A link between Guruswami-Sudan's list-decoding and decoding of interleaved Reed-Solomon codes

Alexander Zeh, Christian Senger

A Link between Guruswami–Sudan's List–Decoding and Decoding of Interleaved Reed–Solomon Codes

Alexander Zeh and Christian Senger
Institute of Telecommunications and Applied Information Theory
Ulm University, Germany
{alexander.zeh,christian.senger}@uni-ulm.de

***Abstract*—The Welch–Berlekamp approach for Reed–Solomon (RS) codes forms a bridge between classical syndrome–based decoding algorithms and interpolation–based list–decoding procedures for list size $\ell = 1$. It returns the univariate error–locator polynomial and the evaluation polynomial of the RS code as a y–root.**

In this paper, we show the connection between the Welch–Berlekamp approach for a specific Interleaved Reed–Solomon code scheme and the Guruswami–Sudan principle. It turns out that the decoding of Interleaved RS codes can be formulated as a modified Guruswami–Sudan problem with a specific multiplicity assignment. We show that our new approach results in the same solution space as the Welch–Berlekamp scheme. Furthermore, we prove some important properties.

***Index Terms*—Guruswami–Sudan (GS) interpolation, Reed–Solomon (RS) codes, Interleaved Reed–Solomon (IRS) codes**

I. Introduction

The Guruswami–Sudan (GS) [6] approach for Reed–Solomon (RS) codes consists of an interpolation and a factorization step of a degree–restricted bivariate polynomial. The usage of multiplicities in the first stage improved the error–correcting capability of Sudan's original work [14]. The set of y–roots of the bivariate interpolation polynomial gives the candidates of the evaluation polynomials of the corresponding RS codes. The GS principle coincides with the Welch-Berlekamp (WB) approach [2] when the list size is $\ell = 1$. Then, $\tau_0 = \lfloor (n-k)/2 \rfloor$ errors can be uniquely corrected, where n is the length and k the dimension of the RS code.

Interleaved Reed–Solomon (IRS) codes are most effective if correlated errors affect all words of the interleaved scheme simultaneously (see [9]). Because of this, IRS codes are mainly considered in applications where error bursts occur. Bleichenbacher *et al.* [3], [4] formulated an IRS decoding procedure with the WB method.

Our contribution covers the reformulation of the Bleichenbacher approach in terms of a modified GS interpolation problem for a heterogeneous IRS scheme as it was investigated in [13]. The heterogeneous IRS code is built by virtual extension of an RS code. The rate restriction and the decoding radius of this scheme are comparable with the parameters of Sudan's original algorithm (where the multiplicity for each point equals one). Also, the corresponding syndrome formulation (for Sudan done in [12], [11]) is equivalent. Hence, it seems to be surprising that this scheme can be formulated as a modified GS interpolation problem, where the multiplicities are assigned in a specific manner.

The paper is organized as follows. First, we shortly describe the GS principle for RS codes in Section III and outline important properties that we will use later. The connection to the WB approach is investigated in Section IV. The virtual extension to an IRS code [13] is described in Section V. Section VI links the GS list–decoding procedure with the WB formulation of the previously described IRS scheme. Furthermore, the equivalence of both approaches is proved and an informal description is given. Finally, Section VII concludes the paper. An example is given in the appendix.

This work has been supported by DFG, Germany, under grants BO 867/17 and BO 867/22-1.

II. Definition and Notation

Here and later, $[n]$ denotes the set of integers $\{1, \ldots, n\}$ and $[n]_0$ denotes the set of integers $\{0, \ldots, n\}$. The entries of an $m \times n$ matrix $\mathbf{S} = \| \ S_{i,j} \ \|$ are denoted $S_{i,j}$, where $i \in [m-1]_0$ and $j \in [n-1]_0$. A univariate polynomial of degree n is noted in the form $A(x) = \sum_{i=0}^{n} A_i x^i$. A vector of length n is denoted by $\mathbf{r} = (r_1, r_2, \ldots, r_n)^T$.

Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be nonzero distinct elements (code locators) of the finite field $\mathbb{F} = GF(q)$ of size q. $\mathcal{L} = \{\alpha_1, \ldots, \alpha_n\}$ is the set containing all code locators. Denote

$$f(\mathcal{L}) = (f(\alpha_i), \ldots, f(\alpha_n))$$

for a given polynomial $f(x)$ over $\mathbb{F}$.

