Conference Paper

Sierpinski Prefactors in the Guruswami–Sudan Interpolation Step

Author(s):
Senger, Christian

Publication Date:
2014

Permanent Link:
https://doi.org/10.3929/ethz-a-010094876

Rights / License:
In Copyright - Non-Commercial Use Permitted
Sierpinski Prefactors in the Guruswami–Sudan Interpolation Step

Christian Senger
ECE, University of Toronto
Toronto, Ontario, Canada
Email: csenger@comm.utoronto.ca

Abstract—Sierpinski prefactors are introduced, a concept that exploits the fact that many binomial coefficients in the Hasse derivative that appears in the Guruswami–Sudan interpolation step are zero modulo the base field characteristic. A reduced Guruswami–Sudan interpolation step for generalized Reed–Solomon codes with significantly fewer unknowns than the original interpolation step is formulated.

I. INTRODUCTION

The re-encoding projection [1], [2] is a well-known method to reduce the complexity of the Guruswami–Sudan interpolation step for decoding generalized Reed–Solomon codes. It basically consists of one additional erasures-only decoding step. We show in this paper that similar predictions about beneficial properties, which allows useful predictions about the solution space of the interpolation step to be made. The computational overhead of the projection is negligible, as it basically consists of one additional erasures-only decoding step. We show in this paper that similar predictions about the solution space of the interpolation step can be made by exploiting an inherent property of finite fields, namely, that all multiples of the field characteristic are zero.

II. PRELIMINARIES

Definition 1. For a prime power q and n, k ∈ N \ {0} with k ≤ n ≤ q let A = {α0, . . . , αn−1} be an ordered set of distinct elements from the finite field Fq with q elements and let B = {β0, . . . , βn−1} be an ordered set of nonzero (not necessarily distinct) elements from Fq. Then the set of vectors

GRS,A,B(Fq; n, k) ≜ {(β0u(α0), . . . , βn−1u(αn−1)) : u(x) ∈ Fq[x], deg[u(x)] < k}

constitutes a generalized Reed–Solomon (GRS) code over Fq.

When possible, we write GRS for GRS,A,B(Fq; n, k). Conventional Reed–Solomon (RS) codes are special cases of GRS codes with A = {1, α, . . . , αn−1} and

B = {1, αb, . . . , αb(n−1)},

where α ∈ Fq is primitive and b ∈ N.

The Guruswami–Sudan algorithm (GSA) [3] for decoding GRS codes can be divided into two steps: the interpolation step (Problem 1) and the factorization step (which is not the focus of this paper). Let e ∈ GRS be a codeword, e ∈ Fqβ be an error vector of Hamming weight wt[v] = ε, and y = e + v be the corresponding received vector obtained from the transmission channel. Furthermore, let I ≜ {0, . . . , n − 1} and let r, ℓ ∈ N \ {0} be two parameters of the GSA with r ≤ ℓ. We associate the polynomial Pℓ(x) ≜ ∏i∈I(x − αi) with I.

Problem 1 (GRS Interpolation Step). Given a received vector y and ε0 ∈ N, find a nonzero bivariate polynomial Q(x, z) = Q0(x) + Q1(x)z + · · · + Qℓ(x)zℓ ∈ Fq[x, z] such that

deg[Qν(x)] ≤ r(n − ε0) − ν(k − 1) − 1 ≜ dν,

for ν = 0, . . . , ℓ and ∀i ∈ I ∀s, t ∈ N : s + t < r and

∑v∈I (ν/t)zν−t × ∑μ∈S xμ−s Qν,µ (x, z) = 0, (1)

where Qν(x) = ∑μ≥0 Qν,µ xµ.

The nested sum in (1) is called the (s, ℓ)th mixed partial Hasse derivative of Q(x, z). The condition that all (s, ℓ)th Hasse derivatives with s + t < r evaluate to zero for all tuples (αi, yj), i ∈ I, means that these tuples are zeros of multiplicity r of Q(x, z). For that reason, we refer to the parameter r as the multiplicity of the GSA. The parameter ℓ is called the list size. The linear system of equations associated with Problem 1 has a nonzero solution Q(x, z) as long as

ε < n(2ℓ − r + 1) − ℓ(k − 1) ≜ ε0.

