Polar codes for the m-user MAC and matroids

Polar Codes for the m-User MAC and Matroids

Emmanuel Abbe, Emre Telatar
Information Processing group, EPFL
Lausanne 1015, Switzerland
Email: {emmanuel.abbe,emre.telatar}@epfl.ch

***Abstract*—In this paper, a polar code for the m-user multiple access channel (MAC) with binary inputs is constructed. In particular, Arıkan's polarization technique applied individually to each user will polarize any m-user binary input MAC into a finite collection of extremal MACs. The extremal MACs have a number of desirable properties: (i) the 'uniform sum rate'[1] of the original channel is not lost, (ii) the extremal MACs have rate regions that are not only polymatroids but matroids and thus (iii) their uniform sum rate can be reached by each user transmitting either uncoded or fixed bits; in this sense they are easy to communicate over. Provided that the convergence to the extremal MACs is fast enough, the preceding leads to a low complexity communication scheme that is capable of achieving the uniform sum rate of an arbitrary binary input MAC. We show that this is indeed the case for arbitrary values of m.**

I. Introduction

In [2], Arıkan shows that a single-user binary input channel can be "polarized" by a simple process that coverts n independent uses of this channel into n successive uses of "extremal" channels. These extremal channels are binary input and either almost perfect or very noisy, i.e., having a uniform mutual information either close to 1 or close to 0. Furthermore, the fraction of almost perfect channels is close to the uniform mutual information of the original channel. For a 2-user binary input MAC, by applying Arikan's construction to each user's input separately, [6] shows that a similar phenomenon appears: the n independent uses of the MAC are converted into n successive uses of "extremal" binary inputs MACs. These extremal MACs are of four kinds: (1) each users sees a very noisy channel, (2) one of the user sees a very noisy channel and the other sees an almost perfect channel, (3) both users see an almost perfect channel, (4) a pure contention channel: a channel whose uniform rate region is the triangle with vertices (0,0), (0,1), (1,0). Moreover [6] shows that the uniform sum rate of the original MAC is preserved during the polarization process, and that the polarization to the extremal MACs occurs fast enough. This allows the construction of a polar code to achieve reliable communication at uniform sum rate.

In this paper, we investigate the case where m is arbitrary. In the two user case, the extremal MACs are not just MACs for which each users sees either a perfect or pure noise channel, as there is also the pure contention channel. However, the uniform rate region of the 2-user extremal MACs are all polyhedron with integer valued constraints. We will see in this paper that the approach used for the 2-user case faces a new phenomenon when the number of users reaches 4, and the extremal MACs are no longer in a one to one correspondence with the polyhedron having integer valued constraints. To characterize the extremal MACs, we first show how an unusual relationship between random variables defined in terms of mutual information falls precisely within the independence notion of the matroid theory. This relationship is used to show that the extremal MACs are equivalent to linear deterministic channels, which is then used to conclude the construction of a polar code ensuring reliable communication for arbitrary values of m. Finally, the problem of considering m arbitrary large is of interest for a polarization of the additive white Gaussian noise channel.

[1] In this paper all mutual informations are computed when the inputs of a MAC are distributed independently and uniformly. The resulting rate regions, sum rates, etc., are prefixed by 'uniform' to distinguish them from the capacity region, sum capacity, etc.

II. The Polarization Construction

We consider a m-user multiple access channel with binary input alphabets (BMAC) and arbitrary output alphabet $\mathcal{Y}$. The channel is specified by the conditional probabilities

$$P(y|\bar{x}), \quad \text{for all } y \in \mathcal{Y} \text{ and } \bar{x} = (x[1], \dots, x[m]) \in \mathbb{F}_2^m.$$

