hat{s}_m$ of $s_m = \sum_\ell a_m \xi_\ell$ that has probability of error at most $\epsilon/3$ for $n$ large enough. Below, we assume $\hat{s}_m = s_m$.

The relay removes the projection of $\hat{s}_m$ onto $y_m$ from $y_m$ to get

$$
r_m = y_m - a_m h_m \hat{s}_m
$$

$$
= \sum_{\ell=1}^L (h_m - a_m h_m) \xi_\ell + z_m
$$

$$
= \sum_{\ell=1}^L (h_m - a_m h_m) \xi_\ell + z_m
$$

105
Define \( g_{n\ell} = h_{n\ell} - \frac{a_{n\ell}}{\|a_{n\ell}\|} a_{n\ell} \) and \( g_m = [g_{m1} \ldots g_{mL}]^T \). It then forms a new effective channel observation
\[
\hat{y}_m = \beta_m r_m + \mu_m s_m
\]
and proceeds to decode the linear combination with coefficient \( h \) using Theorem 2. It is not possible to decode \( b_1 \) first as \( R_{SCF}(h_1, b_1) = 0 \). Decoding \( a_1 \) first requires
\[
R < \frac{1}{2} \log^+ \left( \frac{1 + 6P}{3 + 2P} \right) .
\]

After recovering \( a_1 \), the relay can adjust the channel and decode \( b_1 \) so long as
\[
R < \frac{1}{2} \log^+ \left( \frac{9}{24 + P} \right) .
\]

The example above demonstrates that successive compute-and-forward can make it possible to recover linear combinations that are not available via a direct application of the original compute-and-forward framework. In other words, the relay can first target a linear combination that is “easy” to decode and then use it to create a better effective channel for decoding the second linear combination.

From another perspective, successive compute-and-forward can be used to enlarge the computation rate region for decoding a single linear combination with coefficient vector \( b_m \). The relay should order all viable coefficient vectors \( \{b_m \} \), those satisfying \( \|a_m\|^2 \leq 1 + P\|b_m\|^2 \) by computation rate \( R_{SCF}(h_m, a_m) \) and set aside those \( a_m \) with rates larger than \( R_{SCF}(h_m, b_m) \). It can then calculate which pair \( (a_m, b_m) \) offers the highest rate using Theorem 2. Finally, it applies successive compute-and-forward for this pair and keeps only the second equation. Example 1 demonstrates that this procedure does indeed enlarge the rate region.

VI. GENERALIZATIONS AND EXTENSIONS

Following the framework in [2], successive compute-and-forward can be generalized to include complex-valued channel models as well as unequal message rates. One can also envision extending this technique to the case where each relay may want more than two linear combinations. In this case, the linear combinations obtained thus far should be mixed together with the original channel observation to create a new effective channel for the next targeted linear combination.

REFERENCES


Tunable Sparse Network Coding

Soheil Feizi1, Daniel E. Lucani2, Muriel Médard1

1Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA
2Instituto de Telecomunicações, DEEC, Faculdade de Engenharia da Universidade do Porto, Porto 4200-465, Portugal
Email: sfeizi@mit.edu; dlucani@fe.up.pt; medard@mit.edu

Abstract—A fundamental understanding of the relationship between delay performance and complexity in network coding is instrumental towards its application in practical systems. The main argument against delay-optimal random linear network coding (RLNC) is its decoding complexity, which is $O(n^3)$ for $n$ original packets. Fountain codes, such as LT and Raptor codes, reduce the decoding load on the receiver but at the cost of introducing additional, non-negligible delay. The source of this increased delay is the inherent sparsity of the code, which significantly reduces the impact of a new coded packet, i.e., the probability of a packet to be linearly independent from the knowledge at the receiver, as we approach the end of the transmission (when few degrees of freedom are missing). Thus, the additional overhead is mainly due to the transmission of the last data packets. Our key observation is that switching gears to denser codes as the transmission process progresses could considerably reduce the delay overhead while maintaining the complexity advantages of a sparse code. We propose tunable sparse network coding as a dynamic coding mechanism with a code structure with two regions: a sparse region, with various levels of sparsity, and a dense region, where packets are generated as per RLNC. We characterize the problem in multicast sessions on general networks and illustrate trade-offs in especial cases of interest. We also present a novel mechanism to perform efficient Gaussian elimination for sparse matrices that guarantees linear decoding complexity with high probability.

I. INTRODUCTION

Network coding constitutes a disruptive concept for the operation of communication networks [1] that has evolved from an information theoretic result for achieving capacity in multicast to become an enabler of a wide variety of applications, including communications in ad-hoc networks, data gathering in sensor networks, and data storage. One of the key features of network coding is that it encourages the mixing (coding) of data packets at intermediate nodes, rather than limiting intermediate nodes to store and forward packets. Under this premise, it is no longer required for the system to keep track of which packets have been received: receivers need only accumulate enough coded packets in order to recover the information. Ref. [2] and [3] show that linear codes over a network are sufficient to achieve multicast capacity, while Ref. [4] proved that randomly generated linear codes achieve capacity with high probability.

One of the main arguments against the use of RLNC is that its decoding complexity is $O(n^3)$, where $n$ constitutes the number of original packets. Sparse end-to-end erasure correcting codes, such as LT [5] and Raptor codes [6], reduce the decoding load on the receiver but at the cost of introducing additional, non-negligible delay. More importantly, they lack RLNC’s capability to use re-encode at intermediate nodes. Sparse end-to-end erasure correcting codes tend to choose sparsity in a static manner. Although this sparsity helps to reduce the complexity, it also introduces additional delay overheads. In particular, this inherent (and static) sparsity reduces the impact of a coded packet as the transmission session progresses. In fact, the additional overhead of these codes is mainly due to the transmission of the latter packets.

We revisit the idea of using sparse coding to reduce the decoding complexity, but using a fundamentally different approach in which i) we tune the level of sparsity as the transmission process evolves, and ii) we transition to RLNC for the last transmissions. This tuning process can reduce the delay overhead by using denser codes towards the end of the transmission, while maintaining complexity advantages of a sparse code. We call this scheme Tunable Sparse Network Coding. Unlike RLNC, in tunable sparse network coding the coding coefficients are chosen sparsely, i.e., mostly zero. As the session progresses, these coefficients become denser, i.e., statistical properties of the coding coefficients vary in time.

There are three key ideas in tunable sparse network coding:

- **Sparse coding is more beneficial at the beginning of a transmission session.** Since destination nodes have only received a few degrees of freedom (independent linear combination of the original packets), any sparsely coded packet will constitute a new degree of freedom (or innovative packet) with high probability.
- **Dense coding is required towards the end of the sessions for fast completion** because dense coded packets are innovative with high probability, while sparse coded packets are innovative with low probability.
- **Sparse coding translates in reduced complexity.** A decoder can exploit an encoding matrix with a large number of zero coefficients for improved complexity.

This paper proposes a framework for studying our network coding mechanism over packet erasure networks to analyze the trade-off between the delay performance (i.e., mean number of transmissions) and the decoding complexity of multicast sessions. Finally, we introduce a simple, yet powerful algorithm to organize a sparse matrix in order to provide a linear decoding complexity with high probability.

II. MODEL AND PRELIMINARIES

Consider a general multicast network with one source and several receivers. We model the network as a directed graph, with independent edge erasure probabilities. This assumption may be relaxed in future studies, but it is a fair assumption in many networks. Suppose the source node has $n$ packets to transmit to a subset of the nodes in the network, i.e., a multicast session. Suppose $X$ is a $n \times 1$ vector of source packets whose $i^{th}$ component, $X_i$, represents the $i^{th}$ source packet in the finite field $\mathbb{F}_q$. Suppose the minimum min-cut between
each receiver and source is \( m \). Therefore, the network can deliver \( m \) packets at each transmission round. A transmission session is complete when all destination nodes receive \( n \) source packets. Throughout this paper, we assume \( m < n \). Hence, multiple transmission rounds of \( m \) coded packets are required in a session. Each transmission round is indexed by \( t \).

Let us leverage some of the ideas from the algebraic framework for linear network coding from Ref. [3] to model our problem. For the case of no erasures, the receiver \( i \) gets \( A_i X \), where \( A_i \) is a \( m \times n \) full-rank matrix (since the min-cut rate is \( m \)) after each round. \( A_i \) is called the network coding matrix associated with the receiver \( i \) and can be decomposed into two matrices \( B \) and \( G_i \) (i.e., \( A_i = G_i B \)). \( B \) is a \( m \times n \) precoding matrix which is applied at the source node. This matrix is the same for all receivers. \( G_i \) is a \( m \times n \) matrix representing the effect of performing network coding at intermediate nodes from the source node to the receiver \( i \).

Now, consider the case of having packet erasures over the network links. Since some packets are lost as they traverse the network, the min-cut rate of this network is smaller than the error-free min-cut rate of the network (i.e., \( m \)). For receiver \( i \), define a \( m \times m \) diagonal matrix \( P_i \), whose \( j \)-th component on the diagonal (i.e., \( P_{i,j} \)) is zero with probability \( p_j \), and one with probability \( 1 - p_j \). Probabilities \( p_j \) depend on edge erasure probabilities. Hence, at the end of each transmission round, the destination node \( i \) receives \( P_i A_i X \). In other words, some of coded packets are erased over the network. Considering multiple transmission rounds, \( Y(t) = P_i A_i(t) X \) represents the received coded packets at receiver \( i \) in round \( t \).

### III. Tunable Sparse Network Coding

In this section, we introduce a framework for studying a time-varying coding scheme, with particular emphasis on the proposed case of tunable sparse network coding. A coded packet is uniformly coded when its coding coefficients are uniformly chosen from a finite field \( \mathbb{F}_q \). On the other hand, a coded packet is \( k \)-sparse if it contains exactly \( k \) non-zero coding coefficients. Non-zero coefficients are chosen uniformly from \( \mathbb{F}_q - \{0\} \). Finally, a coded packet is \( k \)-sparse with high probability (w.h.p.) when, with probability \( 1 - k/n \), each coding coefficient is zero, otherwise, it is chosen uniformly from \( \mathbb{F}_q - \{0\} \). For simplicity, consider that \( q \) is sufficiently large, although our techniques extend naturally to small \( q \).

Define \( \rho(A_i(t)) \), the density of a matrix \( A_i(t) \), as the ratio of its non-zero components. A matrix is dense if this ratio is high, e.g., RLNC's \( A_i(t) \) is dense w.h.p. If the ratio is low, the matrix is sparse. In a tunable sparse network coding scheme, the density of \( A_i(t) \) is tuned depending on the transmission round index \( t \). The key idea is that, at the beginning of the transmission session, receivers have only a few coded packets making a sparsely coded packet innovative to the receivers w.h.p. However, towards the end of the transmission session, sparsely coded packets are innovative with low probability because destination nodes have received most of the required degrees of freedom (dof). Hence, \( \rho(A_i(t)) \) should be increased, i.e., densely coded packets should be transmitted.

Depending on the function \( \rho(A_i(t)) \) and its control method, we can classify various tunable sparse network coding schemes. If the density control of \( A_i(t) \) is performed without having feedback from receivers, we say the coding scheme is open-loop. Otherwise, it is a closed-loop scheme. By having different time dependencies of elements of \( A_i(t) \), a variety of coding schemes, such as window-based coding, sliding window-based codings, and generation-based encoding, can be characterized and studied with our framework.

This work focuses on an open loop approach with prior knowledge of the network’s erasure probabilities. In particular, we characterize the delay and complexity performance from the perspective of a receiver and for the special case where the error-free min-cut rate is one. However, the analysis extends seamlessly to (i) multiple receivers with an error-free min-cut rate \( m \) greater than one, and (ii) close-loop schemes, because our analysis relies on characterizing receivers’ performance given the number and type of received coded packets.

#### A. From a Receiver’s Perspective

A tunable sparse network coding scheme with \( k \)-sparsely coded packets for \( m = 1 \) can be described as follows: the source node first transmits \( n \) uncoded packets, where some of these packets are lost due to erasures. These uncoded packets are followed by sparse packets. We shall study two different approaches: i) transmission of \( n_k \) \( k \)-sparse coded packets ,i.e., with exactly \( k \) non-zero coefficients chosen at random, where each non-zero coefficient is chosen uniformly from \( \mathbb{F}_q - \{0\} \), which we call deterministic density, and ii) transmission of \( n_k \) \( k \)-sparse coded w.h.p., which we call randomized density. Finally, \( n_{unt} \) uniformly coded packets are transmitted.

We analyze the effect of \( n_k \) on the delay performance and the decoding complexity for the general case of several levels of sparsity. Without loss of generality, we restrict our delay performance achievability result in Theorem 3 to the case of one type of sparsely coded packets, i.e., only one \( k \neq 1 \) for which \( n_k > 0 \). This result extends seamlessly to the case of different levels of sparsely coded packets.

#### B. Delay Performance

This subsection characterizes the probability that a newly received, sparse coded packet is innovative under specific density distributions. This problem is key to modeling the general problem of a multicast session over a general network, where at each transmission time \( t \) up to \( m \) sparse packets will arrive to a receiver. In the general network case, the choice of precoding and the coding within the network as well as the link erasures will determine the sparsity of the received coded packets for that time \( t \). Considering a scheme with multiple levels of sparsity, a transmission of \( g(d_k|np) \) sparse packets for
a level \( k \) yields \( d_k \) dof, when \( n_p \) dof were previously received. The following lemma characterizes \( g_d(d_k|n_p) \) and \( g_r(d_k|n_p) \) for deterministic and randomized sparsity, respectively.

**Lemma 1.** For a receiver in a multicast session with \( n_p < n \) previously received degrees of freedom,

\[
g_d(d_k|n_p) = \sum_{i=n_p}^{n_p+d_k} \frac{1}{(n_p+j)!} \left( \frac{n}{n_p+j} \right)^j, \quad \text{if } k < (1-\alpha)n. \tag{1}
\]

\[
gr(d_k|n_p) = \sum_{i=n_p}^{n_p+d_k} \frac{1}{(n_p+j)!} \left( \frac{n}{n_p+j} \right)^j, \quad \text{if } k > (1-\alpha)n. \tag{2}
\]

**Proof:** First we compute \( g_d(d_k|n_p) \) for the case of deterministic density and then point out the necessary changes for \( g_r(d_k|n_p) \). Suppose at time \( t \), we have \( i \) dof at the receiver. For the case of deterministic density, a \( k \)-sparse coded packet is not innovative with probability \( \left( \frac{n-1}{n} \right)^j \), which represents the probability of all the \( k \) non-zero coefficients being chosen amongst packets that do not increase the knowledge space of the receiver. We model the reception of a new packet as the Markov chain shown in Figure 1. The expected number of required sparsely coded packets to have \( d_k \) new dof, conditioned on having \( n_p \) innovative packets at time \( t \) is Eq. (1).

For the case of randomized density, a \( k \)-sparser coded packet is not innovative with probability \( (1-k/n(1-i/n))^n \) and again model this as a Markov chain to show Eq. (2).

The following corollary provides approximate expressions for Eq. (1) and (2) for \( n \) is large enough and \( d_k << n - n_p \).

**Corollary 2.** For large \( n \) and \( d_k << n - n_p \). If \( (n_p/n)^k << 1 \) then, \( g_d(d_k|n_p) \approx d_k(1 + (1 - n_p/n)^k) \). If \( (1 - k/n)(1 - n_p/n))^n << 1 \) then, \( g_r(d_k|n_p) \approx d_k(1 + (1 - k/n)(1 - n_p/n))^n \).

**Proof:** Under conditions of Corollary 2, we have that

\[
g_d(d_k|n_p) \approx \sum_{i=n_p}^{n_p+d_k/n} \frac{n}{n_p} \left( \frac{n}{n_p+i} \right)^i \left( 1 - \frac{i}{n} \right)^i \approx \sum_{i=n_p}^{n_p+d_k/n} \frac{i^i}{(n_p+i)!} \left( \frac{n}{n_p+i} \right)^i.
\]

We use similar approximations for \( g_r(d_k|n_p) \).

Define a \( (n_k,n_{uni}) \) tunable sparse network coding scheme as a scheme that transmits \( n \) systematic packets, \( n_{uni} \) uniformly coded packets, and \( n_k \) \( k \)-sparse coded packets. This scheme is achievable if the receiver is expected to recover all \( n \) packets. The following result characterizes achievability for an erasure probability \( \alpha \) as seen by the receiver. For this result, define \( f(d_k) \geq d_k \) as the number of sparse coded packets to have \( d_k \) innovative ones in average. \( f(d_k) - d_k \) represents the performance loss due to using sparse network coding instead of RLNC with large \( q \).

**Theorem 3.** For a network with a single receiver and \( m = 1 \), a \( (n_k,n_{uni}) \) tunable sparse network coding scheme is achievable where \( n_k = f(d_k) | d_k \) and \( d_k + (1-\alpha)n_{uni} = \alpha n \). For a deterministic density of \( k < (1-\alpha)n \), \( f(d_k) = g_d(d_k|(1-\alpha)n) \).

For a randomized density, \( f(d_k) = g_r(d_k|(1-\alpha)n) \).

**Fig. 2.** Example of proposed decoding algorithm (Algorithm 1)

**Proof:** Since the expected value of \( n_p \) is \( (1-\alpha)n \) we compute having \( f(d_k) = E[g_d(d_k|D_1)] \) and \( f(d_k) = E[g_r(d_k|D_2)] \) using Lemma 1. We conclude the proof following a typical argument for large \( n \) since the distribution of \( n_p \) is given by a binomial distribution with success probability \( 1-\alpha \).