Naively solving the system with Gaussian elimination in order to obtain a solution is in O(n3), however, accelerated algorithms can be found in the literature, e.g., Kötter interpolation in [4]. Without loss of generality we assume in the following that the columns of the coefficient matrix (from left to right) are associated with the unknown coefficients Q0,0, . . . , Q0,d2,0, Q1,0, . . . , Q1,d2,0, . . . , Qℓ,0, . . . , Qℓ,d2,0.

III. SIERPINSKI PREFACTORS

In this section, we introduce a new technique that results in structured solutions of Problem 1. In contrast to the well-known re-encoding projection [1], [2], this approach does not require any additional computations, it simply exploits basic properties of the GRS code’s base field Fq. The main idea is to exploit the fact that many of the binomial coefficients in (1) are zero modulo the characteristic of Fq.

To see this, let us consider the left-aligned Pascal triangle in Fig. 1, where the entries are calculated modulo 3. Obviously, the zero entries of the triangle follow regular patterns. The triangle resembles variants of the left-aligned Sierpinski gasket, one of the most basic examples of a self-similar set. In the following, we will refer to a Pascal triangle with entries
The following lemma, whose proof is based on Lucas’ Theorem [5], specifies the conditions for the existence of a zero column \( t_0 \) and its location.

**Lemma 1.** Let \( r, \ell \in \mathbb{N} \setminus \{0\}, r \leq \ell \). If \( \ell < p \) or

\[ \exists a \in \{1, \ldots, p-1\}, j \in \mathbb{N} : r \leq ap^j - 1 \leq \ell \]

then a zero column does not exist. Otherwise, find the least significant base-\( p \) digit \( \ell_i \) of \( \ell \) such that \( \ell_i < p - 1 \). Then,

\[ t_0 = \left\lfloor \frac{r}{p^{\ell_i+1}} \right\rfloor p^{\ell_i+1} - 1 \]

is a zero column. In particular, \( t_0 \) is the maximal zero column.

We will now generalize the concept to zero columns with resolvable spoilers. This will reveal additional structure in solutions \( Q(x, z) \) of Problem 1, i.e., to factorizations of additional univariate polynomials \( Q_p(x) \) besides \( Q_{z_0}(x) \).

Assume there exists a zero column \( t_0 \) in \( \mathbb{S}_p \). Further assume there is a column \( t_1, t_1 < t_0 \), in \( \mathbb{S}_p \) such that

\[ \binom{t_0}{t_1} \neq 0 \mod p \]

and

\[ \forall \nu = t_1 + 1, \ldots, t_0 \neq 0 : \binom{\nu}{t_1} \equiv 0 \mod p. \]

We refer to such a column as a zero column with spoiler at \( (t_0) \), an example is shown in Fig. 1.

If \( Q(x, z) \) is a solution of Problem 1 for a received vector \( y \) and consider (1) for column \( t_1 \). \( t_1 < t_0 \), becomes

\[ \forall i \in I \forall s \in \mathbb{N} : s < r - t_0 \]

and

\[ \binom{t_0}{t_1} z_{t_0-t_1} \sum_{\mu=0}^{d_{t_1}} \left( \binom{t_0}{t_1} \right) x^{\mu-s} Q_{t_s, \mu} \bigg|_{(x, z) = (\alpha_i, y_1)} = 0, \]

(2)

since all summands of the outer sum except the first one are annihilated by the zero binomial weights. This means that the 0th to \( r - t_0 - 1 \)th Hasse derivatives of \( Q_{\alpha_i}(x) \) evaluate to zero at all \( \alpha_i, i \in I \). But then, these \( \alpha_i \) are roots of multiplicity \( r - t_0 \) of \( Q_{\alpha_i}(x) \) and thus \( Q_{\alpha_i}(x) \) can be factored as \( Q_{\alpha_i}(x) = V_{\alpha_i}(x)P(x)^{r-t_0} \), where \( \deg[V_{\alpha_i}(x)] \leq d_{\alpha_i} - n(r - t_0) \).

Theorem [5], specifies the conditions for the existence of a zero column \( t_0 \) and its location.

\[ \binom{t_0}{t_1} \neq 0 \mod p \]

and

\[ \forall \nu = t_1 + 1, \ldots, t_0 \neq 0 : \binom{\nu}{t_1} \equiv 0 \mod p. \]

We refer to such a column as a zero column with spoiler at \( (t_0) \), an example is shown in Fig. 1.