Let $E_m := \{1, \dots, m\}$ and let $X[1], \dots, X[m]$ be mutually independent and uniformly distributed binary random variables. Let $\bar{X} := (X[1], \dots, X[m])$. We denote by Y the output of $\bar{X}$ through the MAC P. For $J \subseteq E_m$, we define

$$X[J] := \{X[i] : i \in J\},$$
$$I[J](P) := I(X[J]; YX[J^c]),$$

where J^c denotes the complement set of J in E_m. Note that

$$\mathcal{I}(P) := \{(R_1, \dots, R_m) : 0 \le \sum_{i \in J} R_i \le I[J](P), \forall J \subseteq E_m\}$$

is an inner bound to the capacity region of the MAC P. We refer to $\mathcal{I}(P)$ as the uniform rate region and to $I[E_m](P)$ as the uniform sum rate. We now consider two independent uses of such a MAC. We define $\bar{X}_1 := (X_1[1], \dots, X_1[m])$, $\bar{X}_2 := (X_2[1], \dots, X_2[m])$, where $X_1[i], X_2[i]$, with $i \in E_m$, are mutually independent and uniformly distributed binary random variables. We denote by Y_1 and Y_2 the respective outputs of $\bar{X}_1$ and $\bar{X}_2$ through two independent uses of the MAC P:

$$\bar{X}_1 \xrightarrow{P} Y_1, \quad \bar{X}_2 \xrightarrow{P} Y_2. \tag{1}$$

We define two additional binary random vectors $\bar{U}_1 := (U_1[1], \dots, U_1[m])$, $\bar{U}_2 := (U_2[1], \dots, U_2[m])$ with mutually

independent and uniformly distributed components, and we put $\bar{X}_1$ and $\bar{X}_2$ in one to one correspondence with $\bar{U}_1$ and $\bar{U}_2$ with $\bar{X}_1 = \bar{U}_1 + \bar{U}_2$ and $\bar{X}_2 = \bar{U}_2$, where the addition is the modulo 2 component wise addition.

Definition 1. Let $P : \mathbb{F}^m \to \mathcal{Y}$ be a m-user BMAC. We define two new m-user BMACs, $P^- : \mathbb{F}_2^m \to \mathcal{Y}^2$ and $P^+ : \mathbb{F}_2^m \to \mathcal{Y}^2 \times \mathbb{F}_2^m$, by $P^-(y_1, y_2|\bar{u}_1) := \sum_{\bar{u}_2 \in \mathbb{F}_2^m} \frac{1}{2^m} P(y_1|\bar{u}_1 + \bar{u}_2) P(y_2|\bar{u}_2)$ and $P^+(y_1, y_2, \bar{u}_1|\bar{u}_2) := \frac{1}{2^m} P(y_1|\bar{u}_1 + \bar{u}_2) P(y_2|\bar{u}_2)$ for all $\bar{u}_i \in \mathbb{F}_2^m$, $y_i \in \mathcal{Y}$, $i = 1, 2$.

That is, we have now two new m-user BMACs with extended output alphabets:

$$\bar{U}_1 \overset{P^-}{\to} (Y_1, Y_2), \quad \bar{U}_2 \overset{P^+}{\to} (Y_1, Y_2, \bar{U}_1) \tag{2}$$

which also defines $I[J](P^-)$ and $I[J](P^+)$, $\forall J \subseteq E_m$.

This construction is the natural extension of the construction for $m = 1, 2$ in [2], [6]. Here again, we are comparing two independent uses of the same channel P (cf. (1)) with two successive uses of the channels P^- and P^+ (cf. (2)). Note that $I[J](P^-) \le I[J](P) \le I[J](P^+)$, $\forall J \subseteq E_m$.