An RS code $\mathcal{RS}(n,k)$ over $\mathbb{F}$ with $n < q$ is given by

$$\mathcal{RS}(n,k) = \{\mathbf{c} = f(\mathcal{L}) : f(x) \in \mathbb{F}_k[x]\}, \tag{1}$$

where $\mathbb{F}_k[x]$ stands for the set of all univariate polynomials with degree less than k and indeterminate x.

RS codes are known to be maximum distance separable (MDS), i.e., their minimum Hamming distance is $d = n-k+1$.

III. The GS principle and the univariate formulation

A. Guruswami–Sudan Approach for Reed–Solomon Codes

Let the n points $\{(\alpha_i, r_i)\}_{i=1}^{n}$,where $\alpha_i, r_i \in \mathbb{F}$ and $\mathbf{r} = (r_1, \ldots, r_n)$ denotes the received word, be interpolated by a bivariate polynomial $Q(x,y)$. The number of errors, that can be corrected, is denoted by τ. The parameter s is the order of

multiplicity of the bivariate interpolation polynomial in the GS algorithm. The list size is denoted by ℓ. The nonzero interpolation polynomial $Q(x,y)$ has to satisfy the following degree conditions:

$$DC_1 := \begin{bmatrix} \deg_{0,1} Q(x,y) & \leq & \ell, \\ \deg_{1,k-1} Q(x,y) & < & s(n-\tau) \end{bmatrix}, \quad (2)$$

where $\deg_{u,v} a(x,y) = ud_x + vd_y$ is the (u,v)–weighted degree of a bivariate polynomial $a(x,y) = \sum_{i=0}^{d_x} \sum_{j=0}^{d_y} a_{i,j} x^i y^j$. The interpolation constraints are:

$$IC_1 := \left[Q^{[a,b]}(\alpha_i, r_i) = 0 \quad \forall i \in [n] \text{ and } \forall a+b < s \right], \quad (3)$$

where $Q^{[a,b]}(x,y)$ represents the mixed Hasse derivative (see [7] for definition) of the polynomial $Q(x,y) \in \mathbb{F}[x,y]$. Analogously, one can say that the GS polynomial must have a multiplicity of s at each point (α_i, r_i).

B. Univariate Formulation of Guruswami–Sudan

In [1], [15] the univariate reformulation of the bivariate GS interpolation problem (*key equations*) was derived. Here, we state some basic properties that will be used later on.

Proposition 1 (Augot-Zeh [1]) *Given $s \geq 1$, let $Q(x,y) = \sum_{t=0}^{\ell} Q^{(t)}(x) y^t$ be the Guruswami-Sudan interpolation polynomial that satisfies (2) and (3) and let $R(x)$ be the Lagrange interpolation polynomial, such that $R(\alpha_i) = r_i \ \forall i \in [n]$ holds. Furthermore, let $G(x) = \prod_{j=1}^{n} (x - \alpha_j)$. Then, $Q(x,y)$ satisfies (3), if and only if there exist s polynomials $B^{(b)}(x) \in \mathbb{F}[x] \ \forall b \in [s-1]_0$ with:*

$$Q^{[b]}(x, R(x)) = B^{(b)}(x) \cdot G(x)^{s-b}, \quad (4)$$

where $\deg B^{(b)}(x) < \ell(n-k) - s\tau + b$.

We remark that $Q^{[b]}(x,y) := Q^{[0,b]}(x,y)$ denotes the b–th Hasse derivative of the bivariate polynomial $Q(x,y)$ with respect to the variable y.

IV. Welch–Berlekamp approach as List–1 Decoder

We recall a simplified version (as in [5] or [8, Ch. 5]) of the WB approach [10, Ch. 7.2] [2] for decoding RS codes up to half the minimum distance ($\tau_0 = \lfloor (n-k)/2 \rfloor$). It is seen as special case of the list–decoding problem of GS.

The interpolation polynomial $Q(x,y)$ of the GS algorithm for $\ell = s = 1$ has the following form:

$$Q(x,y) = Q^{(0)}(x) + Q^{(1)}(x) y,$$

where $\deg Q^{(0)}(x) < n - \tau$ and $\deg Q^{(1)}(x) < n - \tau - k + 1$. Condition (3) simplifies to $Q(\alpha_i, r_i) = 0 \ \forall i \in [n]$ and gives n linear equations. The codeword $\mathbf{c}$ coincides with the received word $\mathbf{r}$ in at least $n - \tau$ positions. Therefore, we have:

$$Q(x, f(x)) = Q^{(0)}(x) + f(x) \cdot Q^{(1)}(x) = 0.$$

So $f(x) = -Q^{(0)}(x)/Q^{(1)}(x)$ and we can rewrite the original interpolation polynomial:

$$Q(x,y) = Q^{(1)}(x) \cdot \left(y + \frac{Q^{(0)}(x)}{Q^{(1)}(x)} \right) = Q^{(1)}(x) \cdot (y - f(x)).$$

