On the Roth and Ruckenstein equations for the Guruswami-Sudan algorithm

Daniel Augot, Alexander Zeh

On the Roth and Ruckenstein Equations for the Guruswami-Sudan Algorithm

Daniel Augot and Alexander Zeh
Team SECRET, INRIA Paris-Rocquencourt, France
{daniel.augot,alexander.zeh}@inria.fr

***Abstract*—In 2000 Roth and Ruckenstein proposed an Extended Key Equation for solving the interpolation step in the Sudan decoding algorithm. Generalizing their idea, a sequence of key equations for the Guruswami-Sudan (GS) algorithm, which is able to list decode a Reed-Solomon code with arbitrary rate, is derived.**
This extension allows a reduction of the number of equations and therefore a reduction of the algorithm's complexity. Furthermore, we indicate how to adapt the Fundamental Iterative Algorithm for block Hankel matrices and thus solving the GS-interpolation step efficiently.

***Index Terms*—Guruswami-Sudan algorithm, list decoding, (Extended) Key Equation, Reed-Solomon codes, polynomial interpolation**

I. Introduction

The Sudan [1] list decoding algorithm is applicable to Reed-Solomon (RS) codes with a code rate $R < 1/3$. It consists of an interpolation and a factorization step. Beside their well-known factorization method Roth and Ruckenstein [2] have also derived a so-called Extended Key Equation (EKE), which is a generalization of the classical Key Equation for unique decoding, by reformulating the interpolation condition of Sudan. The EKE can be solved by an adaption of the Fundamental Iterative Algorithm (FIA) (presented in [3], [4]) for the case of l horizontally arranged Hankel-matrices (where l is the list size).
Guruswami and Sudan [5] extended the originally interpolation approach by using multiplicities of higher order. This increases the decoding radius and can be applied to RS codes with arbitrary rate. Ruckenstein predicted in her thesis [6, Ch. 5] that the resulting set of equations for the GS-case can be solved in quadratic time.
We generalize the idea of Roth and Ruckenstein [2] and obtain a set of key equations for the GS-case, which allows a reduction of the decoding algorithm's complexity.
In the next section we recall shortly the GS-principle and in Section III the derivation of the EKE.
We reformulate the condition for the interpolation step of the GS-algorithm in Section IV to get an appropriate basis for the derivation of the set of key equations, which is presented in the sections V and VI. The corresponding syndrome polynomials are defined in Section VII. In the same way as in the case of the EKE for the Sudan-algorithm, some variables of the resulting set of equations (see Section VIII) can be removed. For a low-rate RS code the gain is very high. In Section IX we describe how this reduced set of equations can be solved efficiently. Finally, we conclude in Section X.

Alexander Zeh is now with the Institute of Communication Networks and Computer Engineering, University of Stuttgart, Pfaffenwaldring 47, D-70569 Stuttgart, Germany alexander.zeh@ikr.uni-stuttgart.de

II. The Guruswami-Sudan principle

The Guruswami-Sudan principle [5] is recalled shortly. Let $\{x_1, \ldots, x_n\}$ be the support of a $[n, k]$ Reed-Solomon code, where all the $x_i \in F_q$ are distinct. Let k be the dimension and $d = n - k + 1$ the minimum distance of the RS code under consideration. The received word is denoted by $y = (y_1, \ldots, y_n)$ and τ is the number of errors that can be corrected. The parameter s is the order of multiplicity of the bivariate interpolation polynomial in the GS-algorithm. Then the GS-polynomial $Q(X, Y)$ has to fulfill the following three conditions:

① $Q(X, Y) \neq 0$;
② $Q(X, Y) = \sum_{t=0}^{l} Q_t(X) Y^t$, where $\deg Q_t(X) < N_t$ with $N_t = s(n - \tau) - t(k - 1)$;
③ $\text{mult}(Q, (x_i, y_i)) \geq s$, $i = 1, \ldots, n$.

We recall that the condition ③ is the multiplicity condition defined as follows: Let $Q(X, Y) = Q_0 + Q_1 + \cdots + Q_i + \cdots$ be given, where Q_i is homogeneous of degree i. The multiplicity of Q at the point $(0, 0)$ is the smallest i such that $Q_i \neq 0$ and the multiplicity of Q at the point (x_i, y_i) is the multiplicity at $(0, 0)$ of the polynomial $Q(X + x_i, Y + y_i)$.
Then for all $f(X)$, corresponding to codewords c such that $d(f, c) \leq \tau$, it holds, that $Q(X, f(X)) = 0$. It is noted, that $s = 1$ in the case of Sudan.