**C. Complexity Analysis**

We present a simple algorithm that reorders the matrix to avoid operations in the forward pass w.h.p. for the processing of sparse packets. This has the crucial effect of avoiding additional density to be created in sparse packets, which keeps the number of operations in the backward pass for the sparse packets as \( O(d_k) \). Define \( P_1 \) as the \( i \)-th original packet, \( C_j(Z) \) as the set of coded packets of \( j \)-sparse packets drawn from \( Z \) subset of the original packets, and \( S_1 \) as the set of packets in a 1-sparse combination. Define \( Sum(F, Z) \) as the set of original packet of subset \( Z \) used only once in the set of coded packets \( F \). Finally, we define \( \Omega \) as the set of all \( n \) original packets.

Fig. 2 (a) illustrates the case of a transmission using tunable sparse network coding. For simplicity, we have assumed that received coded packets were either uncoded, i.e., from the systematic region, or sparse, although for this example \( n \) is kept small for illustration purposes. Fig. 2 (a) shows that packets \( P_1 \) and \( P_2 \) were received uncoded and we use them to substract their contribution from coded packets with a non-zero coefficient for \( P_1 \) and \( P_2 \), i.e., all non-zero elements of the first two columns. The algorithm counts the number of times a packet corresponding to columns on the lower right-hand side, as defined by the dashed lines, is involved in a linear combination. Involvement of the packet in combinations below the dashed line are not counted. Rows and columns shall be reorganized so that packets with a single occurrence will be in the upper left corner, as defined by the dashed lines in Fig. 2 (b). At this point we repeat the process until no single-occurrence packets are identified or until all sparse coded packets have been processed. In Fig. 2 (b), it is clear that the latter is attained because packet \( P_3 \) is involved in only one linear combination below the dashed line. The algorithm is stated in the following.

**Algorithm 1**

**STEP 0:** \( R(0) = \{C_k(\Omega) : k > 1\} \) \( C(0) = \{P_j : P_j \notin S_1\} \)

**STEP i:** If \( Sum(R(i),C(i)) \neq \emptyset \)

\( R(i+1) = R(i) - C_k(Sum(R(i),C(i))) \) if \( k > 1 \),

\( C(i+1) = C(i) - Sum(R(i),C(i)) \)

\( i \leftarrow i + 1 \). Go to next step

**Else** Stop. Proceed with Standard Gaussian Elimination
We compare the following schemes:

- **3-sparse Network Coding**: This scheme considers the transmission of 3-sparse packets only. For determining the delay performance, we use Eq. (1) and use Algorithm 1 to determine complexity.

- **RLNC**: This constitutes a classical RLNC scheme with cubic complexity. In particular, we consider that \( GE(n) = n^3/3 + n^2/2 - 5n/6 \), which is a usual estimate of operations necessary to perform Gaussian elimination. For RLNC we assume that every incoming packet is innovative, which is a good approximation when using large field sizes.

- **Tunable Sparse Network Coding Scheme**: This scheme relies on both a sparse and a dense region, with a tunable threshold to decide when to switch from one to the other. Packets generated in the sparse region are \( k \)-sparse, with \( k \) being incremented every time \( n/100 \) coded packets sent.

Fig. 3 shows the performance of the three schemes as more packets are coming into the system. The right and top-most point for each curve constitutes the final pair of values for delay and complexity. Fig. 3 shows our proposed scheme for different threshold levels, namely when \( 1, 2, 5, 10, 50 \) and \( 75\% \) of the degrees of freedom are missing at the receiver. We observe that i) switching too fast to RLNC is counterproductive from a complexity perspective, and ii) gains in terms of complexity become important when the switch to RLNC happens for the very last packets (See case of 1\%). Finally, the case of switching for the last 1\% helps us confirm our initial intuition, namely that a sparse code’s delay performance is primarily degraded when few degrees of freedom are missing.

V. Conclusions

We revisit the problem of trading off delay performance and decoding complexity but providing a novel framework that uses both sparse and dense coded packets and allows coding at intermediate nodes for multicast sessions in general networks. More generally, we propose that the sparsity level should evolve as the transmission session progresses. To enable this coding flexibility, we proposed an efficient and intuitive algorithm for reordering rows and columns of a matrix in order to perform efficient Gaussian elimination in sparse matrices. This algorithm guarantees linear decoding complexity of sparse packets w. h. p.

Our approach can benefit considerably from the use of feedback in order to change the density of the code and studying efficient feedback mechanisms will be the focus of future work. Future work will also consider efficient and practical pre-coding mechanisms at the source for the case of single and multi source multicast to deal with specific network topologies and practical coding policies at intermediate nodes.

VI. Acknowledgements

This work was supported in part by the Air Force Office of Scientific Research (AFOSR) under award No. FA9550-08-1-0159 and by FCT project PEst-OE/EEI/LA0008/2011.

References


The Flatness Factor in Lattice Network Coding:
Design Criterion and Decoding Algorithm

Jean-Claude Belfiore
Department of Communications and Electronics
Telecom ParisTech, LTCI UMR 5141
46, rue Barrault, 75013 Paris, France
Email: belfiore@enst.fr

Cong Ling
Department of Electrical and Electronic Engineering
Imperial College London
London SW7 2AZ, United Kingdom
Email: cling@ieee.org

Abstract—In a recent work, Nazer and Gastpar proposed the compute-and-forward strategy as a physical-layer network coding scheme. They described a code structure based on nested lattices whose algebraic structure makes the scheme reliable and efficient. In a more recent paper, Niesen and Whiting revealed a fundamental limitation of the decoder used by Nazer and Gastpar. In this work, we consider maximum-likelihood decoding of compute-and-forward, aiming to overcome its limitation. By examining the decoding metric from the viewpoint of Gaussian measures over lattices, we present a design criterion of the lattice code based on the flatness factor, and propose a new decoding algorithm based on inhomogeneous Diophantine approximation.

I. INTRODUCTION

In [1], Zhang et al. introduced the physical-layer network coding concept (PNC) in order to turn the broadcast property of the wireless channel into a capacity boosting advantage. Instead of considering the interference as a nuisance, each relay converts an interfering signal into a combination of simultaneously transmitted codewords. PNC concept has received a particular interest in the last years because it provides means of embracing interference and improving network capacity.

In a recent work [2], Nazer and Gastpar proposed a new physical-layer network coding scheme. The proposed strategy, called compute-and-forward (CF), exploits interference to obtain higher end-to-end transmission rates between users in a network. The relays are required to decode noiseless linear equations of the transmitted messages using the noisy linear combination provided by the channel. The destination, given enough linear combinations, can solve the linear system for its desired messages. This strategy is based on the use of structured codes, particularly nested lattice codes to ensure that integer combinations of codewords are themselves codewords. The authors demonstrated its asymptotic gain using information-theoretic tools. Standard minimum Euclidean distance decoding was assumed.

The authors in [3] followed and generalized the framework of Nazer and Gastpar by introducing the Lattice Network Coding (LNC). They related the Nazer-Gastpar’s approach to the theorem of finitely generated modules over a principle ideal domain (PID). They gave sufficient conditions for lattice partitions to have a vector space structure which is a desirable property to make them well suited for PNC. Then, they generalized the lattice code construction and developed encoding and decoding methods. Standard minimum Euclidean distance decoding was still assumed.

In a more recent work [4], Niesen and Whiting revealed a fundamental limitation of standard minimum Euclidean distance decoding, namely, it achieves no more than 2 degrees of freedom. This is due to the quantization of channel coefficients, which leads to a tradeoff between channel coefficient approximation and noise amplification. This tradeoff was associated with a problem of Diophantine approximation in [4]. They further proposed a scheme achieving higher degrees of freedom based on real interference alignment. However, this scheme is not robust, among many of its shortcomings.

In [5], the first author essentially proposed an analysis of the compute-and-forward strategy when maximum-likelihood (ML) decoding is used. It should be emphasized that ML decoding does not subscribe to the limitation shown in [4]. A new quantity, the Flatness Factor, was introduced, which measures the quality of ML decoding. After changing the definition of the flatness factor in order to be consistent with [8], [9], this paper studies more deeply the properties of it and gives some new insights into lattice network coding.

II. COMPUTE AND FORWARD

In our model, we consider one relay receiving messages from $k$ sources $S_1, \ldots, S_k$ and transmitting a linear combination of these $k$ messages. The relay observes a noisy linear combination of the transmitted signals through the channel. Received signal at the relay is expressed as,

$$y = \sum_{j=1}^{k} h_j x_j + w \quad \text{(1)}$$

where $h_j$ is the channel coefficient between source $S_j$ and the relay and $x_j$ is the vector transmitted by source $S_j$.

The relay searches to transmit a noiseless linear combination of the received signals with integer coefficients given by vector

$$a = [a_1 \ a_2 \ \cdots \ a_k]^T.$$

To achieve that goal, it decodes a noiseless linear combination of the transmitted vectors,

$$x_R = \sum_{j=1}^{k} a_j x_j \quad \text{(2)}$$
and retransmits it to the destination or another relay. We consider a complex-valued channel model with complex inputs and outputs. The channel coefficients $h_i$ are complex, circular, i.i.d. Gaussian, $h_i \sim \mathcal{N}(0, 1)$. $z$ is Gaussian, zero mean, with variance $\sigma^2$ ($z \sim \mathcal{N}(0, \sigma)$). Let $h = [h_1 \; h_2 \; \cdots \; h_k]^T$ denote the vector of channel coefficients. Source vectors $x_j$ are carved from a lattice code. The sources have no channel-side information (CSI). CSI is only available at the relay.

### III. The ML Decoder

#### A. Solving the System of Diophantine Equations

The relay aims to decode a linear system of equations of the transmitted messages and passes it towards the destination. After calculating the vector $a$ chosen following some given criterion, the relay recovers a linear combination of the transmitted signals. We rewrite the received (scaled) signal at the relay in the following form,

$$ y = \lambda + \sum_{j=1}^{k} \xi_j x_j + \nu \quad (3) $$

where $\lambda$ is a point of a lattice $\Lambda$, $\xi_j = h_j - a_j$ and $\nu$ is the additive i.i.d. Gaussian noise. The recovered linear system of equations $\lambda = \sum_{j=1}^{k} a_j x_j$ is a linear system of Diophantine equations. This system admits the following solutions.

Suppose that the transmitted vectors $x_j \in \Lambda_j$ where $\Lambda_j$ are full rank lattices. Then, since

$$ \lambda = \sum_{j=1}^{k} a_j x_j, \quad (4) $$

the lattice in which $\lambda$ lives is

$$ \Lambda = a_1 \Lambda_1 + a_2 \Lambda_2 + \cdots + a_k \Lambda_k. $$

Our aim, here, is to express the messages $x_j$ as a function of $\lambda$, for a given $\lambda \in \Lambda$. But the system of Diophantine equations admits an infinite number of solutions. The Hermite Normal Form (HNF) allows to solve this system [7]. We show here how to proceed.

From Equation (4), we get $\lambda = \sum_{j=1}^{k} a_j M_j z_j$ where $z_j \in \mathbb{Z}[i]^n$ and $M_j$ is a generator matrix for the lattice $\Lambda_j$. Then, Equation (4) can be expressed as

$$ \begin{bmatrix} a_1 M_1 & a_2 M_2 & \cdots & a_k M_k \end{bmatrix} \begin{bmatrix} z_1 & z_2 & \cdots & z_k \end{bmatrix}^T = \lambda. \quad (5) $$

Define $M = [a_1 M_1 \; a_2 M_2 \; \cdots \; a_k M_k]$ and use the Hermite Normal Form of $M$ [7],

$$ M \cdot U = \begin{bmatrix} 0 & B \end{bmatrix}. $$

Decompose the unimodular matrix $U$ into blocks

$$ U = \begin{bmatrix} U_1 & V_1 \\ U_2 & V_2 \\ \vdots & \vdots \\ U_k & V_k \end{bmatrix} $$

where matrices $V_j$ are square $n \times n$ matrices. Then the solution to the system of Diophantine equations is,

$$ x_j = s_j + v_j \quad (6) $$

where $v_j = M_j V_j B^{-1} \lambda$ and $s_j$ is any vector in the lattice $L_j \subset \Lambda_j$ of generator matrix $M_j U_j$.

#### B. ML Decoding Metric

The ML decoder maximizes $p(y/\lambda)$ over all possible values of $\lambda$. The conditional probability $p(y/\lambda)$ can be expressed as,

$$ p(y/\lambda) = \sum_{(x_1, \ldots, x_k) \in \mathbb{Z}[i]^n} p(x_1, \ldots, x_k)p(x_1, \ldots, x_k) \quad (7) $$

where

$$ p(y/x_1, \ldots, x_k) \propto e^{-\|y - \sum_{j=1}^{k} h_j x_j\|^2 / 2\sigma^2}. \quad (8) $$

and $x_1, \ldots, x_k$ are (a priori) supposed equiprobable and given by (6). The decoding rule is now to find

$$ \hat{\lambda} = \arg \max_{\lambda \in \Lambda} \varrho(\lambda), \quad (9) $$

with

$$ \varrho(\lambda) = \sum_{q \in \mathcal{L}} e^{-u(\lambda - q)^2 / 2\sigma^2}. $$

where $u(\lambda) = y - \left(\sum_{j=1}^{k} h_j M_j V_j \right) B^{-1} \lambda$ and $\mathcal{L}$ the $n$-dimensional $\mathbb{Z}[i]$-lattice with generator matrix $C = \sum_{j=1}^{k} h_j M_j U_j$. We observe that, for some values of the parameters, the function $\varrho(\lambda)$ can be almost constant or flat, which will yield a high error probability. Figure III-B illustrate the behavior of the likelihood function for difference noise variances. Clearly, we should avoid the second and third cases where it is almost flat. In the next section, we will use the flatness factor to assess the behavior of the likelihood function.

### IV. The Flatness Factor

#### A. Definition

For a given lattice $\mathcal{L}$ and a vector $y$, we consider the $n$-variable function

$$ f_{\sigma, \mathcal{L}}(y) = \frac{1}{(2\pi\sigma)^n} \sum_{q \in \mathcal{L}} e^{-\|y-q\|^2 / 2\sigma^2}, $$

which is a Guassian measure over a lattice. Obviously, $\varrho(\lambda) \propto f_{\sigma, \mathcal{L}}(u(\lambda))$. This function has been studied in [8]. We want here, to avoid that this function be flat for the lattice $\mathcal{L}$.

**Definition 1.** [Flatness factor] The flatness factor of the Gaussian measure is defined as the maximum ratio $f_{\sigma, \mathcal{L}}(y)$ can deviate from the uniform distribution:

$$ \epsilon_{\mathcal{L}}(\sigma) \equiv \max_{y \in \mathcal{X}} \frac{|f_{\sigma, \mathcal{L}}(y) - E_y f_{\sigma, \mathcal{L}}(y)|}{E_y f_{\sigma, \mathcal{L}}(y)}. \quad (10) $$

Note that this definition is slightly different from that in [5], for the sake of consistency with [9] where the problem of physical-layer security is addressed (flatness is desired in there). The following proposition gives the expression of the
flatness factor in terms of the theta series (the proof is given in [9]).

**Proposition 2.** [Expression of $\epsilon_L(\sigma)$]

\[
\epsilon_L(\sigma) = \mu^n \Theta_L \left( \frac{1}{2\pi \sigma^2} \right) - 1
\]  

(11)

where $\mu = \frac{V(L)}{2\pi \sigma^2}$ is the generalized signal-to-noise ratio, and $\Theta_L(z) = \sum_{\lambda \in L} e^{-\pi \sigma^2 |z|^2}$ is the theta series of $L$.

The flatness factor is closely related to the smoothing parameter studied in [8]. The advantage of the flatness factor is two-fold:

- It gives a precise characterization $\epsilon_L(\sigma)$ by the theta series, so it is more precise than the bounds available in [8].
- The smoothing parameter is mostly concerned with small values of $\epsilon_L(\sigma)$, while the flatness factor can handle both small and large values. The latter is of interest in coding applications.

**B. Design Criterion**

We need that the flatness factor of $L$ be as large as possible to ensure that the maximum likelihood metric will be as different as possible from the likelihood metrics of the other points of the lattice $L$. Formally, we have the following design criterion of the lattice $L$:

**Proposition 3.** [Goodness for network coding] In order to have good decoding performance in compute-and-forward, the theta series $\Theta_L(z)$ should be large.

This requires from the lattice $L$ to be 'bad' as possible in the standard sense of coding (i.e., not dense at all). The generator matrix of $L$ is $\sum_{j=1}^k h_j M_j U_j$. But, since $\sum_{j=1}^k a_j M_j U_j = 0$, from the HNF, we deduce that we have to align vector $a$ with vector $h$ as much as possible.

As an illustration, Figure 2 shows the values of some flatness factors as a function of the generalized signal to noise ratio $\mu$. For our purpose, the Leech lattice is worse than the $\mathbb{Z}^n$ lattice.

**V. DECODING ALGORITHM**

We are now interested in an algorithm which must maximize $\varrho(\lambda)$ in an efficient way. To do this, we need the Fourier transform and Jacobi theta functions. In fact, we will not attempt to compute $\varrho(\lambda)$ itself; instead, we will propose inhomogeneous Diophantine approximation as a solution to ML decoding.