Clearly, $Q^{(1)}(x)$ is the error–locator polynomial (ELP), because it vanishes for τ_0 α_i's. Let the classical ELP $\Lambda(x) = \prod_{j \in \mathcal{J}} (x - \alpha_j)$, where $\mathcal{J}$ is the set of error locations. Then, we can write:

$$Q(x,y) = \Lambda(x) \cdot (y - f(x)). \quad (5)$$

In the WB decoding procedure the polynomial $Q(x,y)$ of (5) is determined by solving n linear homogeneous equations. The standard syndrome–based decoding procedure, that consists of τ_0 equations for the ELP, can be derived by reducing the WB equation.

V. Virtual Extension to an IRS code

A. Basic Principle

We shortly describe the Schmidt–Sidorenko–Bossert scheme [13] where an RS code is virtually extended to an IRS code. This IRS code is denoted by $\mathcal{VIRS}(n,k,s)$, where n and k are the original parameters of the $\mathcal{RS}(n,k)$ code. The parameter s denotes the order of interleaving. Let $p(x) = \sum_{j=0}^{n-1} p_j x^j$ be a univariate polynomial in $\mathbb{F}_n[x]$. Then,

$$p^{<i>}(x) = \sum_{j=0}^{n-1} p_j^i x^j,$$

is the polynomial in $\mathbb{F}_n[x]$ where each coefficient is raised to the power i. Analogously, $\mathbf{c}^{<i>}$ denotes the vector $(c_1^i, \ldots, c_n^i)^T$. The virtual IRS code can be defined as follows.

Definition 1 (Virtual Extension to an IRS code [13]) *Let $\mathcal{RS}(n,k)$ be an RS code with the evaluation polynomials $f(x)$ as defined in (1). The virtually extended Interleaved Reed–Solomon code $\mathcal{VIRS}(n,k,s)$ of order s is given by*

$$\mathcal{VIRS}(n,k,s) = \begin{pmatrix} \mathbf{c}^{<1>} \\ \mathbf{c}^{<2>} \\ \vdots \\ \mathbf{c}^{<s>} \end{pmatrix} = \begin{pmatrix} f(\mathcal{L}) & : f(x) \in \mathbb{F}_k[x] \\ f^2(\mathcal{L}) & : (f(x))^2 \in \mathbb{F}_{2(k-1)+1}[x] \\ \vdots & \\ f^s(\mathcal{L}) & : (f(x))^s \in \mathbb{F}_{s(k-1)+1}[x] \end{pmatrix}.$$

Clearly, the parameter s must satisfy $s(k-1)+1 \leq n$. The scheme is restricted to low–rate RS codes and allows to decode beyond half the minimum distance. The virtual extension is illustrated in Figure 1, where the information length of the i–th codeword is $k^{(i)} = i(k-1)+1$. The decoding procedure for the virtual extension of an RS code is as follows; the elements of received word $\mathbf{r} = \mathbf{c} + \mathbf{e}$ are raised to the power $i = 2, \ldots, s$ $(\mathbf{r}^{<2>}, \mathbf{r}^{<3>}, \ldots, \mathbf{r}^{<s>})$ and a heterogeneous IRS code is obtained. Clearly, through the virtual extension, the error is also "extended" and every single received word

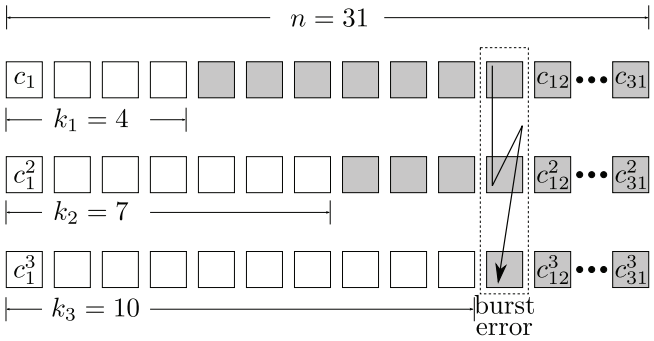

Fig. 1. Illustration of an $\mathcal{RS}(31, 4)$ code that has been virtually extended with interleaving factor $s = 3$. The errors in the $\mathcal{RS}(31, 4)$ code are extended to burst errors in the $\mathcal{VIRS}(31, 4, 3)$ code.