III. The Extended Key Equation (EKE) for the Sudan-algorithm

In this section, the derivation of the Extended Key Equation of the Sudan algorithm [1], which was presented in [2], is summarized. Moreover, the principle of the algorithm solving this key equation is mentioned.
The initial point of the derivation of Roth and Ruckenstein [2] is that condition ③ for $s = 1$ is equivalent to the existence of a polynomial $B(X)$, such that the following relation holds. The polynomial $R(X)$ is the Lagrange interpolation polynomial such that $R(x_i) = y_i$ and $G(X) := \prod_{i=1}^{n}(X - x_i)$:

$$\sum_{t=0}^{l} Q_t(X) \cdot (R(X))^t = B(X) \cdot G(X). \tag{1}$$

Introducing the reversed polynomials $\bar{R}(X)$, $\bar{G}(X)$, $\bar{B}(X)$ and $\Lambda_t(X)$ for $Q_t(X)$ for all $t = 1, \ldots, l$ in Equation (1) and with the reduction $\bmod X^{l(n-k)}$, we obtain the following intermediate equation:

$$\sum_{t=1}^{l} \Lambda_t(X) \cdot X^{(l-t)(n-k)} \cdot (\bar{R}(X))^t \equiv \bar{B}(X) \cdot \bar{G}(X) \bmod X^{l(n-k)}. \quad (2)$$

The formal power series $S_\infty^t(X)$ for all $t = 1, \ldots, l$ is defined by

$$\frac{(\bar{R}(X))^t}{\bar{G}(X)} = X^{(t-1)(n-1)} \cdot S_\infty^t(X) + U_t(X), \quad (3)$$

where $U_t(X) \in F_{(t-1)(n-1)}[X]$ is the entire part of the partial fraction decomposition.

The degree of the syndrome polynomial $S_\infty^t(X)$ in Equation (2) can be limited (to $\tau + N_t - 1$) and the corresponding truncated polynomial is thus denoted by $S^t(X)$. Inserting this definition in (2) and dividing with $X^{(l-1)(n-k)}$ leads to the final expression of the Extended Key Equation of Roth and Ruckenstein for the Sudan algorithm:

$$\sum_{t=1}^{l} \Lambda_t(X) \cdot X^{(t-1)(k-1)} \cdot S^t(X) \equiv \Omega(X) \bmod X^{n-k}, \quad (4)$$

where

$$\deg \Omega(X) < n - k - \tau. \quad (5)$$

Equation (4) (where the RHS is zero) can be written in a more explicit form (see Equation (6)). Notice that the number of unknowns (compared with the interpolation condition ③ for $s = 1$) has been reduced by $n - \tau$. From (4) we obtain

$$\sum_{t=1}^{l} \sum_{c=0}^{N_t - 1} Q_{t,c} \cdot S_{i+c}^t = 0, \quad 0 \le i < \tau. \quad (6)$$

To get an idea of the algorithm, which solves Equations (6) efficiently, it is helpful to consider the matrix representation of the equation.

We write the coefficients of the shortened bivariate interpolation polynomial $Q^*(X, Y)$ (where $Q(X, Y) = Q_0(X) + Q^*(X, Y)$) as a vector $\mathbf{Q}^*$:

$$\mathbf{Q}^* = \begin{pmatrix} \mathbf{Q}_1 \\ \mathbf{Q}_2 \\ \vdots \\ \mathbf{Q}_l \end{pmatrix}, \quad (7)$$

where

$$\mathbf{Q}_t = (Q_{t,0}, Q_{t,1}, \ldots, Q_{t,N_t-1})^T. \quad (8)$$

Equivalent to this representation the syndrome polynomials $S^t(X)$ lead to l Hankel matrices $\mathbf{S}^t = [S_{i,c}^t]_{i,c} \, \forall \, t = 1, \ldots, l$. The number of rows of the matrices $\mathbf{S}^t$ is τ and the number of columns is N_t. Finally, we recall the following matrix representation for the EKE:

$$\begin{pmatrix} \mathbf{S}^1 & \mathbf{S}^2 & \cdots & \mathbf{S}^l \end{pmatrix} \cdot \mathbf{Q}^* = \mathbf{0}. \quad (9)$$

Based on the former work of Feng and Tzeng [3], [4] the proposed algorithm in [2] for an horizontal band of l Hankel matrices $\mathbf{S}^t$ has a time complexity of $O(l\tau^2)$ and a space complexity of $O(l\tau)$.