If \( Q(x, z) \) is a solution of Problem 1 for a received vector \( y \) then (1) for column \( t_1 \), \( t_1 < t_0 \), becomes

\[ \forall i \in I \forall s \in \mathbb{N} : s < r - t_0 \]

and

\[ \binom{t_0}{t_1} z_{t_0-t_1} \sum_{\mu=0}^{d_{t_1}} \left( \binom{t_0}{t_1} \right) x^{\mu-s} Q_{t_s, \mu} \bigg|_{(x, z) = (\alpha_i, y_1)} = 0, \]

(3)

since all summands except the ones for \( \nu = t_1 \) and \( \nu = t_0 \) are annihilated. But, according to (2), the second sum evaluates to zero at all \( \alpha_i \), \( i \in I \), since \( t_0 \) is by assumption a zero column. We refer to \( \binom{t_0}{t_1} \) as a resolvable spoiler for \( t_1 \) because the sum associated with \( \binom{t_0}{t_1} \) vanishes. As a result, we obtain

\[ \forall i \in I \forall s \in \mathbb{N} : s < r - t_0 \]

and

\[ \sum_{\mu=0}^{d_{t_1}} \left( \binom{t_0}{t_1} \right) x^{\mu-s} Q_{t_s, \mu} \bigg|_{x=\alpha_i} = 0, \]

i.e., the \( \alpha_i, i \in I \), are roots of multiplicity \( r - t_0 \) of \( Q_{t_1}(x) \) and thus it can be factored as \( Q_{t_1}(x) = V_{t_1}(x)P(x)^{r-t_0} \), where \( \deg[V_{t_1}(x)] \leq d_{\alpha_i} - n(r - t_0) \).

It is easy to see that if \( \binom{t_0}{t_1} \) is a spoiler for \( t_2, t_2 < t_1 \), then it is also resolvable. Furthermore, it is easy to see that the concept generalizes to multiple spoilers. This leads to the following recursive definition:
Definition 2. Consider $S_p$ and $r, \ell \in \mathbb{N} \setminus \{0\}$. For $\nu \leq t_0$ let
\[ R_\nu^{(\ell)} \triangleq \left\{ t \in \mathbb{N} : \nu < t \leq t_0, \text{it is a zero column with resolvable spoilers} \right\} \]
and
\[ S_\nu^{(\ell)} \triangleq \left\{ t \in \mathbb{N} : \nu < t \leq t_0, \left( \frac{t}{\nu} \right) \text{ is a spoiler for } \nu \right\}. \]

Then $\nu$ is a zero column with resolvable spoilers if and only if $S_\nu^{(\ell)} \subseteq R_\nu$. The basic case is $R_0^{(\ell)} = \{ t_0 \}$ if $t_0$ exists.

Note that zero columns are special cases of zero columns with resolvable spoilers where $S_\nu^{(\ell)} = \emptyset$. The sets of zero columns with resolvable spoilers are non-increasing with $\nu$, i.e., $R_\nu^{(\ell)} \subseteq R_{\mu}^{(\ell)}$. We stress that $R_\nu^{(\ell)}$ contains all zero columns with resolvable spoilers in $S_p$, i.e., it is the set that we are interested in.

Lemma 2. Let $r, \ell \in \mathbb{N} \setminus \{0\}$, $r \leq \ell$. If according to Lemma 1 a maximal zero column $t_0$ of $S_p$ exists then the set of zero columns with resolvable spoilers of $S_p$ is
\[ R_0^{(\ell)} = \left\{ t \in \mathbb{N} : t < r \text{ and } \sum_{\ell = 0}^{t-1} \left( \left( \frac{\ell}{\nu} \right) \text{ mod } p \right) = 0 \right\}, \]
otherwise it is $R_0^{(\ell)} = \emptyset$.