$\mathbf{r}^{<i>}$ is erroneous at the same positions. Due to the additional equations, the decoding radius is increased to:

$$\tau = \left\lfloor \frac{sn - \binom{s+1}{2}(k-1) - s}{s+1} \right\rfloor. \tag{6}$$

The radius τ is greater than $\tau_0 = \lfloor (n-k)/2 \rfloor$ for RS codes with code rate $R < 1/3$. (For further details (e.g. increased failure probability) of this scheme, see [13]). We remark that the rate–restriction and the increased decoding radius coincide with the original Sudan algorithm (where the multiplicity s equals one for all points (α_i, r_i)). Nevertheless, we will show that this scheme is equivalent to a GS interpolation problem with a modified multiplicity assignment and stricter degree constraints. To start the logical chain, we will describe in the following the corresponding system of equations of the s WB equations for a $\mathcal{VIRS}(n, k, s)$ code.

B. Matrix form of the Set of Equations

Bleichenbacher *et al.* [3], [4] described the WB formulation for IRS codes. We recall this approach for the virtually extended Reed–Solomon code $\mathcal{VIRS}(n, k, s)$.
Clearly, we have s WB–equations (see (5)) of the form:

$$\begin{aligned} Q^{<b>}(x, y) &= \Lambda(x) \cdot (y^b - f^b(x)) \\ &=: Q^{(s)}(x) y^b - Q^{(b)}(x), \end{aligned} \tag{7}$$

for all $b \in [s-1]_0$.
For every single WB polynomial $Q^{<b>}(\alpha_i, r_i) = 0$ holds ($i \in [n]$). Note, that through the virtual extension, each received word $\mathbf{r}^{<i>}$ has its errors at the same position and therefore we search one common ELP $\Lambda(x)$. We represent the sn constraints of system (7) in matrix form. Therefore, let the $n \times (\tau + i(k-1) + 1)$ matrix $\mathbf{M}_i$ be:

$$\mathbf{M}_i = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{N_i - 1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{N_i - 1} \\ 1 & \alpha_3 & \alpha_3^2 & \cdots & \alpha_3^{N_i - 1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{N_i - 1} \end{pmatrix}, \tag{8}$$

where $N_i := \tau + i \cdot (k-1) + 1$ and let N be defined as:

$$N = \sum_{i=0}^{s} N_i = (s+1)(\tau+1) + \binom{s+1}{2}(k-1). \tag{9}$$

Furthermore, let the $n \times n$ matrix $\mathbf{R}$ have the following form:

$$\mathbf{R} = \begin{pmatrix} r_1 & \cdots & 0 & 0 \\ 0 & r_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & r_n \end{pmatrix}. \tag{10}$$

Now, we can write the s polynomial equations from (7) in matrix notation. Let $\mathbf{Q} = (\mathbf{Q}^{(0)}, \mathbf{Q}^{(1)}, \ldots, \mathbf{Q}^{(s)})^T$, where $\mathbf{Q}^{(i)} = (Q_0^{(i)}, Q_1^{(i)}, \ldots, Q_{\tau+(s-i)(k-1)}^{(i)})^T$. The homogeneous set of equations is of the form $\mathbf{A} \cdot \mathbf{Q} = \mathbf{0}$, where the $sn \times N$ matrix $\mathbf{A}$ is:

$$\mathbf{A} = \begin{pmatrix} \mathbf{0} & \cdots & \mathbf{0} & -\mathbf{M}_1 & \mathbf{R} \cdot \mathbf{M}_0 \\ \mathbf{0} & \cdots & -\mathbf{M}_2 & \mathbf{0} & \mathbf{R}^2 \cdot \mathbf{M}_0 \\ \vdots & \iddots & \vdots & \vdots & \vdots \\ -\mathbf{M}_s & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{R}^s \cdot \mathbf{M}_0 \end{pmatrix}. \tag{11}$$

The vector $\mathbf{Q}^{(s)}$ gives the coefficients of the ELP $\Lambda(x)$.