It should be mentioned that for the preprocessing of the syndrome polynomials, an explicit expression of the syndrome coefficients S_i^t was derived:

$$S_i^t = \sum_{j=0}^{n} y_j^t \eta_j x_j^i, \quad t = 1, \ldots, l, \, i \ge 0, \quad (10)$$

where $\eta_j^{-1} = \prod_{r \in \{1,\ldots,n\} \setminus \{j\}} (x_j - x_r)$. The missing $Q_0(X)$ can be interpolated with $N_0 = n - \tau$ pairs (x_i, y_i), because of the relation:

$$Q_0(x_i) = -Q^*(x_i, y_i) = -\sum_{t=1}^{l} Q_t(x_i) y_i^t, \quad i = 1, \ldots, n$$

IV. Univariate equations

We now consider the general case of $s > 1$. Let $Q^{[b]}(X, Y)$ denote the b-th Hasse derivative (see [7] for definition) of the bivariate polynomial $Q(X, Y)$ with respect to the Y variable:

$$Q^{[b]}(X, Y) = \sum_{t=b}^{l} \binom{t}{b} Q_t(X) Y^{t-b},$$

where l is the Y-degree of $Q(X, Y)$. There exists a Taylor formula of the form:

$$Q(X, Y + y_i) = \sum_{b=0}^{l} Q^{[b]}(X, y_i) Y^b \quad (11)$$

Let $R(X)$ be the Lagrange interpolation polynomial such that $R(x_i) = y_i$ and $G(X)$ be the polynomial $\prod_{i=1}^{n}(X - x_i)$ (as defined in Section III). Using the Taylor formula with the Hasse derivatives, we can formulate the following proposition.

Proposition 1: One has $\text{mult}(Q, (x_i, y_i)) \ge s$, $i = 1, \ldots, n$ if and only if

$$G(X)^{s-b} | Q^{[b]}(X, R(X)), \quad b = 0, \ldots, s-1. \quad (12)$$

Thus the interpolation condition ③ can be replaced by the condition: for each $b = 0, \ldots, s-1$, there exists a polynomial $B_b(X)$ such that:

$$\begin{aligned} Q^{[b]}(X, R(X)) &= \sum_{t=b}^{l} \binom{t}{b} Q_t(X) R(X)^{t-b} \\ &= B_b(X) G(X)^{s-b}, \end{aligned} \quad (13)$$

with $\deg B_b(X) < l(n-k) - \tau s + b$, as it can be found by counting the degrees.

V. Removing the diagonal terms

We use the Roth and Ruckenstein reversion of the coefficients technique and write $\Lambda_t(X)$, $\bar{R}(X)$, $\bar{G}(X)$ and $\bar{B}_b(X)$ for the reciprocal polynomial of $Q_t(X)$, $R(X)$, $G(X)$ and $B_b(X)$ respectively, which are obtained by reversing the order of the coefficients. Then the Equation (13) leads to

$$\sum_{t=b}^{l} \Lambda_t(X) \binom{t}{b} X^{(l-t)(n-k)} \bar{R}(X)^{t-b} = \bar{B}_b(X) \bar{G}(X)^{s-b} \quad (14)$$

for $b = 0, \ldots, s-1$. Let us write $\text{EKE}_0(b)$ for such an equation. Obviously we can consider the equation modulo $X^{(l-b)(n-k)}$, to get the equation $\text{EKE}(b)$:

$$\sum_{t=b+1}^{l} \Lambda_t(X)\binom{t}{b} X^{(l-t)(n-k)} \bar{R}(X)^{t-b} \equiv \bar{B}_b(X)\bar{G}(X)^{s-b} \mod X^{(l-b)(n-k)}. \quad (15)$$

Proposition 2: Let b be such that $s\tau - bd > 0$. If $\Lambda_{b+1}(X), \Lambda_{b+2}(X), \ldots, \Lambda_l(X)$ is a solution to $\text{EKE}(b)$, then there exists $\Lambda_b(X)$ such that $\Lambda_b(X), \Lambda_{b+1}(X), \ldots, \Lambda_l(X)$ is a solution to $\text{EKE}_0(b)$.