Example 1. Consider the conventional RS code $GRS_A, B(\mathbb{F}_2; 26, 16)$. The characteristic of the code’s base field is $p = 3$. Lemma 1 yields maximal zero column $t_0 = 3$. Fig. 1 shows that for $r = 7$ we have $S_7^{(13)} = \{ 0 \} = R_0^{(13)}$, i.e., $t_1 = 7$ is a zero column with resolvable spoilers and we can set $R_7^{(13)} = \{ 7, 8 \}$. For $r = 6$ we have $S_6^{(13)} = \{ 7, 8 \} = R_0^{(13)}$ and thus it is a zero column with resolvable spoilers as well. This gives $R_0^{(13)} = \{ 6, 7, 8 \}$. For $r = 5$ we have $S_5^{(13)} = \{ 7, 8 \} \subsetneq R_0^{(13)}$ and thus it is a zero column with resolvable spoilers as well. It turns out that for all $t_0 < t_0$ holds $S_t^{(13)} \subseteq \{ 5, 6, 7, 8 \} = R_0^{(13)}$ and thus the only zero columns with resolvable spoilers in $S_5$ with respect to $r = 13$ are $t_0 = 8$, $t_1 = 7$, $t_2 = 6$, and $t_3 = 5$. It can be readily checked that Lemma 2 confirms this result and delivers $R_0^{(13)} = \{ 5, 6, 7, 8 \}$.

The following map will turn out to be useful in the following, it returns either $\nu$ itself or its greatest spoiler:
\[ g : \begin{cases} N \rightarrow N \nu \rightarrow \max(S_\nu^{(\ell)}) \text{ if } S_\nu^{(\ell)} \neq \emptyset \nu \rightarrow \emptyset \text{ if } S_\nu^{(\ell)} = \emptyset \end{cases} \]

Theorem 1. Let $GRS_A, B(\mathbb{F}_q; n, k)$ be a GRS code and $r, \ell$ such that the GSA can correct at most $s_0$ errors. Let further $c \in GRS, c \in \mathbb{F}_q^n$ with $w_{t_1 \ell} | c | \leq s_0$ and $y = c + e$. When the GSA is applied to $y$ it yields a bivariate result polynomial $Q(x, z) = Q_0(x) + Q_1(x)z + \ldots + Q_\ell(x)z^\ell \in \mathbb{F}_q[x, z]$ whose constituent univariate polynomials $Q(x)$, $\nu \in R_0^{(\ell)}$, can be factored as
\[ Q_\nu(x) = V_\nu(x)P_\nu(x)^{r-g[\nu]} \]
where $deg[V_\nu(x)] \leq d_{Q_\nu} - n(r - g[\nu]) = d_{V_\nu}$.

Proof: Let $\nu \in R_0^{(\ell)}$. Since $\nu$ is a zero column with resolvable spoilers, all $\binom{\ell}{\nu}$ with $\nu < t \leq t_0$ are resolvable, i.e.,
\[ \forall t \in S_\nu^{(\ell)} \forall i \in \mathbb{N} : s < r - t \text{ and } \sum_{\mu=s}^{d_{Q_\nu}} \binom{\mu}{s} x^{\mu-s} Q_{t, \mu} \bigg|_{x=\alpha_i} = 0. \quad (6) \]
Since by definition all terms except the ones weighted by the spoilers vanish, we can write (1) as
\[ \forall i \in \mathbb{N} : s < r - \nu \text{ and } \sum_{\mu=s}^{d_{Q_\nu}} \binom{\mu}{s} x^{\mu-s} Q_{t, \mu} \bigg|_{x=\alpha_i} = 0 \]
In order to let the sum over $t$ vanish in the case $S_\nu^{(\ell)} \neq \emptyset$ (i.e., to exploit (6)), we must guarantee $s < r - \nu$ for all $t \in S_\nu^{(\ell)}$, i.e., $s < r - \max(S_\nu^{(\ell)})$. In case $S_\nu^{(\ell)} = \emptyset$ the sum over $t$ is empty and thus it is sufficient to guarantee $s < r - \nu$. Due to the definition (4) of $g[\nu]$ we have $s < r - g[\nu]$ in both cases and thus
\[ \forall i \in \mathbb{N} \forall s \in \mathbb{N} : s < r - g[\nu] \text{ and } \sum_{\mu=s}^{d_{Q_\nu}} \binom{\mu}{s} x^{\mu-s} Q_{t, \mu} \bigg|_{x=\alpha_i} = 0 \]
and the $\alpha_i, i \in I$, are roots of multiplicity $r - g[\nu]$ of $Q_\nu(x)$ and thus it can be factored as in (5). The bound on the degrees of the $V_\nu(x)$ follows from a comparison of the involved polynomial degrees.

We stress that the Sierpinski prefactors $P_\nu(x)^{r-g[\nu]} \in R_0^{(\ell)}$, are fixed a-priori and do not depend on the received vector $y$. This justifies the term prefactor.