VI. Reformulation as a modified Guruswami–Sudan problem

A. Specific Multiplicity Assignment

In this section, we formulate the decoding of an $\mathcal{RS}(n, k)$ code virtually extended to a $\mathcal{VIRS}(n, k, s)$ code as a modified GS interpolation problem. The constraints of the bivariate interpolation polynomial with multiplicities are a modified version of the general GS algorithm introduced in Section III. We show the corresponding homogeneous set of equations and prove the equivalence to the one of Bleichenbacher *et al.* (see (11)).
Let $\overline{Q}(x, y)$ be a bivariate polynomial of $\mathbb{F}[x, y] \setminus \{0\}$, where

$$DC_2 := \begin{bmatrix} \deg_{0,1} \overline{Q}(x, y) \le s, \\ \deg \overline{Q}^{(t)}(x) \le \tau + (s-t) \cdot (k-1) \end{bmatrix}. \tag{12}$$

The modified interpolation constraints for $\overline{Q}(x, y)$ are:

$$IC_2 := \left[\overline{Q}^{[b]}(\alpha_i, r_i) = 0 \quad \forall i \in [n] \text{ and } \forall b \in [s-1]_0 \right], \tag{13}$$

where the parameter s is such that $s(k-1) + 1 \le n$ holds and $\overline{Q}^{[b]}(x, y)$ denotes the b–th Hasse derivative with respect to the variable y of the polynomial $\overline{Q}(x, y)$.

Theorem 1 *It exists at least one nonzero polynomial $\overline{Q}(x, y)$ which satisfies conditions (13).*

Proof: Condition (13) gives sn homogeneous linear equations to the coefficients. The number of possible coefficients is N (as defined in (9)), therefore we get a nonzero solution for the decoding radius τ as in Equation (6) . ∎
The bivariate polynomial $\overline{Q}(x, y)$ that fulfills condition (13) has multiplicity s for all $n - \tau$ error–free positions and

multiplicity one for all τ error positions. Let us state this property in the following theorem.

Theorem 2 *The bivariate polynomial $\overline{Q}(x,y)$ under the constraints DC_2 and IC_2 can be written as:*

$$\overline{Q}(x,y) = \overline{Q}^{(s)}(x) \cdot (y - f(x))^s, \tag{14}$$

where $\overline{Q}^{(s)}(x)$ is the ELP and $f(x)$ is the information polynomial of the RS code (see definition (1)).

Proof: Let us consider the "last" $(s-1)$–th Hasse derivative of $\overline{Q}(x,y)$ with respect to the variable y:

$$\begin{aligned}\overline{Q}^{[s-1]}(x,y) &= \binom{s-1}{s-1} \cdot \overline{Q}^{(s-1)}(x) + \binom{s}{s-1} \cdot \overline{Q}^{(s)}(x)y \\ &= \overline{Q}^{(s-1)}(x) + s \cdot \overline{Q}^{(s)}(x)y \\ &= s \cdot \overline{Q}^{(s)}(x) \cdot \left(y + \frac{\overline{Q}^{(s-1)}(x)}{s \cdot \overline{Q}^{(s)}(x)} \right),\end{aligned}$$

which is by (13) zero for the set $\{(\alpha_i, r_i)\}_{i=1}^n$. Clearly, $\overline{Q}^{[s-1]}(x,y)$ is a WB polynomial for the $\mathcal{RS}(n,k)$ code with information polynomial $f(x) = -\overline{Q}^{(s-1)}(x)/s \cdot \overline{Q}^{(s)}(x)$ (see Section IV).

The $(s-2)$–th Hasse derivative of the interpolation polynomial $\overline{Q}^{[s-2]}(x,y)$ can now be rewritten as:

$$\begin{aligned}\overline{Q}^{[s-2]}(x,y) =& \overline{Q}^{(s-2)}(x) + \binom{s-1}{s-2} \cdot \overline{Q}^{(s-1)}(x)y + \\ & \binom{s}{s-2} \cdot \overline{Q}^{(s)}(x)y^2 \\ =& \overline{Q}^{(s-2)}(x) + (s-1) \cdot \overline{Q}^{(s-1)}(x)y + \\ & \frac{1}{2}s(s-1) \cdot \overline{Q}^{(s)}(x)y^2 \\ =& \frac{1}{2}s(s-1) \cdot \overline{Q}^{(s)}(x) \cdot (y^2 - f(x)y) + \\ & \overline{Q}^{(s-2)}(x),\end{aligned} \tag{15}$$

where

$$\overline{Q}^{[s-2]}(x, f(x)) = 0$$

from the interpolation constraints holds. We can now express $\overline{Q}^{(s-2)}(x)$ as:

$$\begin{aligned}\overline{Q}^{(s-2)}(x) &= -\frac{1}{2}s(s-1) \cdot \overline{Q}^{(s)}(x) \cdot (f(x)^2 - 2f(x)^2) \\ &= \frac{1}{2}s(s-1) \cdot f(x)^2 \cdot \overline{Q}^{(s)}(x).\end{aligned} \tag{16}$$