**A. Fourier transform and Jacobi theta function**

Since $f_{\sigma,L}(y)$ is obviously periodic on $L$, its Fourier transform is defined on the dual lattice $L^\ast$. The Fourier coefficients are given by

\[
f_{\sigma,L}(q^\ast) = \frac{1}{V(L)} e^{-2\pi^2 \sigma^2 ||q^\ast||^2}, \quad q^\ast \in L^\ast.
\]  

(12)

The Fourier expansion of $f_{\sigma,L}(y)$ is then

\[
f_{\sigma,L}(y) = \frac{1}{V(L)} \sum_{q^\ast \in L^\ast} e^{-2\pi^2 \sigma^2 ||q^\ast||^2} e^{2\pi i q^\ast \cdot y}. \quad (13)
\]

Now we express the Gaussian measure as the Jacobi theta function (sometime referred to as the Riemann theta function in the multi-dimensional case), via the Fourier transform (13). Let $\mathbb{H}_n$ be set of symmetric square matrices whose imaginary part is positive definite. For an $n \times n$ matrix $T \in \mathbb{H}_n$ and an $n$-dimensional complex vector $z$, the multi-dimensional theta function is defined as

\[
\theta(z;T) = \sum_{q \in \mathbb{Z}^n} e^{\pi i q^T T q + 2\pi i q^T z}.
\]  

(14)

Comparing with (13), we recognize that

\[
f_{\sigma,L}(y) = \frac{1}{V(L)} \theta(z;T)
\]  

(15)
for $z = C^{-1}y$ and $T = 2\pi i\sigma^2(C^TC)^{-1}$. Known results of the Jacobi theta function may be applied to analyze the Gaussian measure over lattices.

B. The 1-D Real Case

Here,

$$\varrho(\lambda) = \sum_{k \in \mathbb{Z}} e^{-\frac{(\alpha-y-\beta k)^2}{2\sigma^2}}$$

for some given values of $\alpha$ and $\beta$. So, we have to study the function $f_{\sigma,\tau}(y)$ since, obviously, we have

$$\varrho(\lambda) \propto f_{\sigma,\tau}(y - \alpha \lambda).$$

We will show now that ML decoding is equivalent to Diophantine approximation

$$\arg\max_{\lambda \in \Lambda} \varrho(\lambda) \approx \arg\min_{\lambda \in \Lambda, \mathbf{q} \in \mathcal{L}} \|u(\lambda) - \mathbf{q}\|^2. \quad (22)$$

Even if we are unable to prove the conjecture for now, there are evidences supporting a decoder like (22). Since $f_{\sigma,\tau}(y)$ is the Fourier transform of a positive measure, we have

**Conjecture 6.** Maximizing the ML metric is equivalent or close to solving a multidimensional inhomogeneous Diophantine approximation problem. More precisely,

**Proposition 7.** $f_{\sigma,\tau}(y)$ is a positive-definite function. In particular, $f_{\sigma,\tau}(y) \leq f_{\sigma,\tau}(0)$.

Moreover, it is easy to see

**Proposition 8.** The first derivative $f'_{\sigma,\tau}(y) = 0$, while the second derivative $f''_{\sigma,\tau}(y) < 0$, when $y \in \mathcal{L}$.

Therefore, $f_{\sigma,\tau}(y)$ is bell-shaped in the vicinity of a lattice point, which is a local (and also global) maximum. The Diophantine-approximation decoder is a good approximation with respect to this monotonic decoding metric (at least locally).

We close this investigation with a remark on the different roles played by Diophantine approximation in this paper and in [2]. Diophantine approximation was a detrimental effect in [2], while it plays a constructive role in this paper. We expect it will achieve a better performance in compute-and-forward.

**References**


Analysis of the Stochastic Channel Model by Saleh & Valenzuela via the Theory of Point Processes

Morten Lomholt Jakobsen, Troels Pedersen and Bernard Henri Fleury {mlj, troels, bfl}@es.aau.dk
Section Navigation and Communications, Dept. of Electronic Systems, Aalborg University
Fredrik Bajers Vej 7B, DK-9220 Aalborg East, Denmark

Abstract—In this paper we revisit the classical channel model by Saleh & Valenzuela via the theory of spatial point processes. By reformulating this model as a particular point process and by repeated application of Campbell’s Theorem we provide concise and elegant access to its overall structure and underlying features, like the intensity function of the component delays and the delay-power intensity. The flexibility and clarity of the mathematical instruments utilized to obtain these results lead us to conjecture that the theory of spatial point processes provides a unifying mathematical framework to define, analyze, and compare most channel models already suggested in literature and that the powerful tools of this framework have not been fully exploited in this context yet.

I. INTRODUCTION

Literature regarding channel models for (indoor) radio propagation dates back earlier than 1960, and most commonly the wireless multipath channel is characterized via its (time and space varying) impulse response [1]. Two classic and seminal contributions within channel modeling are those by Turin et al. [2] and Saleh & Valenzuela [3]. To some extent the (indoor) model by Saleh & Valenzuela can be seen as a generalization of the (urban) model by Turin. Specifically, the generalization aimed at mimicking cluster alike behavior since this effect was reported to have been observed experimentally.

Ever since the model by Saleh & Valenzuela (for short the S-V model) was proposed in 1987, many refined or marginally extended variants have appeared, see e.g. [4] and [5]. Unfortunately, these channel models have not been developed within any unifying mathematical framework. Instead their treatment is of rather ad-hoc nature and, as a result, their inherent features remain essentially veiled and any two different models are not easily comparable.

Recently the authors of [6] and [7] reformulated and outlined the S-V model in terms of marked point processes. The S-V model has also been revisited in [8] by use of shot-noise tools and point process theory. Among other things the analysis in [7] and [8] show that the overall intensity of the relative delays of multipath components grows linearly with the propagation delay. Unfortunately, the mathematical tools used in [7] to extract the features of the model are not directly associated with the general theory of point processes. On the other hand, the tools used in [8] are rather advanced and the derivations less transparent. Accordingly, the potential theoretical benefits arising through these point process reformulations are not immediately evident.

In this paper we showcase how the general theory of spatial point processes provides an insightful view upon the inherent structure and features of the classical S-V model. Like [7] and [8] we revisit the model and reformulate it as a particular point process. Aligned with [7] we show that the component delays consist of the union of a Poisson point process and a Cox point process and we derive the associated intensity function as an immediate consequence of Campbell’s Theorem. The derivation in [7] is similar but with no reference to Campbell’s Theorem. Furthermore, and in contrast to the involved proofs relying on shot-noise tools in [8], we obtain the delay-power intensity in a simple and direct way by invoking once more Campbell’s Theorem. These results demonstrate the potential of this well-known theorem from the theory of spatial point processes in the context of stochastic channel modeling. In view of this, our conclusion is that the theory of spatial point processes and its powerful tools have not been fully exploited yet to analyze the properties of most proposed stochastic channel models. This theory appears to provide the necessary unifying framework for which these models can be contrasted within.

II. POINT PROCESS FRAMEWORK

We assume familiarity with the basics of the theory of spatial point processes (see [9, Sec. 1.3, Chap. 2] and [10, Sec. 1.5, 6.2] for highly recommendable introductions). Concepts from abstract measure theory will be kept at a minimum.

A. Locally finiteness and simplicity

Denote by $Y$ a locally finite and simple point process defined on a $d$-dimensional space $S \subseteq \mathbb{R}^d$. For intuitive, practical and mathematical reasons, these two properties are convenient to impose since several technical aspects can then be disregarded.

A point process is locally finite if the number of points falling in every bounded Borel set $B \subseteq S$ is almost surely finite. A point process is simple if, almost surely, no two points of the process coincide. Accordingly, any realization of the point process $Y$ can be identified as a countable set of points \( \{y_1, y_2, \ldots \} \), \( y_i \in S \), where the index $i$ of $y_i$ serves solely as a dummy label. Thus, the index is used only to distinguish points and to indicate countability. It does not indicate any ordering of the points.

B. The intensity function and Campbell’s Theorem

Consider the counting function defined, using a generic indicator function $\mathbb{1}[\cdot] \in \{0, 1\}$, as

$$ N_Y(B) := \sum_{y \in Y} \mathbb{1}[y \in B], $$

which equals the random number of points from $Y$ falling in the set $B$. For any fixed and bounded $B$, the count $N_Y(B)$ is
a non-negative integer-valued random variable. The expected value of the counting function \( \mu_y(B) = E[N_y(B)] \) defines a measure on \( S \), the so-called intensity measure of \( Y \). If the intensity measure can be expressed as

\[
\mu_y(B) = \int_B \varphi_y(y) \text{d}y, \quad B \subseteq S,
\]

for a locally integrable function \( \varphi_y : S \to [0, \infty) \), then \( \varphi_y \) is called the intensity function of \( Y \). The case when the intensity function exists is by far the most important for applications [11]. The importance of the intensity function is evident from the following result, often referred to as Campbell’s Theorem.

**Campbell’s Theorem.** Let \( Y \) be a point process on \( S \subseteq \mathbb{R}^d \) with intensity function \( \varphi_y \). Then for a real or complex-valued measurable function \( h : S \to \mathbb{R} \) (or \( \mathbb{C} \)), the random variable \( \sum_{y \in Y} h(y) \) has expected value

\[
E\left[ \sum_{y \in Y} h(y) \right] = \int_S h(y) \varphi_y(y) \text{d}y, \tag{1}
\]

provided that the integral on the right exists.

Proofs with varying degrees of detail can be found in [9, Sec. 3.2], [11, Prop. 4.1] and [12, Thm. 2.2]. Often, the theorem is stated only for non-negative functions \( h \), since the equality in (1) is then unconditionally true, i.e. the integral is always well-defined but possibly divergent. When \( h \) is real-valued some care must be taken since the integral at the right hand side of (1) has no meaning if the positive and the negative part of \( h \) are not integrable. Similar care must be taken for complex \( h \).

**C. Poisson and Cox point processes**

We now define two classes of point processes which are particularly important for our treatment in the forthcoming section, namely Poisson point processes and Cox point processes. These definitions can be found in many text books covering the theory of spatial point processes. Our treatment is directly inspired by [11] and the interested reader may consult [10]–[12] for further details.

**Definition.** A point process \( Y \) on \( S \subseteq \mathbb{R}^d \) is called a Poisson point process with intensity function \( \varphi_y \) if:

\( i \) For any \( B \subseteq S \) with \( \mu_y(B) = \int_B \varphi_y(s) \text{d}s < \infty \) the count \( N_y(B) \) is Poisson distributed with mean \( \mu_y(B) \).

\( ii \) Given that \( N_y(B) = n \in \mathbb{N} \) where \( 0 < \mu_y(B) < \infty \), the distribution of \( Y \cap B \) is the same as that of \( n \) points drawn i.i.d. according to \( \varphi_y \), where

\[
f_n(s) := \frac{\varphi_y(s)}{\mu_y(B)} \mathbb{1}[s \in B].
\]

We write \( Y \sim \text{PoissonPP}(S, \varphi_y) \).

**Definition.** Let \( Z(s), s \in S \), be a non-negative random field such that, almost surely, every realization of \( Z \) is a locally integrable function on \( S \). If a point process \( Y \), conditioned on \( Z \), is a Poisson point process with intensity function \( \varphi_y \), then \( Y \) is called a Cox point process driven by \( Z \).

Cox point processes (also often referred to as doubly stochastic Poisson point processes [10]) are flexible models for clustered point patterns. Specifically, the two-level construction most commonly entails the Cox class to exhibit so-called over-dispersion compared to the Poisson class [11, Sec. 5.2].

**III. The Model by Saleh & Valenzuela**

In this section we analyze the impulse response of the classical S-V model within the framework of spatial point processes. The main purpose of this effort is to straightforwardly derive the features of this model through a flexible and powerful theory. Several relevant aspects of the model are revealed through this reformulation, e.g. its overall delay intensity, a concise and clear derivation of the average power gain and, a simple derivation of the delay-power intensity as well.

**A. Classical formulation**

Saleh & Valenzuela define the channel impulse response with cluster and within-cluster delays as [3, Eq. (25)]

\[
h(t) = \sum_{\ell=0}^{\infty} \sum_{k=0}^{\infty} \beta_{k,\ell} \exp(j\theta_{k,\ell}) \delta(t - (T_\ell + \tau_{k,\ell})), \tag{2}
\]

where \( \delta \) is the Dirac delta and \( j \) is the imaginary unit. The index \( \ell \) indicates a certain cluster and \( k \) is the within-cluster index. By definition in [3], \( T_0 = 0 \) and \( \tau_{0,\ell} = 0 \) for each \( \ell \in \mathbb{N}_0 := \{0\} \cup \mathbb{N} \). Beside these fixed delay components, a sequence of Poisson point processes are suggested such that

- \( \{T_\ell\}_{\ell \in \mathbb{N}} \sim \text{PoissonPP}(\mathbb{R}_+, \Lambda) \)
- \( \{\tau_{k,\ell}\}_{k,\ell \in \mathbb{N}} \sim \text{PoissonPP}(\mathbb{R}_+, \lambda) \) for each \( \ell \in \mathbb{N}_0 \), with \( \Lambda, \lambda > 0 \) being two parameters. Moreover, conditional second-order moments are modeled such that [3, Eq. (26)]

\[
E[\beta_{k,\ell}^2 | T_\ell, \tau_{k,\ell}] = Q \exp(-T_\ell/\Gamma) \exp(-\tau_{k,\ell}/\gamma), \tag{3}
\]

where \( \Gamma, \gamma > 0 \) and \( Q \) being the average power gain of the first component within the first cluster (i.e corresponding to the fixed delay \( T_0 \)). Conditioned on all \( T_\ell \)'s and all \( \tau_{k,\ell} \)'s, the \( \beta_{k,\ell} \)'s are assumed to be mutually independent random variables. Specifically, each power gain \( \beta_{k,\ell} \) conditioned on \( T_\ell \) and \( \tau_{k,\ell} \) should follow an exponential distribution with mean parameter decaying as described by (3). Fig. 1 illustrates the Poisson point processes involved in the S-V model.

Finally, it was mentioned in [3] that practically the doubly-infinite sum in (2) should "stop" whenever each of the exponentially decaying terms in (3) had become small enough. Through the insight gained via the forthcoming reformulation of this classical channel model we are able to motivate a less heuristic "stopping criterion".

**B. Point process formulation**

Naturally, we select the space \( S = \mathbb{R}_+ \) and let \( T_0 = 0 \) as above. In addition, we introduce the point processes:

\[
C := \{T_\ell\}_{\ell \in \mathbb{N}} \quad (\text{all cluster delays except } T_0)
\]

\[
W_\ell := \{T_\ell + \tau_{k,\ell}\}_{k,\ell \in \mathbb{N}} \quad (\text{delays within the } \ell\text{'th cluster})
\]

\[
W := \bigcup_{\ell=0}^{\infty} W_\ell \quad (\text{all within-cluster delays})
\]

\[
Y := C \cup W \quad (\text{all propaganda delays except } T_0).
\]
Notice that $C$ is the Poisson point process specified at first in the previous paragraph. Its intensity function has a simple form, namely $\varrho_c(t) = \Lambda$ for all $t \in S$. By conditioning, we immediately identify a sequence of Poisson point processes

$$W_t \mid T_t \sim \text{PoissonPP} \left( R_c, \lambda I [t > T_t] \right), \quad \ell \in \mathbb{N}_0,$$

and since the Poisson class is stable with respect to countable superpositions [11, Prop. 3.6], we see that

$$W \mid C \sim \text{PoissonPP} \left( R_c, \varrho_W \right),$$

with the staircase-alike intensity function

$$\varrho_w(t) = \lambda + \lambda \sum_{c \in C} \mathbb{I} \{ t > c \}, \quad t \in S. \quad (4)$$

Accordingly, we identify that the point process $W$, without conditioning on $C$, is a Cox point process driven by a stochastic process $Z$ having the same functional form as $\varrho_w$ in (4) but with $C$ being random. The intensity function of the Cox point process $W$ is $\varrho_w(t) = \mathbb{E} \{ Z(t) \}$ [11, Sec. 5.2], and by direct application of Campbell’s Theorem we get

$$\varrho_w(t) = \lambda + \lambda \mathbb{E} \left[ \sum_{c \in C} \mathbb{I} \{ t > c \} \right] = \lambda + \lambda \Lambda t, \quad t \in S.$$

Since $Y = C \cup W$ is a union of almost surely disjoint point processes, its associated intensity function reads [10, Sec. 6.2.3]

$$\varrho_c(t) = \varrho_c(t) + \varrho_w(t) = \Lambda + \lambda + \lambda \Lambda t, \quad t \in S.$$  

It is interesting to notice that the entire set of propagation delays (excluding the first component $T_0$) is the union of a Poisson point process and a Cox point process. Of course, the realization of $W$ depends upon the realization of $C$, i.e. these two point processes are not independent. In [7] this interpretation was inherently adopted, without being explicitly mentioned. Another interesting yet expected observation is that the intensity function $\varrho_c$ rises linearly with propagation delay, see Fig. 2. The jump of height $\Lambda + \lambda$ at $T_0 = 0$ in the graph of $\varrho_c$ appears due to the cluster delays and the delays within the very first cluster. The term $\lambda \Lambda t$ result from the fact that, on average, a total of $\Lambda t$ additional clusters emerge during the interval $[0, t]$, with each and every one of them spawning further delay components at rate $\lambda$.