Definition 2. Let $\{B_n\}_{n \ge 1}$ be i.i.d. uniform random variables valued in $\{-, +\}$. Let the random processes $\{P_n,\ n \ge 0\}$ and $\{I_n[J],\ n \ge 0\}$, for $J \subseteq E_m$, be defined by $P_0 := P$,

$$P_{n+1} := P_n^{B_{n+1}}, \quad I_n[J] := I[J](P_n), \quad \forall n \ge 0.$$

III. Results

Summary: In Section III-A, we show that $\{I_n[J], J \subseteq E_m\}$ tends a.s. to sequence of number which defines a matroid (cf. Definition 5). We then see in Section III-B that the extreme points of a uniform rate region with matroid constraints can be achieved by each user sending uncoded or frozen bits; in particular the uniform sum rate can be achieved by such strategies. We then show in Section III-D, that for arbitrary m, $\{I_n[J], J \subseteq E_m\}$ does not tend to an arbitrary matroid but to a binary matroid (cf. Definition 6). This is used to show that the convergence to the extremal MACs happens fast enough, and that the construction of previous section leads to a polar code having a low encoding and decoding complexity and achieving the uniform sum rate on any binary MAC.

A. The extremal MACs

Lemma 1. *$\{I_n[J], n \ge 0\}$ is a bounded super-martingale when $J \subsetneq E_m$ and a bounded martingale when $J = E_m$.*

Proof: For any $J \subseteq E_m$, $I_n[J] \le m$ and

$$\begin{aligned}
2I[J](P) &= I(X_1[J]X_2[J]; Y_1Y_2X_1[J^c]X_2[J^c]) \\
&= I(U_1[J]U_2[J]; Y_1Y_2U_1[J^c]U_2[J^c]) \\
&= I(U_1[J]; Y_1Y_2U_1[J^c]U_2[J^c]) \\
&\quad + I(U_2[J]; Y_1Y_2U_1[J^c]U_2[J^c]U_1[J]) \\
&\ge I(U_1[J]; Y_1Y_2U_1[J^c]) \\
&\quad + I(U_2[J]; Y_1Y_2\bar{U}_1U_2[J^c]) \\
&= I[J](P^-) + I[J](P^+),
\end{aligned} \tag{3}$$

where equality holds above, if $J^c = \emptyset$, i.e., if $J = E_m$. ∎

Note that the inequality in the above are only due to the bounds on the mutual informations of the P^- channel. Because of the equality when $J = E_m$, our construction preserves the uniform sum rate. As a corollary of previous Lemma, we have the following result.

Theorem 1. *The process $\{I_n[J], J \subseteq E_m\}$ converges a.s..*

Note that for a fixed n, $\{I_n[J], J \subseteq E_m\}$ denotes the collection of the 2^m random variables $I_n[J]$, for $J \subseteq E_m$. When the convergence takes place (a.s.), let us define $I_\infty[J] := \lim_{n\to\infty} I_n[J]$. From previous theorem, $I_\infty[J]$ is a random variable valued in $[0, |J|]$. We will now further characterize these random variables.

Lemma 2. *For any $\varepsilon > 0$ and any m-user BMAC P, there exists $\delta > 0$, such that for any $J \subseteq E_m$, if $I[J](P^+) - I[J](P) < \delta$, we have $I[J](P) - I[J \setminus i] \in [0, \varepsilon) \cup (1 - \varepsilon, 1]$, $\forall i \in J$, where $I[\emptyset] = 0$.*

Lemma 3. *With probability one, $I_\infty[i] \in \{0, 1\}$ and $I_\infty[J] - I_\infty[J \setminus i] \in \{0, 1\}$, for every $i \in E_m$ and $J \subseteq E_m$.*

Note that Lemma 3 implies in particular that $\{I_\infty[J], J \subseteq E_m\}$ is a.s. a discrete random vector.

Definition 3. We denote by $\mathcal{A}_m$ the support of $\{I_\infty[J], J \subseteq E_m\}$ (when the convergence takes place, i.e., a.s.). This is a subset of $\{0, \dots, m\}^{2^m}$.

We have already seen that not every element in $\{0, \dots, m\}^{2^m}$ can belong to $\mathcal{A}_m$. We will now further characterize the set $\mathcal{A}_m$.