Substituting this into (15), we obtain for the $(s-2)$–th Hasse derivative of $\overline{Q}(x,y)$:

$$\overline{Q}^{[s-2]}(x,y) = \frac{1}{2}s(s-1) \cdot \overline{Q}^{(s)}(x) \cdot (y - f(x))^2,$$

which has multiplicity two at the $n-\tau$ error–free positions and multiplicity one at the τ erroneous positions. By induction we can state that $(y - f(x))^s | \overline{Q}(x,y)$ and $Q^{(s)}(x) | \overline{Q}(x,y)$. From DC_2 we know, that no other polynomial factor occurs in $\overline{Q}(x,y)$. ■

B. Informal Description

The degree condition DC_2 and the interpolation constraint IC_2 for the polynomial $\overline{Q}(x,y)$ are a subset of the general GS list–decoding constraints DC_1 and IC_1. The y–degree of $\overline{Q}(x,y)$ corresponds to the number of codewords of the $\mathcal{VIRS}(n,k,s)$ code. Similar to the univariate formulation of the original GS interpolation problem (see (4)) it is sufficient to consider only the Hasse derivatives with respect to variable y.

In the original GS algorithm the b–th Hasse derivative of the interpolation polynomial $Q(x,y)$ is divisible by $G(x)^{(s-b)}$, where $G(x) = \prod_{i=1}^n (x - \alpha_i)$ and n denotes the code length. In our case the b–th Hasse derivative of the modified interpolation polynomial $\overline{Q}(x,y)$ is divisible by $\overline{G}(x)^{(s-b)}$. Here, $\overline{G}(x) = \prod_{i \in [n] \setminus \mathcal{J}} (x - \alpha_i)$ and $[n] \setminus \mathcal{J}$ is the set of error–free positions.

Furthermore, the ELP $\overline{Q}^{(s)}(x)$, where $\deg \overline{Q}^{(s)}(x)$ can be greater than $\lfloor (n-k)/2 \rfloor$, is a factor of $\overline{Q}(x,y)$. The zeros of $\overline{Q}^{(s)}(x)$ have multiplicity one.

The scheme of Section V virtually extends the received vector $\mathbf{r} = (r_1, r_2, \ldots, r_n)$ of an $\mathcal{RS}(n,k)$ code to s received words $\mathbf{r}^{<i>} = (r_1^i, r_2^i, \ldots, r_n^i)$ $\forall i \in [s]$ of s different $\mathcal{RS}(n, i(k-1)+1)$ codes with equal code length n.

C. Set of Equations

Now, we consider the homogeneous set of equations (13). We have $\overline{\mathbf{B}} \cdot \overline{\mathbf{Q}} = \mathbf{0}$, where $\overline{\mathbf{Q}}$ is the vector notation of the interpolation polynomial $\overline{Q}(x,y)$. The $sn \times N$ matrix $\overline{\mathbf{B}}$ can be written as:

$$\begin{pmatrix} \mathbf{0} & \cdots & \mathbf{0} & \binom{s-1}{s-1}\mathbf{M}_1 & \binom{s}{s-1}\mathbf{R}\mathbf{M}_0 \\ \mathbf{0} & \cdots & \binom{s-2}{s-2}\mathbf{M}_2 & \binom{s-1}{s-2}\mathbf{R}\mathbf{M}_1 & \binom{s}{s-2}\mathbf{R}^2\mathbf{M}_0 \\ \vdots & \iddots & \vdots & \vdots & \vdots \\ \mathbf{M}_s & \mathbf{R}\mathbf{M}_{s-1} & \cdots & \mathbf{R}^{s-1}\mathbf{M}_1 & \mathbf{R}^s\mathbf{M}_0 \end{pmatrix}$$

where the sub–matrices $\mathbf{M}_i$ and $\mathbf{R}$ are defined in (8) and (10). The binomial coefficients come from the Hasse derivatives of $\overline{Q}(x,y)$:

$$\overline{Q}^{[b]}(x,y) = \sum_{t=b}^{s} \binom{t}{b} \cdot \overline{Q}^{(t)}(x)y^{t-b}. \tag{17}$$

Note, that the first n rows of matrix $\overline{\mathbf{B}}$ correspond to the $(s-1)$th Hasse derivative of the polynomial $\overline{Q}(x,y)$. The second n rows represents the n interpolation constraints of the $(s-2)$–th Hasse derivative and so on. In the last n rows of matrix $\overline{\mathbf{B}}$ the interpolation polynomial $\overline{Q}(x,y)$ occurs with all terms.