C. Multipath power gain

Analogous to the approach in [3], we consider the following non-negative random variable

$$G := \sum_{k=0}^{\infty} \sum_{\ell=0}^{\infty} \beta_{k,\ell}^2,$$

referred to as the total multipath power gain [3]. By splitting $G$ into three terms corresponding to $T_0$ and arrivals in $C$ and $W$, its expectation can be calculated as

$$\mathbb{E} \{ G \} = \mathbb{E} \{ \beta_{0,0}^2 \} + \mathbb{E} \left[ \sum_{k=1}^{\infty} \sum_{\ell=0}^{\infty} \beta_{k,\ell}^2 \right] + \mathbb{E} \left[ \sum_{k=0}^{\infty} \sum_{\ell=0}^{\infty} \beta_{k,\ell}^2 \right].$$

As in [3] we write $\beta(T_0, \tau_{k,\ell})$ in substitute for $\beta_{k,\ell}$ to facilitate a comprehensible notation in the following. For additional clarity we introduce the function

$$f(\tilde{t}, \tilde{t}) := Q \exp \left( - \tilde{t}/\Gamma - \tilde{t}/\gamma \right), \quad \tilde{t}, \tilde{t} \in S.$$

Notice that $f(T_0, \tau_{k,\ell}) = f(T_0, T_0 + \tau_{k,\ell} - T_0)$ coincides with the expression in (3). Then, by intermediate conditioning on $C$, we calculate the expectation of the term $\{ \ast \}$ as

$$\mathbb{E} \{ \{ \ast \} \} = \mathbb{E} \left[ \sum_{c \in C} \beta^2(c, 0) \right] = \mathbb{E} \left[ \sum_{c \in C} \mathbb{E} \left[ \beta^2(c, 0) \mid C \right] \right] = Q \Lambda \Gamma,$$

where the final step follows by application of Campbell’s Theorem. Next, by defining $C_{[0]} := \{ T_0 \} \cup C$ and with a similar sequence of manipulations involving intermediate conditioning and Campbell’s Theorem, we find the expected value of $\{ \circ \}$ to be

$$\mathbb{E} \{ \{ \circ \} \} = \mathbb{E} \left[ \sum_{c \in C_{[0]}} \sum_{w \in W_c} \beta^2(c, w - c) \right] \quad (6)$$

$$= \mathbb{E} \left[ \sum_{c \in C_{[0]}} \sum_{w \in W_c} \mathbb{E} \left[ \beta^2(c, w - c) \mid c, w \right] \right] = Q(1 + \Lambda \Gamma) \lambda \gamma. \quad (7)$$

Accordingly, the average total power gain is given by

$$\mathbb{E} \{ G \} = \mathbb{E} \{ \beta_{0,0}^2 \} + \mathbb{E} \{ \{ \ast \} \} + \mathbb{E} \{ \{ \circ \} \} = Q + Q \Lambda \Gamma + Q(1 + \Lambda \Gamma) \lambda \gamma = Q(1 + \lambda \gamma)(1 + \Lambda \Gamma), \quad (7)$$

\footnote{Note that in (6) we abuse notation since the collections $W_c$ are not explicitly defined. We only defined these as $W_c$ via the counting index $\ell$.}
as was also reported in a footnote in [3]. Yet, the original sequence of arguments used to obtain this result may appear less instructive, see [3, Eq. (27), (31)] for comparison. Notice that, depending on how we choose to write out the product in (7), we end up with different interpretations of individual average power contributions.

D. Delay-power intensity

Motivated by the definition of $G$ in (5) together with the relationship in (7), we consider

$$p(t) := \sum_{\ell=0}^{\infty} \sum_{k=0}^{\infty} \beta_{k,\ell}^2 \delta \left( t - (T_k + \tau_{k,\ell}) \right).$$

We wish to calculate how the average power gains are distributed across delay. From (7) we already know the mean total power gain, yet we seek to obtain further insight. The above definition of $p(t)$ is motivated by the fact that $\int_0^\infty p(t)dt = G$, and since $E[G]$ is finite, the non-negative random variable $G$ is itself finite almost surely. Accordingly, we define

$$P(t) := E[p(t)], \quad t \in S,$

and we refer to this function as the delay-power intensity. By similar manipulations as in the previous paragraph (conditioning, Campbell’s Theorem, etc.) we find

$$\frac{P(t)}{Q} = \delta(t) + \left\{ \begin{array}{ll}
{\phi}(t) = \lambda \left( 1 - \Lambda \frac{\Gamma - \gamma}{\Gamma} \right) \quad & \Gamma \neq \gamma \\
\gamma \Gamma \quad & \Gamma = \gamma
\end{array} \right.$$

where we have conveniently introduced the two constants

$$k_1 = \Lambda \left( 1 + \lambda \frac{\Gamma - \gamma}{\Gamma} \right) \quad \text{and} \quad k_2 = \lambda \left( 1 - \Lambda \frac{\Gamma - \gamma}{\Gamma} \right).$$

The same expression for $P(t)$ is obtained in [8, Chap. 2.3] using rather involved shot-noise tools with weighty notational overhead. Notice the particular relationship

$$E[G] = E \left[ \int_0^\infty p(t)dt \right] = \int_0^\infty E[p(t)] dt = \int_0^\infty P(t)dt.$$

The delay-power intensity of the S-V model is depicted in Fig. 3. Notice that $P(t)$ is not exponentially decaying, not even when $\Gamma = \gamma$ since $\phi(t)$ rises linearly (compare with the dotted line in Fig. 3).

Finally, as mentioned in the beginning of this section, we are now able to motivate a simple "stopping criterion" suitable, e.g. for simulation purposes. Specifically, select a delay threshold $t_{\text{max}}(\alpha)$ such that

$$\int_0^{t_{\text{max}}(\alpha)} P(t)dt = \alpha E[G],$$

for a relevant choice of $\alpha \in (0,1)$, e.g. $\alpha = 0.99$.

IV. Conclusion

In this contribution we have revisited the radio channel model by Saleh & Valenzuela (the S-V model) within the framework of spatial point processes. We have shown that the component delays in the S-V model emerge from the union of a Poisson point process and a Cox point process. Furthermore, we have demonstrated that the intensity function of the component delays and the delay-power intensity can be derived in a straightforward and rigorous manner as an immediate consequence of Campbell’s Theorem.

The above results indicate that the theory of spatial point processes yields a natural, unifying theoretical framework for dealing with stochastic channel models. This applies in particular to most channel models already suggested in literature, including the models by Turin et al. [2], Spencer et al. [4], and Chong et al. [5]. Our results also reveal that the powerful tools available in this framework, like Campbell’s Theorem, have not been exploited to their full extent in this context yet. Overall the considered application to the S-V model and to some extent the work in [6]–[8] show that the resulting mathematical treatments inherit clarity and conciseness, in addition to rigorousness, in contrast to the traditionally used ad-hoc and heuristic arguments.

ACKNOWLEDGMENT

This work has been funded by the project ICT-248894 Wireless Hybrid Enhanced Mobile Radio Estimators 2 (WHERE2), the 4GMCT cooperative research project co-financed by Intel Mobile Communications, Agilent Technologies, AAAU and the Danish National Advanced Technology Foundation, and by the Danish Agency for Science, Technology and Innovation.

REFERENCES

Low-Complexity Soft-Output Detection for Impulse-Radio Ultra-Wideband Systems Via Combining Multiple Observations

Andreas Schenk\textsuperscript{a} and Robert F.H. Fischer\textsuperscript{b}

\textsuperscript{a}Lehrstuhl für Informationsübertragung, Friedrich-Alexander-Universität Erlangen-Nürnberg, Erlangen, Germany,
\textsuperscript{b}Institut für Nachrichtentechnik, Universität Ulm, Ulm, Germany,
Email: andreas.schenk@int.de, robert.fischer@uni-ulm.de

Abstract—Avoiding explicit channel estimation, autocorrelation-based receivers enable low-complexity detection of impulse-radio ultra-wideband (IR-UWB) signals. In this paper, we present power-efficient IR-UWB detection schemes, which process the receive symbol stream partitioned into overlapping blocks. Properly combining the individual observations gained from each blockwise detection, a final (soft-)decision with improved reliability is obtained. By means of numerical simulations we show that the presented approach enables a reduction of the hardware complexity of the autocorrelation receiver at no degradation in performance and only slightly increased computational complexity, and is perfectly suited especially for coded transmission.

I. INTRODUCTION

Noncoherent receivers are widely regarded as the key to low-complexity detection in impulse-radio ultra-wideband (IR-UWB) systems, which are especially well-suited for short-range low-data-rate communications, such as, e.g., in wireless-sensor networks [1]. The inherent loss in performance of conventional noncoherent autocorrelation-based differential detection (DD), as compared to coherent detection based on explicit channel estimation, can be alleviated by advanced autocorrelation-based detection schemes, which process blocks of receive symbols jointly, i.e., perform multiple-symbol differential detection (MSDD) [2]–[4] or decision-feedback differential detection (DF-DD) [5]. However, significant challenges for implementation of the autocorrelation receiver (ACR) front-end are induced, as delaying the (analog) receive signal over several symbol durations is required to compute the correlation coefficients required for these detection schemes.

In this paper, we propose to obtain multiple observations of the same symbol by processing overlapping blocks of symbols. The resulting information gained from these individual observations is then combined to obtain a final decision with improved reliability. Depending on the choice of the blockwise detection scheme (we consider MSDD and DF-DD) and the method, how the individual observations are combined, the presented scheme is able to deliver hard and soft decisions, and is thus suited for coded and uncoded transmission. The benefit of the presented scheme is to reduce the hardware implementation complexity of the ACR front-end at no degradation in performance.

The proposed scheme can be seen as a development of subset MSDD introduced for noncoherent detection of differential phase-shift keying (DPSK, or more general differential space-time modulation) [6], [7], where similarly multiple observations are generated with an overlapping block-structure. However, as opposed to our approach, in [6], [7] most of the observations are simply treated as unreliable, thus discarded, and only a single observation is processed further.

After defining the IR-UWB system model and briefly reviewing autocorrelation-based detection in Sec.II, multiple-observations combining based on blockwise detection is introduced in Sec.III. The effectiveness of the approach is validated in Sec.IV by means of numerical simulations of uncoded and coded transmission; final remarks conclude the paper.

II. AUTOCORRELATION-BASED DETECTION OF IR-UWB

A. IR-UWB System Model

We consider differentially encoded binary pulse-amplitude-modulated IR-UWB transmission. Assuming no inter-symbol-interference (i.e., the symbol duration $T$ is chosen sufficiently large, such that each pulse has decayed before the next pulse is received) and a time-invariant multipath channel, the sampled receive signal in the $k$th symbol interval may compactly be written as an \((N_s = f_s T)\)-dimensional vector

$$\bar{r}_k = b_k \bar{p} + \bar{n}_k \tag{1}$$

where $f_s$ is the sampling frequency, $b_k$ are differentially encoded information symbols $a_k \in \{ \pm 1 \}$ (i.e., $b_k = a_k - a_{k-1}$ with $b_0 = 1$), and $\bar{p}$ is the (sampled) receive pulse shape, resulting from the convolution of the transmit pulse, multipath channel and receive filter impulse response. Neglecting the reference symbol, after suitable normalization, the energy per symbol is given as $E_s = 1$. $\bar{n}_k$ collects the samples of the zero-mean additive Gaussian noise, each with variance $\sigma_n^2 = f_s N_0/2$, where $N_0/2$ is the two-sided power-spectral density of the underlying additive white Gaussian noise.

B. Autocorrelation Receiver Front-End

Avoiding explicit channel estimation, autocorrelation-based detection computes the correlation of the current symbol with up to $L$ preceding symbols, cf., e.g., [2]–[5], [8]. Significant gains are achieved by adapting the correlation interval $T_i$ to the channel characteristics at hand [1], i.e., considering only
the relevant part \( r_k \) of \( \tilde{r}_k \) for autocorrelation by selecting \( N = T_f f_s \) successive elements (typically the first) out of \( N_0 \). This effectively reduces the time-bandwidth product to \( N = f_s T_f \). Thus, the output of the \( L \)-branch ACR for the \( k \)th symbol is given as, for \( l = 1, \ldots, L \),

\[
z_{k-l,k} = r^\top_{k-l} r_k = b_{k-l} b_k + \eta_{k-l,l} .
\]

(2)

Assuming that the correlation interval captures the entire pulse energy (i.e., due to normalization \( p^\top p = p^2 = 1 \)), \( z_{k-l,k} \) is composed of the phase transition from \( b_{k-l} \) to \( b_k \), and “information × noise” and “noise × noise” terms, summarized in the equivalent noise term \( \eta_{k-l,l} = b_{k-l} p^\top n_k + b_k n^\top_k p + n^\top_k n_k \). It has been shown that already for moderate time-bandwidth products \( N \) this equivalent noise is well approximated as uncorrelated zero-mean Gaussian random variables with variance \( \sigma^2 = 2\sigma_n^2 + N(\sigma_n^2)^2 \) [8]. For clarity, we note that, given the assumptions above, this Gaussian-approximated discrete-time equivalent model is independent of the actual pulse shape, i.e., the channel realization [9]. In this paper, all simulations of the IR-UWB system use this equivalent model.

The correlation coefficients serve as input for various detection schemes [1]–[5], [8], the most simple being symbolwise detection schemes [1]–[5], [8], the most simple being symbolwise detection (DD), evaluating only the sign of the correlation coefficient of the current symbol and its predecessor, i.e., \( a_k^{\text{DD}} = \text{sign}(z_{k-1,k}) \) with \( L = 1 \).

Finally, we point out that, due to the large signal bandwidth, implementation of the ACR is typically envisioned fully in the analog domain, instead of digital processing based on a sufficiently sampled version. This imposes a major drawback of ACR-based detection, namely the required accurate (analog) delay lines. In this paper, we aim to mitigate this drawback by means of detection schemes based on an ACR with less branches, i.e., reduced, \( L \), at no degradation in performance.

III. SOFT-OUTPUT DETECTION BASED ON MULTIPLE OBSERVATIONS

Based on the output of an \( L \)-branch ACR, low-complexity, yet powerful detection schemes process the receive symbol stream partitioned into blocks of \( L \) symbols. Before discussing the generation and combination of multiple observations obtained from this blockwise processing, we briefly review two variants of block-based detection schemes, namely (soft-output) MSDD and DF-DD [2]–[5], which deliver individual (soft) decisions for the symbols within each block.

A. Obtaining an Individual Observation

Keeping notation simple, we consider an arbitrary block of information symbols grouped into a vector \( \mathbf{a} \in \{\pm 1\}^L \) with all indices to be understood as intra-block indices.

1) Soft-Output Multiple-Symbol Differential Detection: MSDD delivers the blockwise-optimal sequence [3], [5], i.e., the sequence with minimum decision metric

\[
\mathbf{a}^{\text{MSDD}} = \arg\min_{\mathbf{a} \in \{\pm 1\}^L} \Lambda(\mathbf{a})
\]

(3)

where the decision metric is defined as

\[
\Lambda(\tilde{\mathbf{a}}) = \sum_{k=1}^L \left( \sum_{l=0}^{L-1} \left( z_{l,k} - \tilde{b}_l \tilde{b}_k z_{l,k} \right) \right)
\]

(4)

and \( \tilde{b}_k \), \( 0 \leq k \leq L \), and \( z_{l,k} \), correspond to the differentially encoded hypothesis \( \tilde{a} \), and the correlation coefficients (cf., (2)) of the considered block, respectively.

Soft decisions, i.e., reliability information on the decision of each symbol, is obtained by extending MSDD to so-called soft-output MSDD (SO-MSDD) [4]. In terms of (max-log approximated) log-likelihood ratios (LLRs), soft output for the \( k \)th (binary) information symbol is given as

\[
\text{LLR}_k = \frac{1}{\sigma^2_n(L + 1)} \left[ a^{\text{MSDD}}_k (\Lambda^{\text{MSDD}}_k - \Lambda^{\text{MSDD}}) \right]
\]

(5)

where \( \Lambda^{\text{MSDD}} = \Lambda(a^{\text{MSDD}}) \) denotes the metric associated with the MSDD estimate (3), and

\[
\Lambda^{\text{MSDD}} = \min_{\tilde{a} \in \{\pm 1\}^L} \Lambda(\tilde{a})
\]

(6)

the decision metric of the corresponding counter hypothesis, i.e., the minimum metric with the restriction \( a^{\text{MSDD}}_k = -a^{\text{MSDD}}_k \).

Utilizing the triangular structure of the decision metric, MSDD can be viewed as a tree-search-problem, which in turn can efficiently be solved employing the single-tree-search soft-output sphere decoder (SO-SD) [10], [4]. To further reduce the computational complexity of the SO-SD in particular at low SNR, LLR clipping during the SO-SD search process (clipping level \( \text{LLR}_{\text{max}} \)) [10], [4] is applied. In addition, we employ an optimized decision order within the search process. This sorting of the SD input is based on the same optimization criterion as of DD-DD (cf. Sec. III-A2 and [5]), and requires some modifications to the original SO-SD algorithm [4]. Minimum throughput of the MSDD device, despite the varying complexity of the SD, can effectively be guaranteed by introducing a cumulative maximum complexity limit (e.g., per codeword) similar to [10]. Due to space limitations, these techniques are not described in greater detail.

2) Decision-Feedback Differential Detection: A closely-related detection scheme is blockwise DD-DD [5], which decides the symbols within each block in a successive manner taking into account the feedback from already decided symbols within the block. In [5] it has been shown that DD-DD achieves close-to-optimum performance at very low, and in particular constant computational complexity, if the decision order is optimized, such that in each step the most reliable symbol is decided first (taking into account the actual correlation coefficients and the previous decisions, see [5] for details).

B. Obtaining Multiple Observations

In the related context of noncoherent detection of DPSK (and more general unitary differential space-time modulation), in [6], [7] it has been proposed to employ MSDD in combination with an overlapping block-structure. Since multiple blocks thus contain the same symbol, processing of each block delivers (possibly different) beliefs on the same symbol, i.e., multiple observations are available. Observing that the reliability of the estimates degrades at the block edges for
DPSK [6], [7], only the middle part of each block is processed further, so-called subset MSDD, as illustrated in the left part of Fig. 1. Already available observations of symbols at the block edges are treated as unreliable and are simply discarded.

Avoiding to discard already available observations, we propose to suitably combine all observations obtained from processing of each block, resulting in a (possibly more reliable) final decision. The basic concept is illustrated on the right hand side of Fig. 1. There are different options how to combine multiple observations to deliver a final (soft) decision for the respective symbol, as discussed in Sec. III-C. In addition note that, in the context of MSDD of IR-UWB, significantly different reliabilities within each block cannot be observed, and, as we employ an optimized decision order within each block (cf., [5] and Sec. III-A), the positions of the most reliable symbols are no longer limited to the block center.