Definition 4. A polymatroid is a set E_m, called the ground set, equipped with a function $f : 2^m \to \mathbb{R}$, called a rank function, which satisfies

$$\begin{aligned}
&f(\emptyset) = 0 \\
&f[J] \le f[K], \quad \forall J \subseteq K \subseteq E_m, \\
&f[J \cup K] + f[J \cap K] \le f[J] + f[K], \quad \forall J, K \subseteq E_m.
\end{aligned}$$

Theorem 2. *For any MAC and any distribution of the inputs $X[E]$, we have that $\rho(S) = I(X[S]; YX[S^c])$ is a rank function on E, where we denote by Y the output of the MAC with input $X[E]$. Hence, (E, ρ) is a polymatroid.*

(A proof of this result can be found in [7].) Therefore, any realization of $\{I_n[J], J \subseteq E_m\}$ defines a rank function and the elements of $\mathcal{A}_m$ define polymatroids.

Definition 5. A matroid is a polymatroid whose rank function is integer valued and satisfies $f(J) \le |J|$, $\forall J \subseteq E_m$. We denote by MAT_m the set of all matroids with ground state E_m. We also define a basis of a matroid by the collection of maximal subsets of E_m for which $f(J) = |J|$. One can show that a matroid is equivalently defined from its bases.

Using Lemma 3 and the definition of a matroid, we have the following result.

Theorem 3. *For every $m \ge 1$, $\mathcal{A}_m \subseteq \mathrm{MAT}_m$.*

We will see that the inclusion is strict for $m \geq 4$.

B. Communicating On Matroids

We have shown that, when n tends to infinity, the MACs that we create with the polarization construction of Section II are particular MACs: the mutual informations $I_\infty[J]$ are integer valued (and satisfy the other matroid properties). A well-known result of matroid theory (cf. Theorem 22 of [4]) says that the vertices of a polymatroid given by a rank function f are the vectors of the following form:

$$\begin{aligned} x_{j(1)} &= f(A_1), \\ x_{j(i)} &= f(A_i) - f(A_{i-1}), \quad \forall 2 \leq i \leq k \\ x_{j(i)} &= 0, \quad \forall k < i \leq m, \end{aligned}$$

for some $k \leq m$, $j(1), j(2), \ldots, j(m)$ distinct in E_m and $A_i = \{j(1), j(2), \ldots, j(i)\}$. He hence have the following.

Corollary 1. *The uniform rate regions of the MACs defined by $\mathcal{A}_m$ have vertices on the hypercube $\{0,1\}^m$. In particular, when operating at a vertex each user sees either a perfect or pure noise channel.*

C. Convergence Speed and Representation of Matroids

Convention: for a given m, we write the collection $\{I_\infty[J], J \subseteq E_m\}$ by skipping the empty set (since $I_\infty[\emptyset] = 0$) and as follows: when $m = 2$, we order the sequence as $(I_\infty[1], I_\infty[2], I_\infty[1,2])$, and when $m = 3$, as $(I_\infty[1], I_\infty[2], I_\infty[3], I_\infty[1,2], I_\infty[1,3], I_\infty[2,3], I_\infty[1,2,3])$, etc.