Proof: Consider the equation in the $Q_i(X)$'s as in Equation (13). Isolating $Q_b(X)$, we get

$$Q_b(X) + \sum_{t=b+1}^{l} \binom{t}{b} Q_t(X) R(X)^{t-b} = B_b(X)G(X)^{s-b}. \quad (16)$$

and thus $Q_b(X)$ is the remainder of the Euclidean division of $\sum_{t=b+1}^{l}\binom{t}{b}Q_t(X)R(X)^{t-b}$ by $G(X)^{s-b}$, as long as $\deg Q_b(X) < \deg G(X)^{s-b}$, which gives $s(n-\tau)-b(k-1) \leq (s-b)n$ i.e. $s\tau - bd \geq 0$. ∎

The polynomials $\bar{G}(X)^{s-b}$ are invertible mod $X^{(l-b)(n-k)}$. Thus, after division by $\bar{G}(X)^{s-b}$, Equation (15) implies $(l-b)(n-k) - \deg B_b$ linear equations on the coefficients of the $\Lambda_t(X)$. Or $(l-b)(n-k) - \deg B_b > 0 \iff s\tau - bd > 0$. Let b_0 be the maximum b such that $s\tau - b_0 d \geq 0$, i.e. $b_0 = \lfloor \frac{s\tau}{d} \rfloor$.

VI. The Matrix Form

It can be shown that the Equation (13) leads to a linear system, which can be written in block form:

$$\begin{pmatrix} \mathbf{S}^{0,0} & \mathbf{S}^{0,1} & \ldots & \ldots & \ldots & \mathbf{S}^{0,l} \\ 0 & \mathbf{S}^{1,1} & \ldots & \ldots & \ldots & \mathbf{S}^{1,l} \\ \vdots & & \ddots & & \vdots & \\ 0 & \ldots & 0 & \mathbf{S}^{s-1,s-1} & \ldots & \mathbf{S}^{s-1,l} \end{pmatrix} \begin{pmatrix} \mathbf{\Lambda}_0 \\ \vdots \\ \mathbf{\Lambda}_l \end{pmatrix} = 0, \quad (17)$$

where each matrix $\mathbf{S}^{b,t}$ has $(s-b)n$ rows (number of equations for each order b of the derivation), and $\deg Q_t < N_t$ columns. In the case of $s = 1$ the matrix has only one horizontal block and the optimization of Roth and Ruckenstein was to remove the Q_0 (Λ_0) term in the first equation. In our case, we can remove the Λ_i for $i < b_0$.

VII. Explicit expression of the syndromes

Since $G(X)$ is relatively prime to $X^{(l-b)(n-k)}$, it admits an inverse modulo $X^{(l-b)(n-k)}$. By $S_\infty^{b,t}(X)$ the Taylor series of $\bar{R}(X)^{t-b}/\bar{G}(X)^{s-b}$ is denoted. Then the Equation (15) gives, for $b = 0, \ldots, s-1$:

$$\sum_{t=b+1}^{l} \Lambda_t(X)\binom{t}{b} X^{(l-t)(n-k)} S_\infty^{b,t}(X) \equiv \bar{B}_b(X) \mod X^{(l-b)(n-k)}. \quad (18)$$

Since all the terms of degree higher than $(l-b)(n-k)$ are discarded by the modulo operation, it is sufficient to consider $S^{b,t}(X) \equiv S_\infty^{b,t}(X) \bmod X^{(l-b)(n-k)-(l-t)(n-k)}$, i.e. $S^{b,t}(X) \equiv S_\infty^{b,t}(X) \bmod X^{(t-b)(n-k)}$. Thus Equation (18) is equivalent to:

$$\sum_{t=b+1}^{l} \Lambda_t(X)\binom{t}{b} X^{(l-t)(n-k)} S^{b,t}(X) \equiv \bar{B}_b(X) \mod X^{(l-b)(n-k)}. \quad (19)$$