D. Equivalence of Both Sets of Equations

In the following, we show the equivalence between the systems of equations determining the IRS scheme of Section V and the one determining the modified GS interpolation polynomial $\overline{Q}(x,y)$. Due to space limitations we will sketch the basic steps of the proof.

First, let us consider the relation between vectors $\mathbf{Q}$ and $\overline{\mathbf{Q}}$:

$$\begin{aligned}\overline{Q}(x,y) =& \overline{Q}^{(s)}(x)(y-f(x))^s \\ =& \overline{Q}^{(s)}(x)\cdot\left(\sum_{i=0}^{s}\binom{s}{i}(-1)^i y^{s-i} f(x)^i\right).\end{aligned}$$

In vector notation, we have:

$$(\mathbf{Q}^{(0)},\ldots,\binom{s}{s-2}\mathbf{Q}^{(s-2)},-\binom{s}{s-1}\mathbf{Q}^{(s-1)},\mathbf{Q}^{(s)})^T = (\overline{\mathbf{Q}}^{(0)},\ldots,\overline{\mathbf{Q}}^{(s-2)},\overline{\mathbf{Q}}^{(s-1)},\overline{\mathbf{Q}}^{(s)})^T.$$

Let the matrix $\mathbf{B}$ be such that:

$$\overline{\mathbf{B}}\cdot\overline{\mathbf{Q}} = \mathbf{B}\cdot\mathbf{Q}.$$

Matrix $\mathbf{B}$ is then (first column not printed):

$$\mathbf{B} = \begin{pmatrix} \cdots & \mathbf{0} & -\binom{s}{s-1}\mathbf{M}_1 & \binom{s}{s-1}\mathbf{R}\mathbf{M}_0 \\ \cdots & \binom{s}{s-2}\mathbf{M}_2 & -\binom{s}{s-1}\binom{s-1}{s-2}\mathbf{R}\mathbf{M}_1 & \binom{s}{s-2}\mathbf{R}^2\mathbf{M}_0 \\ \iddots & \vdots & \vdots & \vdots \\ \cdots & \cdots & -\binom{s}{s-1}\mathbf{R}^{s-1}\mathbf{M}_1 & \mathbf{R}^s\mathbf{M}_0 \end{pmatrix}.$$

After simplification, we obtain:

$$\mathbf{B} = \begin{pmatrix} \cdots & \mathbf{0} & -\mathbf{M}_1 & \mathbf{R}\mathbf{M}_0 \\ \cdots & \frac{1}{2}s(s-1)\mathbf{M}_2 & -s(s-1)\mathbf{R}\mathbf{M}_1 & \frac{1}{2}s(s-1)\mathbf{R}^2\mathbf{M}_0 \\ \iddots & \vdots & \vdots & \vdots \\ \cdots & \cdots & -s\mathbf{R}^{s-1}\mathbf{M}_1 & \mathbf{R}^s\mathbf{M}_0 \end{pmatrix}.$$

The second band of n rows of matrix $\mathbf{B}$ can be multiplied with $-\mathbf{R}s(s-1)$–times the first band of $\mathbf{B}$ and then divided by $-\frac{1}{2}s(s-1)$. We obtain the second band of n rows of matrix $\mathbf{A}$. Repeating this operation, matrix $\mathbf{B}$ can be transformed into matrix $\mathbf{A}$ (11).

VII. Conclusion

We investigated a virtual extension of an RS code to an IRS code from an interpolation–based list–decoding approach point of view.

The Bleichenbacher scheme was used to form the system of equations for the IRS scheme (based on a virtual extension). Then, the original constraints of the GS list–decoding algorithm were modified and the equivalence of the resulting system of equations with the Bleichenbacher scheme for the IRS code has been shown.

References

[1] D. Augot and A. Zeh, "On the Roth and Ruckenstein Equations for the Guruswami-Sudan Algorithm," in *Information Theory, 2008. ISIT 2008. IEEE International Symposium on*, 2008, pp. 2620–2624. [Online]. Available: http://dx.doi.org/10.1109/ISIT.2008.4595466

[2] E. R. Berlekamp and L. Welch, "Error correction of algebraic block codes," US Patent Number 4,633,470.