When $m = 2$, [6] shows that $\{I_\infty[J], J \subseteq E_m\}$ belongs a.s. to $\{(0,0,0), (0,1,1), (1,0,1), (1,1,1), (1,1,2)\}$. These are precisely all the matroids with two elements. The speed of convergence to these matroids is shown to be fast in [6] through the following steps. The main idea is to deduce the convergence speed of $I_n[J]$ from the convergence speed obtained in the single user setting, which we know is fast enough, namely as $o(2^{-n^\beta})$, for any $\beta < 1/2$, cf. [3]. We do not need to check the speed convergence for $(0,0,0)$. For $(1,0,1)$, the speed convergence can be deduced from the $m = 1$ speed convergence result as follows. First note that $I(X[1];Y) \leq I[1](P) = I(X[1];YX[2])$. Then, it is shown that, if $I[1](P_n)$ tends to 1, it must be that along those paths of the B_n process, $\hat{I}[1](P_n)$ tends to 1 as well, where $\hat{I}[i](P) = I(X[i];Y)$. Now, since $\hat{I}[1](P_n)$ tends to 1, it must tend fast from the single user result. A similar treatment can be done for $(0,1,1)$ and $(1,1,2)$. However, for $(1,1,1)$, another step is required. Indeed, for this case, $\hat{I}[1](P_n)$ and $\hat{I}[2](P_n)$ tend to zero. Hence, $\hat{I}[1,2](P) = I(X[1]+X[2];Y)$ is introduced and it is shown that $\hat{I}[1,2](P_n)$ tends to 1. Moreover, if we denote by Q the single user channel between $X[1] + X[2]$ and Y, we have that $\hat{I}[1,2](P) = I(Q)$, $\hat{I}[1,2](P^-) = I(Q^-)$ and $\hat{I}[1,2](P^+) = I(U_2[1] + U_2[2]; Y_1Y_2U_1[1]U_1[2]) \geq I(U_2[1] + U_2[2]; Y_1Y_2U_1[1] + U_1[2]) = I(Q^+)$. Hence, using the single user channel result, $\hat{I}[1,2](P_n)$ tends to 1 fast. Note that a property of the matroids $\{(0,0,0), (0,1,1), (1,0,1), (1,1,1), (1,1,2)\}$ is that we can express any of them as the uniform rate region of a deterministic linear channel: $(1,0,1)$ is in particular the uniform rate region of the MAC whose output is $Y = X[1]$, $(0,1,1)$ corresponds to $Y = X[2]$, $(1,1,1)$ to $Y = X[1] + X[2]$ and $(1,1,2)$ to $(Y_1, Y_2) = (X[1], X[2])$.

Now, when $m = 3$, all matroids are also in a one to one correspondence with linear forms and a similar treatment to the $m = 2$ case is possible. This is related to the fact that any matroid on 2 or 3 elements can be represented in the binary field. We now introduce the definition of binary matroids.

Definition 6. *Linear matroids:* let A be a $k \times m$ matrix over a field. Let E_m be the index set of the columns in A. The rank of $J \subseteq E_m$ is defined by the rank of the sub-matrix with columns indexed by J.
Binary matroids: A matroid is binary if it is a linear matroid over the binary field. We denote by BMAT_m the set of binary matroids with m elements.

1) The $m = 4$ Case: We have that MAT_4 contains 17 unlabeled matroids (68 labeled ones). However, there are only 16 unlabeled binary matroids with ground state 4. Hence, there must be a matroid which does not have a binary representation. This matroid is given by $(1,1,1,1,2,2,2,2,2,2,2,2,2,2,2)$ (one can easily check that this is not a binary matroid). It is denoted $U_{2,4}$ and is the uniform matroid of rank 2 with 4 elements (for which any 2 elements set is a basis). Luckily, one can show that there is no MAC leading to $U_{2,4}$ and the following holds.

Lemma 4. $\mathcal{A}_4 \subset \mathrm{BMAT}_4 \subsetneq \mathrm{MAT}_4$.

Hence, the $m = 4$ case can be treated in a similar manner as the previous cases. We conclude this section by proving the following result, which implies Lemma 4.