Example 2. From Example 1 we have $R_0^{(13)} = \{ 5, 6, 7, 8 \}$, i.e., Theorem 1 guarantees factorizations of $Q_5(x)$, $Q_6(x)$, $Q_7(x)$, and $Q_8(x)$. They are $Q_5(x) = V_5(x)P_5(x)^2$, $Q_6(x) = V_6(x)P_6(x)^2$, $Q_7(x) = V_7(x)P_7(x)^2$, and $Q_8(x) = V_8(x)P_8(x)^2$, with $d_{V_5} = 72$, $d_{V_6} = 57$, $d_{V_7} = 42$, and $d_{V_8} = 27$, respectively, because $g[5] = 6$, $g[6] = 7$, $g[7] = 8$, $g[8] = 8$, $d_{Q_5} = 124$, $d_{Q_6} = 109$, $d_{Q_7} = 94$, and $d_{Q_8} = 79$.

Theorem 1 states that some of the univariate constituent polynomials of the GSA interpolation step (Problem 1) have certain prefactors. We will now show how this knowledge can be exploited in order to simplify solving the interpolation step. More precisely, we show that the associated linear system of equations in $\sum_{\nu=0}^{s_0} (d_{Q_\nu} + 1)$ unknowns can be reduced to a linear system of smaller size.

As noted before, GSA interpolation (Problem 1) amounts to finding the solution of a linear system of equations. This can be done naively using Gaussian elimination. Several faster methods have been developed, all of which exploit the structure of the involved coefficient matrix. Such methods can be

\footnote{Note that this is the generalization of (3) to multiple spoilers.}
applied to a reduced linear system of equations, which can be obtained using Sierpinski prefactors. The key idea here is to exploit the a-priori known structure of the solutions.

In the following, it will be convenient to have the sets

\[ \mathcal{F} \triangleq \{ \nu : 0 \leq \nu \leq \ell, Q_{\nu}(x) \text{ has prefectors} \} \]
\[ \mathcal{F}^c \triangleq \{ \nu : 0 \leq \nu \leq \ell, \nu \notin \mathcal{F} \}. \]

Let us consider the factorization of a univariate constituent polynomial \( Q_{\nu}(x), \nu \in \mathcal{F} \), into a Sierpinski prefactor \( P_{\nu}(x)^{-g_{\nu}} \) and the corresponding quotient polynomial \( V_{\nu}(x) \).

For simplicity, let us denote the \( P_{\nu}(x)^{-g_{\nu}} \) by \( F_{\nu}(x) = \sum_{i=0}^{\deg(F_{\nu}(x))} F_{\nu,i} x^i \).

This gives \( Q_{\nu}(x) = V_{\nu}(x) F_{\nu}(x) \) for \( \nu \in \mathcal{F} \) with coefficients

\[ Q_{\nu,\mu} = \sum_{i=0}^{\mu} V_{\nu,\mu-i} F_{\nu,i}, \quad \mu = 0, \ldots, d_Q. \tag{7} \]

where we implicitly used that the \( i \)th coefficient of a polynomial with \( i < 0 \) or \( i \) greater than the degree of the polynomial is zero. In order to simplify the following description, let us agree on trivial prefactors \( F_{\nu}(x) = 1 \) for all \( Q_{\nu}(x), \nu \in \mathcal{F}^c \).

In these cases, the quotient polynomials are \( V_{\nu}(x) = Q_{\nu}(x) \). Note that the constant term \( F_{\nu,0} \) of any prefactor is nonzero. This allows us to write

\[ V_{\nu,\mu} = Q_{\nu,\mu} - \sum_{i=1}^{\mu} V_{\nu,\mu-i} F_{\nu,i} \]
\[ = \frac{Q_{\nu,\mu}}{F_{\nu,0}} - \sum_{i=1}^{\mu} F_{\nu,i} V_{\nu,\mu-i}, \quad \mu = 0, \ldots, d_Q. \tag{8} \]

which shows that \( V_{\nu,\mu} \) is a linear combination of the \( V_{\nu,i}, i = 0, \ldots, \mu - 1 \), and \( Q_{\nu,\mu} \).

We can exploit (8) for \( \mu = 0, \ldots, d_Q \) in order to obtain a solvable linear system whose solution comprises the coefficients of \( V_{\nu}(x) \) (preparation) and then exploit (7) for \( \mu = d_Q + 1, \ldots, d_Q \) in order to dispose of the redundant columns of the coefficient matrix (reduction). Both steps — preparation and reduction — are based on applying a simple lemma from linear algebra with certain parameters.