Of course, the generation of multiple observations, i.e., processing of overlapping blocks, leads to an increased computational complexity and processing delay; however, the analog ACR front-end remains unchanged. As we aim for a flexible tradeoff between performance and computational complexity, we vary the mutual shift \( s = 1, \ldots, L \) of adjacent blocks (i.e., overlap of \( L - s \) symbols) to adjust the number of multiple observations for each symbol. Thus, we obtain on average \( L/s \) observations per symbol (for finite symbol streams this value can be ensured by reducing the blocksize at the beginning and at the end), with maximum overlap for \( s = 1 \), and the traditional single observation per symbol for \( s = L \). Note that blocksize and overlap are defined based on the information symbols; the respective blocks of \( L + 1 \) differentially encoded symbols overlap by at least one symbol.

C. Combining Multiple Observations

Depending on the employed blockwise detection scheme, different options can be considered how multiple observations are combined to a final estimate of the information symbol.

1) Combining Multiple Soft Decisions: If soft decisions are available for each individual observation, as obtained from SO-MSDD, we may consider these observations as independent (though independence cannot be assured), and obtain the resulting final estimate according to the principle of parallel information combining [11]. In terms of LLRs, the resulting LLR for each symbol is then directly given as the sum of the corresponding individual LLRs.

In the case of coded transmission, the resulting LLR can directly be passed to the subsequent (soft-input) channel decoder. Since LLR clipping affects each SO-SD run, the maximum absolute input value is \( L \cdot \text{LLR}_{\text{max}} \). Final hard-decisions can be obtained by evaluating only the sign of the sum of the LLRs, corresponding to combining the individual hard decisions according to their reliability.

2) Combining Multiple Hard Decisions: Based on multiple hard decisions, here obtained from DF-DD (of course, hard-output MSDD is also possible, but not considered for brevity), a final hard decision is directly given following the majority of the individual decisions (i.e., evaluating the sign of the sum of the individual estimates), which effectively treats each observation with equal reliability (in case of a draw, we choose \( \pm 1 \) at random). Clearly, this strategy leads to improved performance only if more than two observations are available per symbol, i.e., only if \( s < L/2 \).

However, the most interesting option is to combine multiple hard decisions of the same symbol to form a single soft decision. Exemplarily, consider the case that three (possibly different) hard decisions are available. If these coincide, the reliability of this symbol is three times as large as the reliability of only a single observation, whereas if only two coincide and one differs, the reliability is reduced to the case of a single observation. This method can be implemented by using the sum of the individual hard-decisions as (quantized and scaled) “soft-output”. Depending on the employed channel decoder, scaling of these soft-output values may be neglected if the decoding metric is scale-invariant (e.g., in a convolutional coded system employing the Viterbi algorithm for soft-decision decoding). However, e.g., in an LDPC-coded system, the soft output should be scaled to match the decoder input range.

IV. PERFORMANCE AND COMPLEXITY

Modeling a realistic IR-UWB scenario [1], for numerical simulations we set the time-bandwidth product to \( N = 400 \), corresponding, e.g., to an ACR correlation interval of \( T_s = 33 \text{ ns} \) and a Nyquist frequency of \( 6 \text{ GHz} \). Typically, the symbol duration is chosen larger (e.g., \( T_s = 75 \text{ ns} \)) to preclude inter-symbol interference.

We evaluate the effectiveness of the presented approach based on the key figures performance (i.e., the required energy per bit \( E_b \) vs. spectral noise density \( N_0 \)) and computational complexity at a desired bit error rate (BER) operating point. As a measure for the computational complexity of MSDD we use the average number of visited nodes per symbol of the SO-SD tree-search process. Due to LLR clipping and the optimized decision order, its variance is relatively low and can effectively be upper-bounded by introducing a cumulative maximum complexity limit. On the contrary, DF-DD has constant complexity, which, using its relation to SD-based tree search [5], corresponds to a single node per symbol.

First, we consider uncoded transmission (\( E_b = E_s \), i.e., multiple observations are combined to yield a final hard decision. Fig. 2 depicts the tradeoff performance vs. (average) complexity at an operating point of \( \text{BER} = 10^{-3} \), obtained by adjusting the mutual shift of the blocks (\( s = 1, \ldots, L \)) for a blocksize \( L = 3, 5 \) and 10. We consider the two detection schemes combining multiple soft decisions obtained from SO-
MSDD (sign of sum of LLRs), and combining multiple hard decisions obtained from DF-DD (sign of sum of estimates). For SO-MSDD, the LLR clipping level is set to \( \text{LLR}_{\text{max}} = 15 \). For both cases the upper-left point corresponds to the maximum block-overlap (maximum number of \( L \) observations, \( s = 1 \)), and the lower-right point to traditional detection with only a single observation per symbol (no overlap, \( s = L \)).

The performance of SO-MSDD improves with increasing number of combined individual soft-decisions, with gains of up to 0.8 dB compared to traditional MSDD; the increase in complexity is proportional to the average number of observations per symbol, \( L/s \). For comparison, tradeoff-curves employing the SO-SD without LLR clipping are also given, which prove that LLR clipping is crucial to achieve low complexity at only slight performance degradation [4], [10].

Combining multiple hard decisions (DF-DD) improvements are only achieved for \( s < L/2 \), as otherwise only up to two observations are available. However, as opposed to the varying complexity of SD-based MSDD, DF-DD achieves even larger gains at lower and, in particular, fixed complexity.

Finally, the performance-complexity tradeoff is evaluated for coded transmission at \( \text{BER} = 10^{-6} \) in Fig. 3. We consider a bit-interleaved coded modulation scheme employing maximum-free-distance convolutional codes (non-recursive, non-systematic, zero-padded encoder [12]) with constraint length \( \nu = 4 \), a random block-interleaver (size 1500 symbols), and, following the reasoning in [9], a code-rate of \( R_c = 2/3 \) (\( E_b = E_c R_c \)). As we aim for soft-decision decoding using the Viterbi algorithm, the final soft decision is obtained by combining either multiple soft decisions (sum of LLRs) in case of SO-MSDD as blockwise detection scheme, or multiple hard decisions (sum of estimates) in case of DF-DD, cf. Sec. III-C.

It can be observed that for all block sizes each additional observation leads to notable gains. Combining of multiple observations is especially effective, if multiple hard decisions are combined to a single soft decision (DF-DD); the difference between the traditional single observation and \( L \) observations, e.g., amounts to almost 2 dB for \( L = 10 \). Consequently, this scheme enables to effectively tradeoff low-cost computational complexity against costly implementation complexity of the ACR front-end at no degradation in performance by processing shorter, but overlapping blocks (thus, lower maximum delay required in the ACR) and combining the multiple observations.

V. CONCLUSIONS

In this paper, we have proposed a power-efficient, yet low-complexity detection scheme for autocorrelation-based IR-UWB receivers, which is based on combining multiple observations for the same symbol obtained from blockwise detection using an overlapping block structure. Our approach is able to deliver hard and soft decisions with improved reliability at only marginal increase in computational complexity, by simplified speaking, repeating very-low-complexity steps multiple times and combining the individual observations. It is perfectly suited especially for coded transmission and enables to reduce the blocksize, and thus also the implementation complexity of the analog autocorrelation receiver front-end, at no degradation in performance.

REFERENCES

Amplify-and-Forward Versus Decode-and-Forward Relaying: Which is Better?

Georgy Levin and Sergey Loyka

Abstract—Performance of multi-hop MIMO relay channels under the amplify-and-forward and decode-and-forward protocols are compared via the capacity and SNR gains. In an $N$-hop channel of linear topology with multi-antenna source and destination and single-antenna relay nodes, the capacity gain of the DF relaying over the AF one does not exceed $\log_2 N$ bit/s/Hz and its SNR gain does not exceed $N$, for any channel realization. This conclusion also applies to selection relaying, to the outage probability/capacity and the ergodic capacity in an arbitrary block-fading channel, and can be further extended to hybrid relaying. The conditions under which the DF and AF relaying have nearly identical performance are identified.

I. INTRODUCTION

Due to its numerous advantages (e.g. improved coverage, throughput, system capacity, power/battery life etc.), multi-hop relaying has recently attracted significant attention in both academia [1] and industry. Most common relaying strategies are decode-and-forward (DF) and amplify-and-forward (AF). While a DF relay decodes, re-modulates and retransmit the received signal, an AF one simply amplifies and retransmit the signal without decoding. Compared to an AF relay, the complexity of a DF one is significantly higher due to its full processing capability. The DF protocol also requires a sophisticated media access control layer, which is unnecessary in the AF protocol. Overall, a DF relay is nearly as complex as a base station. Does the performance improvement of DF relaying overweight its complexity burden? To answer this question (in part), the present paper will quantify this performance improvement.

There seems to be no consensus in the literature as to the question: What relaying protocol is better, AF or DF? While some studies find the DF protocol to be superior, others find the other way around. Indeed, it has been shown in [2] based on numerical simulations, that the AF multi-hop relaying outperforms the DF one under uncoded BPSK modulation in terms of outage probability and bit error rate (BER), which was explained by the error propagation effect in the DF relaying outweighing the noise amplification of the AF relaying. An analysis of a maximum likelihood demodulation presented in [3] for coherent cooperative diversity in uncoded BPSK systems shows that the DF relaying with more than one relay loses about half of the diversity of the AF relaying.

These studies, however, are limited to uncoded systems. Most modern communications systems rely on powerful channel codes and the uncoded results do not extrapolate directly to those systems. Indeed, it was shown in [4] that single-antenna multi-hop Rayleigh-fading relay channels under the DF protocol achieve higher ergodic (mean) capacity than under the AF one. A similar conclusion was obtained in [5] for the ergodic capacity of MIMO multi-hop relay systems. The study in [6] shows that the outage probability in multi-hop relay channels is higher under the AF protocol, which automatically transforms into smaller outage capacity. Therefore, one has to conclude that while the AF protocol is better for uncoded systems (where the error propagation effect outweighs the noise amplification), the opposite is true for systems using powerful capacity-approaching codes. Finally, the popular diversity-multiplexing framework (DMT, see e.g. [7]) has been also applied to relay channels [8][9]. We caution the reader that this framework, due to its asymptotic nature ($SNR \rightarrow \infty$), is known to provide misleading conclusions in many scenarios (including relay ones) as far as the finite-SNR performance is concerned [6][10].

In this paper, we consider coded systems via their capacity analysis (i.e. the fundamental limit to error-free data transmission) and quantify the performance superiority of the DF relaying over the AF one, for a fixed channel (or, alternatively, for a given realization of an arbitrary-fading channel), via two performance metrics: capacity and SNR gains. The main result is that, in an N-hop channel with multi-antenna source and destination and single-antenna relay nodes, the capacity gain of the DF relaying does not exceed $\log_2 N$ bit/s/Hz and its SNR gain does not exceed $N$. This conclusion also applies to selection relaying, to the outage probability/capacity and the ergodic capacity in an arbitrary block-fading channel, and can be further extended to hybrid relaying. The conditions under which the DF and AF relaying have nearly identical performance and, thus, the DF relaying is not worth the effort due to its higher complexity, are identified.

II. RELAY CHANNEL MODEL AND CAPACITY

Let us consider a multi-hop relay channel when the source (transmitter) and the destination (receiver) are equipped with multiple antennas, and the full-duplex relay nodes have a
single antenna, as shown in Fig. 1. In the paper, we assume that the channel is of linear topology, i.e. only adjacent relays can “see” each other [8] and there is no direct (source-destination) link (this is the case when relay nodes are needed most), and that the full CSI is available at the source and the destination.

A. Amplify-and-Forward Protocol

The signal received by i-th relay is \( y_i = h_i x_{i-1} + \xi_i \), \( i \geq 1 \), where \( x_{i-1} \) is the signal transmitted by (i-1)-th relay, \( h_i \) is the i-th hop channel (between (i-1) and i-th relays), and \( \xi_i \) is i-th relay AWGN noise, and we assume the baseband, discrete-time, frequency-flat channel model. The transmitted signal by i-th relay in the AF mode is \( x_i = \sqrt{K}/y_i \), where \( K \) is its power gain. Thus, the input-output relationship of the whole N-hop AF relay channel is

\[
y = \sqrt{K_{N-1}...K_1} h_N h_{N-1} \cdots h_1 x + \sqrt{K_{N-1}...K_1} h_N h_{N-1} \cdots h_2 \xi_1 + \cdots + \sqrt{K_{N-1}} h_N \xi_{N-1} + \xi_N
\]

(1)

where \( x \) and \( y \) are the transmitted (source) and received (destination) signal vectors, \( h_1, h_N \) are the 1-st and last hop channels (bold and regular characters denote vectors and scalars); note that 1-st and N-th hops are vector channels, all others are scalars, \( \xi_i \sim CN(0, \sigma_i^2) \), \( i = 1...N - 1 \), \( \xi_N \sim CN(0, \sigma_N^2) \). \( I \) is identity matrix, \( \ast \) denotes Hermitian conjugation. Without loss of generality, the relay power gains \( K_i \) are further absorbed into \( h_2...h_N \) via the substitution \( h_i \rightarrow \sqrt{K_{N-1}} h_i \).

To find the capacity of the channel in (1), consider the sufficient statistics for \( y \), which is (see e.g. [6][7]),

\[
z = |h_N|^{-1} h_N^\dagger y = |h_N|^{-1} h_N^\dagger x + |h_N|^{-1} h_N^\dagger h_2 \xi_1 + \cdots + |h_N|^{-1} h_N^\dagger \xi_{N-1} + h_N^\dagger \xi_N
\]

(2)

where \( |h|^2 = h^\dagger h \). The 1st term represents the signal received at the destination, and the other terms represent the relay noise propagated to the destination and the destination own noise. Note that sufficient statistics preserves the mutual information and capacity, as well as error rate under maximum-likelihood decoding, so that (2) is a scalar channel equivalent to (1). From this, the SNR at the destination can be expressed as

\[
g_N...g_2 h_N^\dagger R_s h_1/\sigma_y^2 \leq \sum_{k=1}^{N} g_k/\sigma_k^2 = \gamma_{AF}
\]

(3)

where \( R_s = E[xx^\dagger] \) is the covariance matrix of the source transmitted signal, \( \sigma_y^2 = tr R_s = E[xx^\dagger] \) is the total power, \( g_k = |h_k|^2 \) is the power gain of \( k \)-th hop channel, and \( \sigma_k^2 = \sigma_N^2 + \sum_{k=1}^{N-1} \sigma_k^2 \prod_{i=k+1}^{N} g_i \) is the total noise power at the destination. The inequality in (3) follows from \( h_1^\dagger R_s h_1 \leq |h_1|^2 \sigma_N^2 \), and the equality is achieved when \( R_s = \sigma_N^2 h_1 h_1^\dagger/|h_1|^2 \), i.e. beamforming from the source to the 1-st relay \( x = s \cdot h_1/|h_1| \), where \( s \) is the scalar transmitted symbol of the total power \( \sigma_N^2 \). From (2), achieving the upper bound in (3) also requires maximum ratio combining (MRC, also known as spatial matched filtering) at the destination.

The AF relay channel capacity, i.e. the ultimate bound to error-free data transmission under the AF protocol, can now be compactly expressed from the upper bound in (3) as

\[
C_{AF} = \log(1 + \gamma_{AF}) \text{[bit/s/Hz]}
\]

(4)

where \( \gamma_{AF} = (\sum_{i=1}^{N-1} \gamma_i^{-1})^{-1} \) is the equivalent SNR, i.e. an SNR in the AWGN channel that has the same capacity as the N-hop AF relay channel above, and \( \gamma_i = g_1...g_i \sigma_i^2/\sigma_N^2 \) is the SNR at i-th relay if all previous relays were noiseless \( (i = N \) corresponds to the destination), which is also the SNR at the destination when all the relays but i-th, and also the destination are noiseless. The capacity in (4) is achieved by the beamforming at the source (towards 1-st relay), the MRC at the destination and using a temporal capacity-achieving code on the equivalent scalar channel. Since \( \gamma_{AF} \) is an increasing function of \( \gamma_i \), each AF relay has to use the maximum available power/gain.

B. Decode-and-Forward Protocol

The system model in this case is

\[
y_1 = h_1 x + \xi_1, \ y_2 = h_2 x + \xi_2,..., \ y = h_N x + \xi_N.
\]

(5)

where \( x \) and \( y_i \), \( i = 1...N - 1 \), are the transmit and received signals at the relays. The DF relay channel capacity is limited by the weakest link,

\[
C_{DF} = \min_{i=1...N} \{C_i\} = \log(1 + \gamma_{DF})
\]

(6)

where \( C_i = \log(1 + \gamma_i) \) is the capacity of i-th hop, \( \gamma_i = g_i...g_i \sigma_i^2/\sigma_N^2 \) is the SNR at i-th relay, and \( \gamma_{DF} = \min_{i=1...N} \{\gamma_i\} \) is the effective SNR of an AWGN channel of the same capacity as the DF relay channel. This is also the relay channel capacity for the linear topology in Fig. 1. To make a fair comparison, we have set the transmitted signal power at each relay node to be equal to that in the AF protocol, i.e. \( g_1...g_N \sigma_N^2 \) for i-th relay.

Note that the capacity in (6) is achieved by beamforming at the source and MRC at the destination, in combination with a temporal capacity-achieving code for each hop (unlike the AF protocol, where a single temporal code is required for the whole channel).

III. COMPARISON OF AF AND DF PROTOCOLS

We are now in a position to compare the capacities in (4) and (6), which represent the ultimate rate bounds for coded systems under these protocols.

2When no source CSI is available, the best transmission strategy is isotropic signaling, \( R_s = \sigma_N^2 \mathbf{I}/n_s \) (see e.g. [6][7]), \( n_s \) is the number of source antennas, which achieves \( \gamma_{AF}/n_s \) at the destination, so that all the results below will hold with appropriately scaled SNR.