Lemma 5. *$U_{2,4}$ cannot be the uniform rate region of any MAC with four users and binary uniform inputs.*

Proof: Assume that $U_{2,4}$ is the uniform rate region of a MAC. We then have

$$I(X[i,j];Y) = 0, \tag{4}$$
$$I(X[i,j];YX[k,l]) = 2, \tag{5}$$

for all i,j,k,l distinct in $\{1,2,3,4\}$. Let y_0 be in the support of Y. For $x \in \mathbb{F}_2^4$, define $\mathbb{P}(x|y_0) = W(y_0|x)/\sum_{z\in\mathbb{F}_2^4} W(y_0|z)$. Then from (5), $\mathbb{P}(0,0,*,*|y_0) = 0$ for any choice of $*,*$ which is not $0,0$ and $\mathbb{P}(0,1,*,*|y_0) = 0$ for any choice of $*,*$ which is not $1,1$. On the other hand, from (4), $\mathbb{P}(0,1,1,1|y_0)$ must be equal to p_0. However, we have form (5) that $\mathbb{P}(1,0,*,*|y_0) = 0$ for any choice of $*,*$ (even for $1,1$ since we now have $\mathbb{P}(0,1,1,1|y_0) > 0$). At the same time, this implies that the average of $\mathbb{P}(1,0,*,*|y_0)$ over $*,*$ is zero. This brings a contradiction, since from (4), this average must equal to p_0. ∎

Moreover, a similar argument can be used to prove a stronger version of Lemma 5 to show that no sequence of MACs can have a uniform rate region that converges to $U_{2,4}$.

2) Arbitrary values of m: We have seen in previous section that for $m = 2, 3, 4$, the extremal MACs are not any matroids but binary matroids. This allows us to conclude that $\{I_n[J], J \subseteq E_m\}$ must tend fast enough to $\{I_\infty[J], J \subseteq E_m\}$. Indeed, by working with the linear deterministic representation of the MACs, the problem of showing that the convergence speed is fast in the MAC setting is a consequence of the single-user setting result shown in [2]. We now show that this approach can be used for any values of m.

Definition 7. A matroid is BUMAC if its rank function r can be expressed as $r(J) = I(X[J]; YX[J^c])$, $J \subseteq E_m$, where $X[E]$ has independent and binary uniformly distributed components, and Y is the output of a binary input MAC.

Theorem 4. *A matroid is BUMAC if and only if it is binary.*

The converse of this theorem is easily proved and the direct part uses the following steps, which are detailed in [1]. First the following theorem on the representation of binary matroids due to Tutte, whose proof can be found in [5].

Theorem 5 (Tutte)**.** *A matroid is binary if and only if it has no minor that is $U_{2,4}$.*

A minor of matroid is a matroid which is either a restriction or a contraction of the original matroid to a subset of the ground set. A contraction can be defined as a restriction on the dual matroid, which is another matroid whose bases are the complement set of the bases of the original matroid. Using Lemma 4, we already know that $U_{2,4}$ is not a restriction of any BUMAC matroid. To show that a BUMAC matroid cannot have $U_{2,4}$ as a contraction, Lemma 4 can be used in a dual manner, since one can show that the rank function of the dual of a BUMAC matroid is given by $r^*(J) = |J| - I(X[J]; Y)$.

Theorem 6. *Let $X[E]$ have independent and binary uniformly distributed components. Let Y be the output of a MAC with input $X[E]$ and for which $f(J) = I(X[J]; YX[J^c])$ is integer valued, for any $J \subseteq E_m$. We know from previous theorem that $f(\cdot)$ is also the rank function of a binary matroid, so let A be a matrix representation of this binary matroid. We then have*

$$I(AX[E]; Y) = \text{rank}A = f(E_m).$$

The proof of previous theorem, with further investigations on this subject can be found in [1]. Moreover, one can show a stronger version of these theorems for MACs having a uniform rate region which tends to a matroid. Now, this result tells us that the extremal MACs are equivalent to linear deterministic channels. This suggests that we could have started from the beginning by working with $S[J](P) := I(\sum_{i \in J} X_i; Y)$ instead of $I[J](P) = I(X[J]; YX[J^c])$ to analyze the polarization of a MAC. The second measure is the natural one to study a MAC, since it characterizes the rate region. However, we have just shown that it is sufficient to work with the first measure for the purpose of the polarization problem considered here. Indeed, one can show that $S[J](P_n)$ tends either to 0 or 1 and Eren Şaşoğlu has provided a direct argument showing that these measures are fully characterizing the extremal MACs. Moreover, the process of identifying which matroids can have a rank function derived from an information theoretic measure, such as the entropy, has been investigated in different works, cf. [8] and references therein. In the next section, we summarize our polar code construction for the MAC.