[3] D. Bleichenbacher, A. Kiayias, and M. Yung, "Decoding of Interleaved Reed–Solomon Codes over Noisy Data," in *Automata, Languages and Programming*, ser. Lecture Notes in Computer Science, 2003, ch. 9, p. 188. [Online]. Available: http://dx.doi.org/10.1007/3-540-45061-0_9

[4] ——, "Decoding Interleaved Reed–Solomon codes over noisy channels," *Theor. Comput. Sci.*, vol. 379, no. 3, pp. 348–360, 2007. [Online]. Available: http://dx.doi.org/10.1016/j.tcs.2007.02.043

[5] P. Gemmell and M. Sudan, "Highly resilient correctors for polynomials," *Informartion Processing Letters*, vol. 43, no. 4, pp. 169–174, 1992. [Online]. Available: http://dx.doi.org/10.1016/0020-0190(92)90195-2

[6] V. Guruswami and M. Sudan, "Improved decoding of Reed-Solomon and algebraic-geometry codes," *IEEE Transactions on Information Theory*, vol. 45, no. 6, pp. 1757–1767, 1999. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=782097

[7] H. Hasse, "Theorie der höheren Differentiale in einem algebraischen Funktionenkörper mit vollkommenem Konstantenkörper bei beliebiger Charakteristik." *J. Reine Angew. Math.*, vol. 175, pp. 50–54, 1936.

[8] J. Justesen and T. Hoholdt, *A Course in Error-Correcting Codes (EMS Textbooks in Mathematics)*. European Mathematical Society, February 2004.

[9] Krachkovsky and Y. X. Lee, "Decoding of parallel Reed–Solomon codes with applications to product and concatenated codes," August 1998, pp. 55+. [Online]. Available: http://dx.doi.org/10.1109/ISIT.1998.708636

[10] T. K. Moon, *Error Correction Coding: Mathematical Methods and Algorithms*. Wiley-Interscience, June 2005.

[11] R. M. Roth and G. Ruckenstein, "Efficient decoding of Reed-Solomon codes beyond half the minimum distance," *Information Theory, IEEE Transactions on*, vol. 46, no. 1, pp. 246–257, 2000. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=817522

[12] G. Ruckenstein, "Error decoding strategies for algebraic codes," Ph.D. dissertation, Technion, 2001. [Online]. Available: http://www.cs.technion.ac.il/users/wwwb/cgi-bin/tr-info.cgi/2001/PHD/PHD-2001-01

[13] G. Schmidt, V. Sidorenko, and M. Bossert, "Decoding Reed-Solomon Codes Beyond Half the Minimum Distance using Shift-Register Synthesis," in *Information Theory, 2006 IEEE International Symposium on*, 2006, pp. 459–463. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4036003

[14] M. Sudan, "Decoding of reed solomon codes beyond the error-correction bound," *Journal of Complexity*, vol. 13, no. 1, pp. 180–193, March 1997. [Online]. Available: http://dx.doi.org/10.1006/jcom.1997.0439

[15] A. Zeh, C. Gentner, and D. Augot, "A Berlekamp-Massey Approach for the Guruswami-Sudan Decoding Algorithm for Reed-Solomon Codes," *preprint*, 2010.

Appendix

Let us consider an $\mathcal{RS}(16,4)$ code over $\mathbb{F} = GF(17)$ with parameter $s=2$ (number of interleaving and multiplicity for the modified GS algorithm). The corresponding increased decoding radius is $\tau = 7$ (see (6)).

The code locators are $\alpha_i = \alpha^{i-1}\ \forall i \in [n]$, where α is 3. For the information polynomial $f(x) = 1 + x + x^2 + x^3$ (see (1)) and an error $\mathbf{e}$ of weight $\tau = 7$ we get the following vectors:

$$\begin{aligned}\mathbf{c} &= (4,6,4,6,0,3,12,2,0,14,7,9,0,15,15,4)\\ \mathbf{e} &= (1,2,3,4,5,6,7,0,0,0,0,0,0,0,0,0)\\ \mathbf{r}^{<1>} &= (5,8,7,10,5,9,2,2,0,14,7,9,0,15,15,4)\\ \mathbf{r}^{<2>} &= (8,13,15,15,8,13,4,4,0,9,15,13,0,4,4,16).\end{aligned}$$

The conditions (13) on the modified bivariate polynomial $\overline{Q}(x,y)$ give the following solution:

$$\begin{aligned}\overline{\mathbf{Q}} =& (5,14,8,6,14,9,5,9,12,12,4,2,3,16,5,9,11,\\ & 15,13,4,7,2,16,4,16,5,4,2,4,3,12,5,16).\end{aligned}$$

And the corresponding modified bivariate interpolation polynomial;

$$\begin{aligned}\overline{Q}(x,y) =& (x+2)(x+4)(x+7)(x+8)(x+12)(x+14)\cdot\\ & (x+16)(y+16x^3+16x^2+16x+16)^2,\end{aligned}$$

is factorizable as stated in Theorem 2.