3The signal power constraint is the standard one for the RF/microwave amplifier design [11]. Some authors set the same total (signal + noise) power. Our analysis can be extended to that scenario as well. In particular, our lower bounds will hold and also the upper bounds in the high SNR regime.
Proposition 1: The capacity gain \( \Delta C = C_{DF} - C_{AF} \) of the DF relaying over the AF one in a N-hop relay channel in Fig. 1 is bounded as follows:

\[
0 \leq \Delta C \leq \log N \tag{7}
\]

for any channel realizations \( h_1, h_2, \ldots, h_N \). When \( C_{DF} < \infty \), the lower bound is achieved if and only if the destination and all the relays but one are noiseless. The upper bound is achieved if and only if all hops are equally strong and the SNR is sufficiently high, \( \gamma_1 = \gamma_2 = \ldots = \gamma_N \to \infty \).

Proof: Since \( \Delta C = \log [(1 + \gamma_{DF})(1 + \gamma_{AF})^{-1}] \), the lower bound follows from,

\[
\gamma_{AF} = (\gamma_1^{-1} + \ldots + \gamma_N^{-1})^{-1} \leq \min(\gamma_1, \ldots, \gamma_N) = \gamma_{DF}
\]

where the equality is achieved if and only if \( \gamma_k < \infty \) for some \( k \) and \( \infty \) otherwise, provided that \( \gamma_{DF} < \infty \). To prove the upper bound, let \( \gamma_{[1]} \leq \gamma_{[2]} \leq \ldots \leq \gamma_{[N]} \) be the ordered SNRs. Note that \( \gamma_{AF} \geq \gamma_{[1]}/N \) and \( \gamma_{DF} = \gamma_{[1]} \), so that

\[
\Delta C \leq \log N + \log[(1 + \gamma_{[1]})(N + \gamma_{[1]})^{-1}] \leq \log N
\]

The 1st inequality becomes equality when \( \gamma_1 = \gamma_2 = \ldots = \gamma_N \) and the 2nd one – when \( \gamma_{[1]} \to \infty \).

It follows from Proposition 1 that \( C_{DF} \geq C_{AF} \), i.e. the AF relaying is sub-optimal in general (for arbitrary channel realization). In practical terms, \( C_{DF} \approx C_{AF} \), i.e. no significant gain is provided by the DF relaying over AF one, when one relay (or the destination) is much weaker than the others, \( \gamma_{[1]} \ll \gamma_{[2]} \). Under such condition, the AF relaying is a preferable solution since DF one incurs a significant complexity penalty in the relay design and implementation, and its capacity \( C_{DF} = \log(1 + \gamma_{[1]}) \approx C_{AF} \) is almost the same as that of the AF one (dominated by the weakest hop). The gain is maximum when all hops are equally strong and, for a two-hop channel, it never exceeds 1 bit/s/Hz.

The advantage of the DF relaying over the AF one can also be cast in terms of an SNR gain. Define the SNR gain \( G \) of the DF relaying from the following:

\[
C_{AF}(G \gamma_0) = C_{DF}(\gamma_0) \tag{8}
\]

where \( \gamma_0 = \sigma^2_0/\sigma^2_K \) is the source SNR. It shows how much more SNR (or, equivalently, the source power) is required for the AF relaying to achieve the same capacity as the DF relaying. This gain can be characterized as follows.

Proposition 2: The SNR gain of DF relaying over AF one for the N-hop relay channel in Fig. 1 is bounded as follows:

\[
1 \leq G \leq N \tag{9}
\]

and the lower bound is achieved when the destination and all the relays but one are noiseless. The upper bound is achieved when all hops are equally strong, \( \gamma_1 = \gamma_2 = \ldots = \gamma_N \).

Proof: Follows along the same line as that of Proposition 1 using \( G = \gamma_{DF}/\gamma_{AF} \).

We note that an equivalent form of (9) is

\[
C_{AF}(\gamma_0) \leq C_{DF}(\gamma_0) \leq C_{AF}(N \gamma_0) \tag{10}
\]

The capacity gain \( \sigma^2_N = g_N \sigma^2_{K-1} = \ldots = g_N g_{N-1} \ldots g_2 \sigma^2_1 \) \( \gamma \)

i.e. the destination own noise power equals to the noise power of any relay propagated to the destination. This balance of all noise powers is required to exploit the full advantage of the DF relaying. When all noise powers are the same, i.e. \( \sigma^2_1 = \ldots = \sigma^2_N \), this reduces to \( g_N = \ldots = g_2 = 1 \), which is equivalent to \( h_i^2 K_{i-1} = 1 \), i.e. each relay compensates for the path loss of the hop following it.

An approximate (practical) condition for achieving the lower bound is \( \gamma_{[1]} \ll \gamma_{[2]} \). For a two-hop channel, this reduces to \( \sigma^2_2 \propto g_2 \sigma^2_1 \) or \( \sigma^2_2 \propto g_2 \sigma^2_1 \), i.e. either the destination is significantly more noisy than the relay (as seen at the destination) or the other way around \( \gamma \), which is illustrated in Fig. 2. This is the case when the DF relaying is not worth the complexity effort. In any case, the DF relaying outperforms the AF relaying by not more than 1 bit/s/Hz or 3 dB in a two-hop channel.

To capture the conditions when the upper and lower bounds are achieved in Propositions 1 and 2, we introduce the following definition.

Definition 1: The relay channel in Fig. 1 is balanced when \( \gamma_1 = \gamma_2 = \ldots = \gamma_N \) (the upper bounds are achieved in (9), and in (7) when the SNR is sufficiently high). The relay channel is misbalanced when \( \gamma_{[1]}/\gamma_{[2]} \to 0 \) (the lower bounds are achieved in (7) and (9)).

While Propositions 1 and 2 compare the DF and AF relaying for any given channel realization (or a fixed channel), the corresponding comparison can also be made for randomly-block-fading channels in terms of their two main performance metrics, outage probability and outage capacity [7]. In particular, the SNR gain bounds in (9) also apply to the latter metrics, and also to the ergodic capacity. The outage probability is

\[\text{e.g. when there is a line-of-sight (LOS) link between the base station and the relay, but no LOS between the relay and a mobile user.}\]
defined as [7],

\[ P_{out}(\gamma_0) = \Pr \{ C(\gamma_0) < R \} \]  \hspace{1cm} (12)

i.e. the probability that the channel is not able to support the target rate \( R \), where \( C(\gamma_0) \) is the instantaneous channel capacity. We further comment that the channel outage probability is also the best achievable codeword error probability. It follows from (10) that, for any fading distribution,

\[ P_{out}^{AF}(N\gamma_0) \leq P_{out}^{DF}(\gamma_0) \leq P_{out}^{AF}(\gamma_0) \]  \hspace{1cm} (13)

From this, the DF relaying has at most \( N \)-fold SNR gain over the AF relaying in terms of the outage probability, i.e. as in (9), and the DF and AF relaying have the same diversity gain (under arbitrary fading distribution). The outage capacity is the largest rate such that the outage probability does not exceed a given threshold \( \epsilon \) [7],

\[ C_{\epsilon}(\gamma_0) = \max \{ R : P_{out}(\gamma_0, R) \leq \epsilon \} \]  \hspace{1cm} (14)

where \( P_{out}(\gamma_0, R) \) denotes the outage probability as a function of the SNR \( \gamma_0 \) and the target rate \( R \). Using this definition and (13), it follows that

\[ C_{\epsilon}^{AF}(\gamma_0) \leq C_{\epsilon}^{DF}(\gamma_0) \leq C_{\epsilon}^{AF}(N\gamma_0) \]  \hspace{1cm} (15)

so that the SNR gain of the DF relaying in terms of the outage capacity does not exceed \( N \) either. From (10), the same inequity also holds in terms of the ergodic (mean) capacity \( C(\gamma_0) : C_{DF}(\gamma_0) \leq C_{DF}(\gamma_0) \leq C_{AF}(N\gamma_0) \).

Note that the results above hold for arbitrary fading distribution. They can also be extended to more complicated relay channel topologies under selection relaying, which is done in the next section.

IV. SELECTION RELAYING

Let us now consider a two-hop relay channel under selection relaying, where only the best relay node (out of \( N \)) is used at any time. It is motivated by its low complexity and also by the fact that little interference is created to other users since only one relay is transmitting [9]. Below, we compare the DF and AF protocols for this selection relaying scheme.

Proposition 3: The capacity gain \( \Delta C = C_{DF} - C_{AF} \) and the SNR gain \( G = \gamma_{DF}/\gamma_{AF} \) of the DF relaying over the AF relaying in a two-hop selection relaying channel are bounded as follows:

\[ 0 \leq \Delta C \leq 1 \text{ bit/s/Hz}, \quad 1 \leq G \leq 2 \]  \hspace{1cm} (16)

for any channel realization. The lower bounds are achieved when either the destination or the best DF relay is noiseless, i.e. the channel is misbalanced. The upper bounds are achieved when the best AF and DF relays are the same, its two hops are equally strong, i.e. the channel is balanced, \( \gamma_1 = \gamma_2 \) and, for the capacity gain, the SNR is sufficiently high, \( \gamma_1 = \gamma_2 \rightarrow \infty \).

Note that the bounds in (16) are independent of the total number of nodes \( N \) (out of which the best one is selected) and are the same as in (7) and (9) for \( N = 2 \), i.e. selection relaying in a two-hop channel does not improve the maximum possible gain of the DF over AF relaying.

We note that these selection relaying results can also be extended to the \( N \)-hop selection relaying, as in Fig. 3, using the same reasoning as above.

Proposition 4: The capacity gain \( \Delta C \) and the SNR gain \( G \) of the DF relaying over the AF relaying in a \( N \)-hop selection relaying channel in Fig. 3 are bounded as follows:

\[ 0 \leq \Delta C \leq \log N, \quad 1 \leq G \leq N \]  \hspace{1cm} (17)

The lower bounds are achieved when the destination and all the relays but one of the best DF relaying path are noiseless (misbalanced channel). The upper bounds are achieved when the best DF and AF relaying paths are the same and all the hops of the best path are equally strong (balanced channel) and, for the capacity gain, the SNR is sufficiently high, \( \gamma_1 = \gamma_2 = \cdots = \gamma_N \rightarrow \infty \).

Finally, we point out that similar results also hold for a hybrid relaying scheme, where some of the relay nodes are DF ones and the rest are AF, and that all the bounds also extend to the outage probability/capacity and the ergodic capacity under arbitrary fading distribution, as discussed in Section III.

REFERENCES

Complexity analysis for ML-based sphere decoder achieving a
vanishing performance-gap to brute force ML decoding

Arun Singh and Petros Elia
Mobile Communications Department
EURECOM, Sophia Antipolis, France
Email: {singhak, elia}@eurecom.fr

Joakim Jaldén
ACCESS Linnaeus Center, Signal Processing Lab
School of Electrical Engineering, KTH, Stockholm, Sweden
Email: jalden@kth.se

Abstract—This work identifies the computational resources re-
quired for the maximum likelihood (ML)-based sphere decoding
solutions that achieve, in the high-rate and high-SNR limit, a
vanishing gap to the error-performance of the optimal brute
force ML decoder. These error performance and complexity
guarantees hold for most multiple-input multiple-output scen-
arios, all reasonable fading statistics, all channel dimensions and
all full-rate lattice codes. The analysis also identifies a rate-
reliability-complexity tradeoff establishing concise expressions for
the optimal diversity gain achievable in the presence of any
run-time constraint imposed due to the unavailability of enough
computational resources required to achieve a vanishing gap.

I. INTRODUCTION

For multiple-input multiple-output (MIMO) systems, error
probability and encoding-decoding complexity are widely con-
sidered to be two limiting and interrelated bottlenecks (cf.
[1], [2]). Specifically, if a small gap to the brute-force maxi-

mum likelihood (ML) performance is acceptable then different
channel matrices [1], [2]) have been known to provide a complexity-performance
tradeoff. Albeit suboptimal in terms of the error-performance,
these SD based solutions might result in a preferable rate-

tradeoff. We consider general m × n point-to-point MIMO channel represen-
tation

\[ y = \sqrt{\rho} H x + w \]  

(1)

where \( x \in \mathbb{R}^m \), \( y \in \mathbb{R}^n \) and \( w \in \mathbb{R}^n \) respectively
describe the transmitted codewords, the received signal vectors, and
the additive white Gaussian noise with unit variance, where \( \rho \)
denotes the signal to noise ratio (SNR), and where the fading matrix
\( H \in \mathbb{R}^{n \times m} \) is assumed to be random, with elements
drawn from arbitrary statistical distributions.

The sphere decoding solutions require that the underlying code
be linear, an assumption that we adopt here and consider
encoding and decoding schemes relating to real lattices (cf.
[5]). Specifically for \( r \geq 0 \), a (sequence of) full-rate
(lattice) code(s) \( X_r \) is given by \( X_r = \Lambda_r \cap R \) where the
shaping region \( R \) is a compact convex subset of \( \mathbb{R}^n \) that is
independent of \( \rho \), where \( \Lambda_r \triangleq \rho^{-\frac{r}{2}} \Lambda \) and \( \Lambda \triangleq \{ Gs \ | \ s \in \mathbb{Z}^n \} \),
where \( \mathbb{Z}^n \) denotes the \( n \) dimensional integer
lattice, and where generator matrix \( G \in \mathbb{R}^{m \times n} \) is full rank

and independent of \( \rho \). After vectorization the codewords take the
form

\[ x = \rho^{-\frac{r}{2}} Gs, \quad s \in S_r \triangleq \mathbb{Z}^n \cap \rho^{-\frac{r}{2}} R, \]  

(2)

where \( R \subset \mathbb{R}^n \) is a natural bijection of the shaping region \( \rho R \)
that preserves the code, and contains the all zero vector \( 0 \). For
simplicity we consider \( R \triangleq [-1, 1]^n \) to be a hypercube in \( \mathbb{R}^n \),
although this could be relaxed. Combining (1) and (2) yields
the equivalent system model

\[ y = M s + w, \]  

(3a)

where \( M = \rho^{-\frac{r}{2}} H G \in \mathbb{R}^{n \times n} \).  

(3b)

B. Sphere Decoder

Let \( QR = M \) be the thin \( QR \) factorization of the code-
channel matrix \( M \) and \( r = Q^H y \), then (3a) yields \( r = R \hat{s} + Q^H w \) and the ML decoder for this system takes the form

\[ \hat{s}_{ML} = \arg \min_{\hat{s} \in \mathbb{Z}^n} ||r - R \hat{s}||^2. \]  

(4)

We use SD to implement the decoder in (4), which identifies
as candidates the vectors \( \hat{s} \in S_r \) that for some search radius
\( \xi > 0 \), satisfy \( ||r - R \hat{s}||^2 \leq \xi^2 \). The algorithm specifically
uses the upper-triangular nature of \( R \) to recursively identify
partial symbol vectors \( \hat{s}_k, k = 1, \ldots, \kappa \), for which

\[ ||r_k - R_k \hat{s}_k||^2 \leq \xi^2, \]  

(5)

where \( \hat{s}_k \) and \( r_k \) respectively denote the last \( k \) components of
\( \hat{s} \) and \( r \), and where \( R_k \) denotes the \( k \times k \) lower-right submatrix
of \( R \).

We note that the error performance and the total number of
visited nodes is a function of the search radius \( \xi \). We use fixed
search radius \( \xi = \sqrt{\rho} \log \rho \) for some \( \rho > k d(r) \) such

\[ P \left( ||Q^H w||^2 > \xi^2 \right) \leq P \left( ||w||^2 > \frac{\xi^2}{\kappa} \right) \leq \rho^{-d(r)}, \]  

(6)

which implies a vanishing probability of excluding the trans-
mitted information vector from the search. We use \( \xi \) to denote
the exponential equality, i.e., we write \( f(\rho) \approx \rho^B \) to denote

\[ \lim_{\rho \to \infty} \frac{\log f(\rho)}{\log \rho} = B, \]  

and \( \leq, \geq \) are defined similarly.
C. Rate-reliability-complexity tradeoff in outage-limited MIMO communications

In the high SNR regime, a given encoder \( \mathcal{X} \) and decoder \( \mathcal{D} \) are said to achieve a multiplexing gain \( r \) and diversity gain \( d_\mathcal{D}(r) \) if (cf. [1])

\[
\lim_{\rho \to \infty} \frac{R(\rho)}{\log \rho} = r, \quad \text{and} \quad -\lim_{\rho \to \infty} \log \frac{P_e}{\log \rho} = d_\mathcal{D}(r)
\]

where \( P_e \) denotes the probability of codeword error with a ML-based sphere decoder \( \mathcal{D} \), employing time-out policies.

We characterize complexity in terms of the complexity exponent (cf. [4], [6]). Let \( N_{\text{max}} \) denote the amount of computational resources, in floating point operations (flops) per \( T \) channel uses, that the transceiver is endowed with, in the sense that after \( N_{\text{max}} \) flops, the transceiver must simply terminate, potentially prematurely and before completion of its task. The complexity exponent then takes the form

\[
c(r) := \lim_{\rho \to \infty} \frac{N_{\text{max}}}{\log \rho}.
\]

We note that the complexity exponent is intimately intertwined with the achievable error performance and that any attempt to reduce \( c(r) \) may be at the expense of a substantial degradation in error-performance.

For ML-based SD a vanishing performance gap to ML can, in the high SNR regime, be quantified as

\[
g(c) := \lim_{\rho \to \infty} \frac{P_e}{\log \rho} = 1
\]

where \( P(\hat{s}_{\text{ML}} \neq s) \) describes the error probability of the brute force ML decoder, and where \( c \) is the complexity exponent that describes the computational resources required to achieve this performance gap. Generally a smaller performance gap requires a larger complexity exponent.