D. Polar code construction for MACs

Let $n = 2^l$ for some $l \in \mathbb{Z}_+$ and let $G_n = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{\otimes l}$ denote the lth Kronecker power of the given matrix. Let $U[k]^n := (U_1[k], \ldots, U_n[k])$ and

$$X[k]^n = U[k]^n G_n, \quad k \in E_m.$$

When $X[E_m]^n$ is transmitted over n independent uses of P to receive Y^n, define the channel $P_{(i)} : \mathbb{F}_2^m \to \mathcal{Y}^n \times \mathbb{F}_2^{m(i-1)}$ to be the channel whose inputs and outputs are $U_i[E_m] \to Y^n U^{i-1}[E_m]$. Let $\varepsilon > 0$ and let $A[k] \subset \{1, \ldots, n\}$ denote the sets of indices where information bits are transmitted by user k, which are chosen as follows: for a fixed $i \in \{1, \ldots, n\}$, if $\|\{I[J](P_{(i)}) : J \subseteq E_m\} - \mathbb{B}\| < \varepsilon$ for some binary matroid $\mathbb{B}$ (where the distance above refers to the euclidean distance between the corresponding 2^m dimensional vectors), then pick a basis of $\mathbb{B}$ and include i in $A[k]$ if k belongs to that basis. If no such binary matroid exists, do not include i in $A[k]$ for all $k \in E_m$. Choose the bits indexed by $A[k]^c$, for all k, independently and uniformly at at random, and reveal their values to the transmitter and receiver.

For an output sequence Y^n, the receiver can then decode successively $U_1[E_m]$, then $U_2[E_m]$, etc., till $U_n[E_m]$. Moreover, since $I[E_m](P)$ is preserved through the polarization process (cf. the equality in (3)), we guarantee that for every $\delta > 0$, there exists a n_0 such that $\sum_{k=1}^m |A[k]| > n(I[E_m](P) - \delta)$, for $n \geq n_0$. Using the results of previous section, we can then show the following theorem, which ensures that the code described above allows reliable communication at sum rate.

Theorem 7. *For any $\beta < 1/2$, the block error probability of the code described above, under successive cancellation decoding, is $o(2^{-n^\beta})$.*

Moreover, this codes has an encoding and decoding complexity of $O(n \log n)$, from [2].

REFERENCES

[1] E. Abbe, *Information, Matroid and Extremal Channels.* Preprint.

[2] E. Arıkan, *Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels,* IEEE Trans. Inform. Theory, vol. IT-55, pp. 3051–3073, July 2009.

[3] E. Arıkan and E. Telatar, *On the rate of channel polarization,* in Proc. 2009 IEEE Int. Symp. Inform. Theory, Seoul, pp. 1493–1495, 2009.

[4] J. Edmonds, *Submodular functions, matroids and certain polyhedra,* Lecture Notes in Computer Science, Springer, 2003.

[5] J. Oxley, *Matroid Theory,* Oxford Science Publications, New York, 1992.

[6] E. Şaşoğlu, E. Telatar, E. Yeh, *Quasi-polarization for the two user binary input multiple access channel*. Preprint.

[7] D. Tse and S. Hanly, *Multi-access Fading Channels: Part I: Polymatroid Structure, Optimal Resource Allocation and Throughput Capacities,* IEEE Trans. Inform. Theory, vol. IT-44, no. 7, pp. 2796-2815, November 1998.

[8] Z. Zhang and R. Yeung, *On characterization of entropy function via information inequalities,* IEEE Trans. on Information Theory, vol. 44, no. 4, pp. 1140-1452, 1998.