As a result of this process, the original coefficient matrix associated with (1), whose \( \sum_{i=0}^{\ell}(d_{Q_{\nu}} + 1) \) columns are associated with \( Q_{0,0}, \ldots, Q_{0,\ell}, d_{Q_{\nu}}, Q_{1,0}, \ldots, Q_{1,\ell}, d_{Q_{\nu}}, \ldots, Q_{\ell,0}, \ldots, Q_{\ell,\ell} \), is converted into a reduced matrix, whose \( \sum_{i=0}^{\ell-1}(d_{Q_{\nu}} + 1) + \sum_{i=0}^{\ell}(d_{Q_{\nu}} + 1) \) columns are associated with \( V_{0,0}, \ldots, V_{0,\ell}, d_{V_{\nu}}, V_{1,0}, \ldots, V_{1,\ell}, d_{V_{\nu}}, \ldots, V_{\ell,0}, \ldots, V_{\ell,\ell} \).

This allows the following reformulation of a reduced GSA interpolation step:

**Problem 2 (Reduced GSA Interpolation Step).** Given a received vector \( y \) with Sierpinski prefactors \( F_{\nu}(x) = P_{\nu}(x)^{-g_{\nu}}, \nu \in \mathcal{F} \), find a nonzero bivariate polynomial

\[ \tilde{Q}(x, z) = \sum_{\nu \in \mathcal{F}} V_{\nu}(x) y^\nu + \sum_{\nu \in \mathcal{F}^c} Q_{\nu}(x) y^\nu \in \mathbb{F}_q[x, z] \]

such that \( \deg[V_{\nu}(x)] \leq d_V \) and \( \deg[Q_{\nu}(x)] \leq d_Q \) and

\[ \forall i \in \mathcal{I}, \forall s, t \in \mathcal{I} : s + t \leq r \] and

\[ \sum_{\nu \in \mathcal{F}} \left( \sum_{\mu=0}^{d_Q} \left( \sum_{\Delta=0}^{d_Q} \left( \sum_{\nu,\mu} F_{\nu,\mu} \right) x^{\mu+\Delta} s^{\nu} \right) \right) \]

\[ \triangleq \text{LUT}[s,i,\nu,\mu] \]

\[ + \sum_{\nu \in \mathcal{F}} \left( \sum_{\mu=0}^{d_Q} \left( \sum_{\nu,\mu} F_{\nu,\mu} \right) x^{\mu-s} \right) \]

\[ \triangleq \text{LUT}[s,i,\nu,\mu] \]

\[ = 0. \]

The sums with summation index \( \mu \) are independent of the received vector \( y \) and their addends can be pre-calculated and stored in a lookup table \( \text{LUT}[s,i,\nu,\mu] \). A solution \( \tilde{Q}(x, z) \) of Problem 1 can easily be recovered from a solution \( Q(x, z) \) of Problem 2 using the prefactors. \( Q(x, z) \) can then be used as input to the GSA factorization step in order to complete the decoding. A reduced GSA factorization step that can operate directly on \( \tilde{Q}(x, z) \) in order to construct the result list was proposed in [1], [2].

**Example 3.** Sierpinski prefactors work particularly well for the two conventional RS codes \( GR_{512}(F_{255}, 255, 191, 65) \) and \( GR_{512}(F_{255}, 255, 144, 112) \) considered by Köpper and Vardy in [6].

The GSA for \( GR_{512} \) can correct up to \( 25 = 34 \) errors with multiplicity \( r = 16 \) and list size \( \ell = 18 \). This requires solving a linear system in 34694 unknowns. Sierpinski prefactors reduce the system to 31379 unknowns. The GSA with \( r = 4 \) and \( \ell = 5 \) for \( GR_{512} \) can correct up to \( 29 = 59 \) errors. The associated linear system has 2559 unknowns, which can be diminished to 2049 unknowns using Sierpinski prefactors.

We emphasize that Sierpinski prefactors can easily be combined with the re-encoding projection, resulting in a significant reduction of the Guruswami–Sudan interpolation step beyond the reduction enabled by re-encoding alone. More details and the missing proofs are provided in [7].

**Acknowledgment**

The author is grateful to Frank R. Kschischang for his valuable comments on the manuscript. This work has been supported by DFG under grant SE 2279/1-1.

**References**