At this point a natural question to ask would be - how large computational resources are required to achieve a vanishing gap to the brute force ML performance. While this question was first addressed and partially answered in [4] for the specific settings of i.i.d. Rayleigh fading quasi-static channels with specific channel dimensions, specific codes, and specific permutation orderings, we here provide answers for the most general MIMO settings, i.e., for all reasonable fading statistics, all channel dimensions, all MIMO scenarios and all full-rate lattice codes.

II. COMPLEXITY OF ML-BASED SPHERE DECODING

The total number of visited nodes is commonly taken as a measure of the sphere decoder complexity which is given by

\[
N_{SD} = \sum_{k=1}^{\kappa} N_k,
\]

where \( N_k \) denotes the number of visited nodes at layer \( k \) that corresponds to the \( k \)th component of the transmitted symbol vector \( s \) and is given by \( N_k \triangleq |N_k| \) where \( N_k \triangleq \{ \hat{s}_k \in \mathbb{S}_k^c \mid \| \mathbf{r}_k - \mathbf{R}_k \hat{s}_k \| \leq \xi^2 \} \).

At this point we want to clarify that the analysis presented here is specific to sphere decoding, and that it does not account for any other ML based solutions that could, under some (arguably rare) circumstances, be more efficient. A classical example of such rare circumstances would be a MIMO scenario, or equivalently a set of fade statistics, that always generate diagonal channel matrices.

We are interested in the ML-based SD complexity required to achieve a vanishing gap to brute force ML performance. We recall that a ML-based SD with run-time constraints, in addition to making the ML errors \( \hat{\mathcal{S}}_{\text{ML}} \neq \mathcal{S} \), also makes errors when the run-time limit of \( \rho^x \) flops for \( x > c(r) \) becomes active, as well as when the fixed search radius \( \xi \) causes \( N_k = 0 \). Consequently the corresponding performance gap to the brute force ML decoder, takes the form (cf. (9))

\[
g(x) = \lim_{\rho \to \infty} \frac{P(\hat{\mathcal{S}}_{\text{ML}} \neq \mathcal{S} \cup \{ N_{SD} \geq \rho^x \} \cup \{ N_k = 0 \})}{P(\hat{\mathcal{S}}_{\text{ML}} \neq \mathcal{S})} = 0.
\]

Now going back to (8), and having in mind appropriate timeout policies that guarantee a vanishing gap, the complexity exponent \( c(r) \) can be bounded as \( c(r) \leq c(r) \leq \tau(r) \), where

\[
\tau(r) \triangleq \inf \{ x \mid -\lim_{\rho \to \infty} \log \frac{P(\mathcal{N}_k \geq \rho^x)}{\log \rho} > d(r) \},
\]

\[
\tau(r) \triangleq \sup \{ x \mid -\lim_{\rho \to \infty} \log \frac{P(\mathcal{N}_k \geq \rho^x)}{\log \rho} < d(r) \},
\]

respectively denote sufficient and necessary conditions that guarantee a vanishing gap to ML performance.

Though our complexity results are applicable for all channel dimensions, we here assume\(^2\) \( n \geq m \) and define \( \mu_i \triangleq \frac{-\log \mu_i(\mathbb{H}^T \mathbb{H})}{\log \rho} \), \( i = 1, \cdots, m \). The upper bound follows from [4, Theorem 2] and is given by

\[
\tilde{c}(r) \triangleq \max_{\mu} \min_{\kappa} \sum_{i=1}^{\kappa} \left( \frac{\tau T}{\kappa} - \frac{1}{2}(1 - \mu_k) \right) \frac{(\tau T - 1/2)}{\kappa} +
\]

\[
\text{s.t. } I(\mu) \leq d(r),
\]

\[
\mu_1 \geq \cdots \geq \mu_k \geq 0,
\]

where \( \mu \triangleq (\mu_1, \cdots, \mu_k) \) satisfies the large deviation principle with rate function \( I(\mu) \). Equivalently for \( \mu^* \triangleq (\mu_1^*, \cdots, \mu_k^*) \) being one of the maximizing vectors such that \( I(\mu^*) = d(r) \),

\[^2\]For \( n < m \), we can consider a new \( \tilde{\mathcal{G}} = \tilde{U}^T \mathcal{G} \in \mathbb{R}^{n \times n} \) which is full-rank and square matrix, and where \( \tilde{U} \in \mathbb{R}^{n \times n} \) has orthogonal columns and a new \( \tilde{\mathbf{H}} = \tilde{U} \tilde{U}^T \in \mathbb{R}^{n \times n} \). As no explicit assumption is made regarding the fading distribution of \( \tilde{\mathbf{H}} \), results will directly apply for \( \mathbf{H} \) and \( \mathcal{G} \).
we have that \( \hat{c}(r) = \sum_{i=1}^{\kappa} \min \left( \frac{\kappa}{n} - \frac{1}{2} (1 - \mu^*_i), \frac{\kappa}{n} \right) \). Furthermore, given the monotonicity of the rate function \( I(\mu) \), and the fact that the objective function in (12) does not increase in \( \mu_i \), beyond \( \mu_i = 1 \), we may also assume without loss of generality that \( \mu^*_i \leq 1 \) for \( i = 1, \ldots, \kappa \). It then follows that

\[
\tau(r) \leq \hat{c}(r) = \sum_{i=1}^{\kappa} \left( \frac{\kappa}{n} - \frac{1}{2} (1 - \mu^*_i) \right). \tag{13}
\]

A. Universal Lower Bound on Complexity

In this section we establish that \( \hat{c}'(r) = \hat{c}(r) \), i.e., the sphere decoder visits a total number of nodes that is close to \( \rho^{\hat{c}(r)} \) with a probability that is large compared to the probability of decoding error \( P(\hat{S}_{ML} \neq S) \approx \rho^{-\hat{c}(r)} \).

We let \( q \in [1, \kappa] \) be the largest integer for which \( \frac{\kappa}{n} - \frac{1}{2} (1 - \mu^*_i) > 0 \), in which case (13) takes the form

\[
\hat{c}(r) = \sum_{i=1}^{q} \left( \frac{\kappa}{n} - \frac{1}{2} (1 - \mu^*_i) \right). \tag{14}
\]

We quickly note that without loss of generality we can assume that \( q \geq 1 \) as otherwise \( \hat{c}(r) = c(r) = 0 \). Consequently it is the case that \( \mu^*_i > 0 \) for \( i = 1, \ldots, q \).

We proceed to define three events \( \Omega_1, \Omega_2, \Omega_3 \) which we will prove to be jointly sufficient so that the total number of nodes visited by the sphere decoder, employing a channel dependent fixed decoding order, is close to \( \rho^{c(r)} \). These events are given by

\[
\Omega_1 \triangleq \{ \mu^*_i - 2 \delta < \mu_i < \mu^*_i - \delta, j = 1, \ldots, q \}
\]

\[0 < \mu_i < \delta, i = q + 1, \ldots, \kappa\}, \tag{15}\]

for a given small \( \delta > 0 \),

\[
\Omega_2 \triangleq \left\{ \|w\|^2 < \frac{\xi^2}{\kappa} \right\}, \tag{16}\]

\[
\Omega_3 \triangleq \left\{ \|s\| < \frac{1}{2} \rho^{\frac{c(r)}{\kappa}} \right\}. \tag{17}\]

Note also that by choosing \( \delta \) sufficiently small, and using the fact that \( \mu^*_i > 0 \) for \( i = 1, \ldots, q \), we may without loss of generality assume that \( \Omega_1 \) implies that \( \mu_i > 0 \) for all \( i = 1, \ldots, \kappa \).

Following the footsteps of [4, Lemma 2] it can be shown that in the presence of events \( \Omega_1, \Omega_2, \Omega_3 \) we can remove the ML-based SD boundary constraints \( \mathbb{S}_n^\kappa \) (cf. (4)). This removal allows us to lower bound the number of nodes visited at layer \( k \) as (cf. [4, Lemma 1])

\[
N_k \geq \frac{k}{2} \frac{2 \xi}{\sqrt{\kappa} \sigma_r(R_k)} \left[ \sqrt{\kappa} \right]. \tag{18}\]

In the following, and up until (28), we will work toward upper bounding \( \sigma_i(R_k) \) for the case of \( q \in [1, \kappa-1] \), the case of \( q = \kappa \) is treated separately later on. Towards this we first consider a Greedy QR decomposition. The diagonal elements of \( \check{R} \) satisfy \( \check{r}_{11} \geq \cdots \geq \check{r}_{pp} \). Let \( M_{ip} \in \mathbb{R}^{n \times p} \) contains the first \( p \) columns of \( M \). It then follows that

\[
M_{ip} \triangleq M_{P} = \tilde{Q} \check{R}_p, \tag{19}\]

where, \( \Pi_p \) and \( \check{R}_p \) denote the sub matrices consisting of the first \( p \) columns of \( \Pi \) and \( \check{R} \) respectively. Now let \( R_p \) be the \( p \times p \) upper triangular matrix consisting of the first \( p \) rows of \( \check{R}_p \), then we get that \( \sigma_1(M_{ip}M_{ip}) = \sigma_i(R_p^H R_p) \) for \( i = 1, \ldots, p \). For \( R_p^H R_p \), having diagonal entries \( \check{r}_{11}^2 \geq \cdots \geq \check{r}_{pp}^2 \) and singular values \( \sigma_1(M_{ip}M_{ip}) \leq \cdots \leq \sigma_p(M_{ip}M_{ip}) \), we have that for \( k = 1, \ldots, p \) then (cf. [8, Theorem 2.3])

\[
\prod_{i=1}^{k} \check{r}_{ii}^2 \leq \prod_{i=1}^{k} \sigma_{p-i+1}(M_{ip}M_{ip}). \tag{20}\]

From [7, Lemma 4.3] regarding the Greedy QR decomposition, we have that \( \check{r}_{kk}^2 \geq \sigma_{k-i+1}(M^H M) \) for \( k = 1, \ldots, p \), and it follows that

\[
\prod_{i=1}^{k} \check{r}_{ii}^2 \geq \prod_{i=1}^{k} \sigma_{k-i+1}(M^H M) / \kappa - i + 1. \tag{21}\]

Consequently we have that for \( k = 1, \ldots, p \)

\[
\sigma_{k-p+1}(M_{ip}M_{ip}) \geq \sigma_{k-i+1}(M^H M) \prod_{i=1}^{k} \frac{1}{2mT - i + 1}. \tag{22}\]

We then have \( \sigma_{k-p+1}(M_{ip}M_{ip}) \leq \sigma_{k-i+1}(M^H M), k = 1, \ldots, p \) (cf. [9, Theorem 4.3.15]), and it follows that for \( k = 1, \ldots, p \)

\[
\sigma_{k-p+1}(M_{ip}M_{ip}) \leq \sigma_{k-i+1}(M^H M). \tag{23}\]

Recalling that \( \sigma_1(M^H M) \leq \cdots \leq \sigma_m(M^H M) \), we have that \( \sigma_1(M_{ip}M_{ip}) \geq \sigma_i(M^H M) \) for \( i = 1, \ldots, q \). \( \tag{24}\)

The above inequality allows us to apply Lemma 3 from [4], which in turn gives that

\[
\sigma_i(R_k) \leq \sigma_1(M) + 1 \, \sigma_i(M) = \left[ \sigma_{q+1}(M) + 1 \right] \sigma_i(M), \tag{25}\]

for \( i = 1, \ldots, q \), where exponential equality follows from (23). From (3b) for \( i = 1, \ldots, \kappa \), we have that

\[
\sigma_i(M) \leq \rho^{-\delta(i) + \frac{1}{2}(1-\mu_i)}. \tag{26}\]

Furthermore (15) gives that

\[
\sigma_1(R_k) \leq \rho^{-\delta(i) + \frac{1}{2}(1-\mu_i)} \quad \text{for} \quad i = 1, \ldots, q \tag{27a}\]

\[
\sigma_1(M) \leq \rho^{-\delta(i) + \frac{1}{2}(1-\mu_i)} \leq \rho^{-\delta(i) + \frac{\kappa}{n}}, \tag{27b}\]

\[
\sigma_{q+1}(M) \geq \rho^{-\delta(i) + \frac{1}{2}(1-\mu_{q+1})} \geq \rho^{-\delta(i) + \frac{1}{2}(1-\delta)}. \tag{27c}\]

Substituting (27) in (25) gives that

\[
\sigma_i(R_k) \leq \rho^{-\delta(i) + \frac{1}{2}(1-\mu_i)} \quad \text{as} \quad i = 1, \ldots, q. \tag{28}\]
Consequently, going back to (18), we have that
\[
2\kappa \sqrt{\frac{2\kappa}{\sqrt{k\sigma(R_k)}}} - \sqrt{k} \geq \rho \left( \frac{2\kappa}{\sqrt{k\sigma(R_k)}} - \frac{2}{\sqrt{k}}(1-\mu_i^*) \right).
\] (29)

As a result, for \( k = q \) with \( q \in [1, K-1] \) we have that
\[
N_q \geq \rho \sum_{i=1}^{q} \left( \frac{2\kappa}{\sqrt{k\sigma(R_k)}} - \frac{2}{\sqrt{k}}(1-\mu_i^*) \right) = \rho \left( \frac{2\kappa}{\sqrt{k\sigma(R_k)}} - \frac{2}{\sqrt{k}}(1-\mu_i^*) \right),
\] (30)

where the last equality follows from (14). For the case of \( q = K \), from (18) and (27a) we have that
\[
N_K \geq \rho \sum_{i=1}^{K} \left( \frac{2\kappa}{\sqrt{k\sigma(R_k)}} - \frac{2}{\sqrt{k}}(1-\mu_i^*) \right) = \rho \left( \frac{2\kappa}{\sqrt{k\sigma(R_k)}} - \frac{2}{\sqrt{k}}(1-\mu_i^*) \right).
\] (31)

Consequently for \( q \in [1, K] \) we have that \( N_{SD} \geq \rho \left( \frac{2\kappa}{\sqrt{k\sigma(R_k)}} - \frac{2}{\sqrt{k}}(1-\mu_i^*) \right) \) for small \( \delta > 0 \), where \( K \in \left( \frac{2\kappa}{\sqrt{k\sigma(R_k)}} \right) \).

We note that (15)-(17) jointly imply that \( N_{SD} \geq \rho \left( \frac{2\kappa}{\sqrt{k\sigma(R_k)}} - \frac{2}{\sqrt{k}}(1-\mu_i^*) \right) \). For some \( \delta' \equiv K\delta + \delta_1 \), where \( \delta > \delta_1 > 0 \), it follows that
\[
P \left( N_{SD} \geq \rho \left( \frac{2\kappa}{\sqrt{k\sigma(R_k)}} - \frac{2}{\sqrt{k}}(1-\mu_i^*) \right) \right) \geq P \left( \Omega_1 \cap \Omega_2 \cap \Omega_3 \right) \geq P \left( \Omega_1 \right) \] (32)

where exponential equality follows from the independence of the events \( \Omega_1, \Omega_2 \) and \( \Omega_3 \) and from the fact that \( P \left( \Omega_2 \right) \geq \rho^0 \) (cf.(6)) and \( P \left( \Omega_3 \right) \geq \rho^0 \). With \( \Omega_1 \) being an open set, we have that
\[
- \lim_{\rho \to \infty} \frac{P \left( \Omega_1 \right)}{\log \rho} \leq \inf_{\mu \in \Omega_1} I(\mu) = I(\tilde{\mu}) < I(\mu^*) = d(r) \] (33)

where \( \tilde{\mu} = \{ \mu_i^* - 2\delta, \ldots, \mu_n^* - 2\delta, 0, \ldots, 0 \} \), where the last inequality follows from the monotonicity of the rate function \( I(\mu) \) and where the last equality follows from the fact that, by definition, \( I(\mu^*) = d(r) \).

Consequently (32) and (33) along with the definition of the lower bound in (11b) imply that \( c(r) = \tilde{c}(r) \), for arbitrarily small \( \delta > 0 \). The following lemma directly holds corresponding to a vanishing performance gap.

**Lemma 1:** Irrespective of channel fading statistics and of the full-rate code applied, for every realization of channel \( M \) there exists a channel dependent column permutation matrix \( \Pi \) such that the ML-based sphere decoder with decoding order \( \Pi \) has the complexity exponent \( c(r) = \tilde{c}(r) \).

To show the dependence of the complexity exponent \( c(r) \) on the ML-based sphere decoder, we consider the following theorem.

**Theorem 1:** For any full-rate code and fading distribution such that \( P \left( \Pi_M = \Pi_k \right) > \epsilon \), for some \( \epsilon > 0 \), the complexity exponent of the ML-based sphere decoder with any fixed decoding order is given by \( c(r) = \tilde{c}(r) \).

**IV. CONCLUSIONS**

The presented performance guarantees hold for the most general MIMO settings, i.e., for all reasonable fading statistics, all channel dimensions, all MIMO scenarios and all full-rate lattice codes. Such guarantees may be utilized for the practical implementation of telecommunication systems.

**REFERENCES**


Symbol-by-symbol APP Decoding based on Supercode Decoding

Jürgen Freudenberger
and Uwe Kaiser
HTWG Konstanz
University of Applied Sciences, Konstanz, Germany
Institute for System Dynamics (ISD)
Email: juergen.freudenberger@htwg-konstanz.de

Abstract—An efficient sub-optimum symbol-by-symbol soft in/soft-out a posteriori probability (APP) decoding algorithm for linear binary block codes is presented. The three-step decoding procedure consists of: 1) list decoding of two supercodes, 2) calculating the intersection of these two lists, and 3) symbol-by-symbol APP decoding for the intersection. The presented results indicate that the proposed decoding procedure obtains good estimates of the ideal soft-output values and reduces the decoding complexity significantly. It may be an attractive alternative to conventional implementations of APP decoding.

I. INTRODUCTION

Most commonly, symbol-by-symbol a posteriori probability (APP) decoding of block codes is implemented by representing the code as a graph, the so-called trellis, and applying the well-known BCJR algorithm [1]. Alternative implementations of soft in/soft-out decoding are based on the soft-output Viterbi algorithm [2] or sub-optimum versions of the BCJR algorithm [3].

In this paper we consider a different approach which is based on the concept of supercode decoding introduced by Barg et al. [4]. The algorithm from [4] actually combines several previously known decoding strategies for discrete memoryless channels with the new idea of supercode decoding. A generalization of all employed decoding steps to channels with continuous output alphabets appears to be difficult. Therefore, we concentrate on the problem of supercode decoding. Consequently the intermediate decoding steps differ from that described in [4]. In particular we present efficient solutions to the problems: 1) list decoding of supercodes and 2) calculating the intersection \( L = \bigcap_i L_i \). The list \( L \) is represented as a trellis and the final decoding step 3) can be performed using, for example, Viterbi decoding in this trellis. Such a trellis based supercode decoding was devised and investigated for the binary symmetrical channel (BSC) in [5].

Example 1: Consider for example the code \( C = \{(0000), (1110), (1011), (0101)\} \) with parity-check matrix

\[
H = \begin{pmatrix}
1 & 1 & 0 & 1 \\
0 & 1 & 1 & 1 
\end{pmatrix}
\]

We obtain

\[
H_1 = \begin{pmatrix}
1 & 1 & 0 & 1 
\end{pmatrix}
\]

\[
C_1 = \{(0000), (1100), (1110), (0010), (1011), (1001), (1011), (0101)\}
\]

and

\[
H_2 = \begin{pmatrix}
0 & 1 & 1 & 1 
\end{pmatrix}
\]

\[
C_2 = \{(0000), (1000), (0110), (1110), (1011), (1101), (0011), (0101)\}
\]
where the underlined vectors are the codewords of the code \( C \).

Supercode decoding is performed in three steps:

1) List decoding of each supercode \( C_i \) such that the transmitted codeword is in the list \( L_i \), provided that the weight of the error pattern is less or equal \( \rho \).

2) Calculating the intersection \( \mathcal{L} = \cap L_i \). These are the codewords of the code \( C \) that are in the ball around the received sequence.

3) Applying symbol-by-symbol soft in/software decoding to the list \( \mathcal{L} \).

The idea here is that list decoding of the supercodes is less complex than a decoding approach which is based on the code itself. The supercodes are represented by their minimal trellis [6]. The first decoding step is performed by a marking algorithm which labels all state transitions in a supercode trellis that corresponds to a codeword in the list \( \mathcal{L}_i \).

The list \( \mathcal{L} \) is also represented by a trellis. This trellis is constructed using the merging algorithm. The merging algorithm calculates the intersection \( \mathcal{L} = \cap \mathcal{L}_i \) by merging the labeled state transitions from both supercode trellises.

Before we describe the algorithm’s implementation we introduce the data structures which the trellis is composed of.

III. TRELLIS REPRESENTATION

A trellis \( T = (S, W) \) is a directed graph with a set of states \( S = \{ \sigma \} \) and a set of branches \( W = \{ w \} \) which connects the nodes. The set \( S \) can be split into \( n + 1 \) subsets \( S = S_0 \cup S_1 \cup \cdots \cup S_n \), where \( n \) denotes the length of the code. Such a subset is also called a level \( S_i \) of the trellis. Each branch \( w \) has a label \( b \in \{ 0, 1 \} \) which represents the code symbol \( v_i(w_i) \).

To represent the trellis, three data structures are used. One for the node \( \sigma \), a list of nodes for a level \( S_i \), and a list of the list of nodes for the complete trellis \( S \). The branches \( W \) are references which are stored in the nodes.

A node can have up to two predecessors \( N_0^P(\sigma) \) and successors \( N_0^S(\sigma) \), \( b \in \{ 0, 1 \} \). The references to the predecessors and successors are assigned to zero if there is no corresponding node. Each incoming branch \( w_i^P \) which connects \( \sigma \) with \( N_0^P(\sigma) \) and outgoing branch \( w_i^S \) which connects \( \sigma \) and \( N_0^S(\sigma) \) has a metric. We differentiate between two metric values. The forward metric \( \Lambda^F(\sigma) \), which is the metric between \( \sigma \) and \( N_0^S(\sigma) \), and the backward metric \( \Lambda^B(\sigma) \), which is the metric between \( \sigma \) and \( N_0^S(\sigma) \). Furthermore a node stores the markings \( M_0(\sigma) \) for the outgoing branches \( w_i^S \). Hence, a node of the super code trellises can be described as a 10-tupel.

\[
\sigma = (\Lambda_0^B(\sigma), \Lambda_0^F(\sigma), \Lambda_0^L(\sigma), \Lambda_0^U(\sigma), N_0^P(\sigma), N_0^S(\sigma), N_0^U(\sigma), M_0(\sigma), M_1(\sigma))
\]

These nodes are used to construct the trellises of the supercodes. For the trellis representing the list \( \mathcal{L} \) we have to extend the node with four attributes. Two references \( N^{(1)}(\sigma) \) and \( N^{(2)}(\sigma) \) which point to the corresponding nodes in the supercode trellises. Additionally the level \( L(\sigma) \) of the node and a visited flag \( V(\sigma) \) were added to implement the breath first search efficiently. Thus, a node of the trellis can be described as a 14-tupel.

\[
\sigma = (\Lambda_0^B(\sigma), \Lambda_0^F(\sigma), \Lambda_0^L(\sigma), \Lambda_0^U(\sigma), N_0^P(\sigma), N_0^S(\sigma), N_0^U(\sigma), N^{(1)}(\sigma), N^{(2)}(\sigma), M_0(\sigma), M_1(\sigma), V(\sigma), L(\sigma))
\]

The implementation uses three trellises for decoding. The two supercode trellises \( T^{(1)} \) and \( T^{(2)} \) for the supercodes \( C_1 \) and \( C_2 \), and the trellis \( T \) for the code \( C \). Each node \( \sigma \) in \( T \) has a reference to a node \( \sigma^{(1)} \) in \( T^{(1)} \) and \( \sigma^{(2)} \) in \( T^{(2)} \), such that

\[
\sigma = \left( \begin{array}{c}
\sigma^{(1)} \\
\sigma^{(2)}
\end{array} \right).
\]

IV. SUPERCODE DECODING

The first step of supercode decoding is list decoding of each supercode \( C_i \) such that the transmitted codeword is in the list \( L_i \) provided that the weight of the error pattern is less or equal \( \rho \). With trellis based supercode decoding the list decoding is performed in the trellis of the supercodes and each list is represented by a marked trellis. Hence, the first decoding step is called the marking algorithm.

a) The marking algorithm: The marking algorithm is applied to the two supercode trellises.

Step 1: Set \( \Lambda_0^F(\sigma_0) = \Lambda_0^L(\sigma_0) = 0 \) and \( M_0(\sigma_0) = M_1(\sigma_0) = 0 \).

Step 2: Calculate the forward metric for each node \( \sigma_t \), \( t = 1, \ldots, n \) when \( N_0^P(\sigma_t) \neq 0, b = 0, 1; \)

\[\Lambda_0^F(\sigma_t) = \Lambda_0^L(N_0^P(\sigma_t)) + \lambda(\omega_{t-1})\]

with

\[
\Lambda_0^F(\sigma) = \begin{cases} 
\min(\Lambda_0^F(\sigma), \Lambda_0^L(\sigma)), & \text{if } N_0^P(\sigma) \neq 0 \land N_0^S(\sigma) \neq 0 \\
\Lambda_0^L(\sigma), & \text{if } N_0^P(\sigma) \neq 0 \land N_0^S(\sigma) = 0 \\
\Lambda_0^L(\sigma), & \text{if } N_0^P(\sigma) = 0 \land N_0^S(\sigma) = 0
\end{cases}
\]

Reset all markings: \( M_0(\sigma_t) = 0 \)

Step 2: If \( \Lambda_0^F(\sigma_n) \leq \rho \), stop decoding.

Step 3: Set \( \Lambda_0^B(\sigma_0) = \Lambda_0^B(\sigma_n) = 0 \).

Step 4: Calculate the backward metric for each node \( \sigma_t \), \( t = n-1, \ldots, 0 \) when \( N_0^P(\sigma_t) \neq 0, b = 0, 1; \)

\[\Lambda_0^B(\sigma_t) = \Lambda_0^B(N_0^S(\sigma_t)) + \lambda(\omega_{t-1})\]

with

\[
\Lambda_0^B(\sigma) = \begin{cases} 
\min(\Lambda_0^B(\sigma), \Lambda_0^L(\sigma)), & \text{if } N_0^P(\sigma) \neq 0 \land N_0^S(\sigma) \neq 0 \\
\Lambda_0^L(\sigma), & \text{if } N_0^P(\sigma) \neq 0 \land N_0^S(\sigma) = 0 \\
\Lambda_0^L(\sigma), & \text{if } N_0^P(\sigma) = 0 \land N_0^S(\sigma) = 0
\end{cases}
\]
Set markings for $b = 0, 1$:

\[ M_b(\sigma) = M(N_b^S(\sigma)) \wedge ((\Lambda^F(\sigma) + \Lambda^b(\sigma)) \leq \rho) \]

with \( M(\sigma) = M_0(\sigma) \vee M_1(\sigma) \).

Considering that each node of both supercode trellises has to be visited twice the runtime complexity of the marking algorithm is given by the size of the supercode trellises.

The second step of supercode decoding is the calculation of the intersection \( L = \cap_i L_i \). Again, the intersection \( L = \cap_i L_i \) is represented by a trellis. The intersection is calculated with the merging algorithm.

### b) The merging algorithm (Breath first Viterbi):

Before we introduce the merging algorithm we have to define a queue. This queue is needed for the breath first search implementation. A queue is a list of \( m \) nodes \( Q = \{ \sigma_1, \sigma_{i+1}, \ldots, \sigma_{i+m-1} \} \) which can shrink and grow dynamically. The queue has two operations. One to add a node at the end \( Q = enqueue(Q, \sigma) = \{ \sigma_1, \ldots, \sigma_{i+m-1}, \sigma \} \) and a second to remove the first node \( \sigma, Q = dequeue(Q) = \sigma_i, \{ \sigma_{i+1}, \ldots, \sigma_{i+m-1}, \sigma_{i+m} \} \).

**Step 1:** Set \( \Lambda^F(\sigma_0) = \Lambda^f(\sigma_0) = 0 \) and \( Q = enqueue(Q, \sigma_0) \).

**Step 2:** Breath first search

\[ \text{while}(\sigma = dequeue(Q)) \]

\[ \{ \]

\[ i f(L(\sigma) > 0) \]

\[ \{ \]

\[ \Lambda^F(\sigma) = \Lambda^F(N^F(\sigma)) + \lambda(\omega_{L(\sigma)-1}) \]

\[ \Lambda^f(\sigma) = \Lambda^f(N^f(\sigma)) + \lambda(\omega_{L(\sigma)-1}) \]

\[ \} \]

\[ M_0(\sigma) = M_0(N^{(1)}(\sigma)) \wedge M_0(N^{(2)}(\sigma)) \]

\[ i f(\sigma = M_0(\sigma) \wedge \neg V(N^S_0(\sigma)) \}

\[ V(N^S_0(\sigma)) = 1 \]

\[ Q = enqueue(Q, N^S_0(\sigma)) \}

\[ \} \]

\[ M_1(\sigma) = M_1(N^{(1)}(\sigma)) \wedge M_1(N^{(2)}(\sigma)) \]

\[ i f(M_1(\sigma) \wedge \neg V(N^S_1(\sigma)) \}

\[ V(N^S_1(\sigma)) = 1 \]

\[ Q = enqueue(Q, N^S_1(\sigma)) \}

\[ \} \]

**Step 3:** Find best path from \( \sigma_{n-1} \) to \( \sigma_0 \) considering only the marked nodes.

**Step 4:** Reset markings and visited flags. (Second breath first search run, with inverted visited flag)

This algorithm avoids iterating over the supercode trellis nodes. In order to reduce the runtime complexity we introduce a pairing of supercode trellis nodes which can be done once before the actual decoding. The simplest way to do this is to create the trellis of the code \( C \). To achieve that a node of the trellis is implicitly marked we add two references to the corresponding nodes in the supercode trellises. As a result, a node in the trellis is marked if both corresponding nodes in the supercode trellises are marked. To calculate the metrics of the marked nodes we cannot iterate over all trellis nodes to check if a node is marked. This would mean that the merging algorithm has the same runtime complexity as Viterbi decoding. Instead of iterating over all nodes we use a breath first search [7] to visit only the marked nodes. The breath first search was chosen because it traverses the trellis level by level. Consequently, the metrics can be calculated as in the marking algorithm.

### V. Simulation results

In this chapter we present some simulation results for binary Reed-Muller code. We compare the trellis based supercode decoder with the Viterbi and BCJR algorithms.

The simulation results for APP decoding are presented in Fig. 1. The left diagram shows the bit error rates for the \( R.M(3,6) \) code (with code length \( n = 64 \) and dimension \( k = 42 \)). With \( \rho = 5 \) the APP decoding based on supercode decoding achieves almost BCJR-performance. With \( \rho = 4 \) the decoding performance is close to that of the Max-Log-MAP algorithm. In the right diagram we present the quality of the soft output values as the error compared to the bit error rate \( P_b \). We estimate the bit error rate from the soft output values as

\[ \tilde{P}_b = \frac{1}{K} \sum_{k=1}^{K} \frac{1}{1 + e^{L_5}} \]

where \( L \) is a soft output value [8], [9]. The right diagram in Fig. 1 presents the relative error

\[ \frac{|\tilde{P}_b - P_b|}{P_b} \]

It can be seen that with \( \rho = 5 \) the quality of the soft output is comparable to the Max-Log-MAP algorithm.

Table I shows the number of nodes visited by the supercode decoding algorithm for different boundaries. Additionally the number of nodes visited by the Viterbi algorithm is presented. As said before, the complexity of the marking algorithm is independent of the input sequence and the bounded distance. Hence we can divide the complete decoding complexity in a static part, caused by the marking, and a dynamic part, caused by the merging. For \( R.M(2,5) \) (with code length \( n = 32 \) and dimension \( k = 16 \)) and \( \rho = 4 \) the number of visited nodes by the Viterbi and supercode decoding algorithm are almost similar. But for \( R.M(3,6) \) and \( \rho = 4 \) the Viterbi algorithm has to visit eight times more nodes than the supercode decoding algorithm.

### VI. Conclusions

In this work we have presented an efficient sub-optimum symbol-by-symbol soft in sof-out a posteriori probability (APP) decoding algorithm for linear binary block codes. The new method is based on trellis based supercode decoding.
which was introduced in [5]. The new implementation presented in this paper reduces the runtime complexity compared to the approach presented in [5].

The presented simulation results indicate that the proposed APP decoding procedure obtains good estimates of the ideal soft-output values and reduces the decoding complexity significantly compared to decoding in the complete syndrome trellis. It is therefore an attractive alternative to conventional implementations of APP decoding for linear binary block codes.

LDPC codes or turbo codes that are based on binary block codes usually employ high rate Hamming codes [10], [11], [12] that allow conventional low complexity APP decoding. The new algorithm may enable other code constructions that are based on block codes with higher error correcting capabilities.

REFERENCES


Author Index

Abbe, E. .......... 44, 51
Altu˘g, Y. .......... 15
Amir, E. .......... 8
Belfiore, J.-C. ..... 111
Blasco-Serrano, R. . 55
Bossert, M. ........ 6, 63
Boston, N. .......... 83
Bross, S. I. ......... 24
Bustin, R. .......... 20
Conti, D. .......... 83
Cuff, P. ........... 11
Dimakis, A. G. ..... 49
D¨orpinghaus, M. ... 28
Elia, P. .......... 127
Erez, U. ........... 99
Etezadi, F. ......... 95
Feizi, S. .......... 107
Fischer, R. F. H. ... 119
Fleury, B. H. ...... 115
Freudenberger, J. . 131
Gastpar, M. ....... 51
Geiger, B. .......... 32
Goela, N. .......... 51
Grant, A. .......... 67
Huber, M. .......... 87
Jakobsen, M. L. ... 115
Jaldén, J. .......... 127
Kaiser, U. .......... 131
Karzand, M. ....... 59
Khisti, A. .......... 95
Kim, Y.-H. .......... 5
Koch, T. .......... 36
Kontoyiannis, I. .... 48
Kubin, G. .......... 32
Land, I. .......... 67
Lapidoth, A. ....... 36
Levin, G. .......... 123
Ling, C. .......... 111
Li, X. ............. 75
Loyka, S. .......... 123
Lucani, D. E. ...... 107
Macris, N. .......... 79
Mathar, R. .......... 28
Matsumoto, R. ...... 75
Médard, M. ....... 107
Nazer, B. .......... 103
Orlitsky, A. ....... 5
Pedersen, T. ....... 115
Permuter, H. ...... 24
Rooij, S. de ....... 40
Rüngeler, M. ...... 28
Saber Tehrani, A. ... 49
Schenk, A. .......... 119
Shah, D. .......... 6
Shamai, S. .......... 20
Singh, A. .......... 127
Skoglund, M. ...... 55
Soljanin, E. ....... 6
Steinberg, Y. ....... 8
Subramanian, R. ... 71
Telatar, E. .......... 5
Thobaben, R. ...... 55
Trott, M. .......... 95
Tuninetti, D. ...... 12
Urbanke, R. ....... 5
Venkat, K. .......... 43
Viterbo, E. .......... 6
Vuffray, M. ...... 79
Wachtler, A. ........ 63
Wagner, A. B. ....... 15
Wang, G. .......... 67
Weissman, T. ...... 43
Wigger, M. ....... 19
Wornell, G. W. .... 99
Zamir, R. .......... 91
Zeh, A. .......... 63