Let $T_{b,t}(X)$ denote $\binom{t}{b}X^{(l-t)(n-k)}S^{b,t}(X)$. Then Equation (19) leads to $s\tau - bd$ equations:

$$\sum_{t=b+1}^{l} \left(\Lambda_t(X)T_{b,t}(X)\right)_{|i} = 0,$$

where

$$i = \deg B_b(X) + 1, \ldots, (l-b)(n-k).$$

and where $P(X)_{|i}$ denotes the i-th coefficient of a given polynomial $P(X)$. Now

$$\left(\Lambda_t(X)T_{b,t}(X)\right)_{|i} = \sum_{j=0}^{i} \Lambda_{t|i-j} T_{b,t|j},$$

and the condition $i - j < N_t$ has to be fulfilled. From the inequality $i \geq \deg B_b(X) + 1$, we can bound j:

$$\begin{aligned} j &> i - N_t \\ &> l(n-k) + b + 1 - sn + t(k-1) \end{aligned} \quad (20)$$

Since $T_{b,t} = \binom{t}{b}X^{(l-t)(n-k)}S^{b,t}(X)$, this amount take the coefficient of $S^{b,t}(X)$ of index larger than:

$$(l(n-k)+b+1-sn+t(k-1)) - (l-t)(n-k) = b+1-sn-t+nt \quad (21)$$

into account. On the other hand, we express the Euclidean division of $\bar{R}(X)^{t-b}$ by $\bar{G}(X)^{s-b}$ as $\bar{R}(X)^{t-b} = \bar{U}_{b,t}(X)\bar{G}(X)^{s-b} + \bar{V}_{b,t}(X)$. In the following partial fraction decomposition:

$$S_\infty^{b,t}(X) = \frac{\bar{R}(X)^{t-b}}{\bar{G}(X)^{s-b}} = \bar{U}_{b,t}(X) + \frac{\bar{V}_{b,t}(X)}{\bar{G}(X)^{s-b}} \quad (22)$$

the entire part $\bar{U}_{b,t}(X)$ has degree $(n-1)(t-b) - (s-b)n = b+1-sn-t+nt$ which exactly one less than in Equation (21). This means that the entire part has not be taken into account, and that only the coefficients of the fraction $\bar{V}_{b,t}(X)/\bar{G}(X)^{s-b}$ of index higher than or equal to $b+1-sn-t+nt$ has to be computed. Then we have (from [8]):

$$\begin{aligned} \frac{\bar{V}_{b,t}(X)}{\bar{G}(X)^{s-b}} &= \sum_{i=1}^{n} \eta_i \frac{\bar{V}_{b,t}(x_i^{-1})}{(1-x_iX)^{s-b}} \\ &= \sum_{i=1}^{n} \eta_i \bar{V}_{b,t}(x_i^{-1}) \sum_{j=0}^{\infty} \binom{s-b-1+j}{j} x_i^j X^j \\ &= \sum_{j=0}^{\infty} \binom{s-b-1+j}{j} \left(\sum_{i=1}^{n} \eta_i \bar{V}_{b,t}(x_i^{-1}) x_i^j \right) X^j \\ &= \sum_{j=0}^{\infty} \binom{s-b-1+j}{j} \left(\sum_{i=1}^{n} \eta_i y_i^{t-b} x_i^j \right) X^j \\ &= \sum_{j=0}^{\infty} S_j^{b,t} X^j, \end{aligned}$$

which corresponds to the "syndrome polynomials" of Ruckenstein's thesis [6].

VIII. Substituting Backwards

With the previous statements we can subdivide the algorithm solving the interpolation step of the Guruswami-Sudan principle in two stages.
First, the reduced system, consisting of the equations $\mathrm{EKE}(b_0+1),\ldots,\mathrm{EKE}(s-1)$ with the polynomials $\Lambda_{b_0+1}(X),\ldots,\Lambda_l(X)$, is solved (see Section IX). In the second step the missing polynomials $\Lambda_i(X)\ \forall\ i \leq b_0$ can be iteratively calculated. For instance suppose that $\Lambda_{b+1}(X),\ldots,\Lambda_l(X)$ are known (with $b \leq b_0$). Then one can use Equation (19) to get $B_b(X)$:

$$\sum_{t=b+1}^{l} \Lambda_t(X)\binom{t}{b} X^{(l-t)(n-k)} S^{b,t}(X) \equiv \bar{B}_b(X) \mod X^{(l-b)(n-k)}. \quad (23)$$

Then, to get $\Lambda_b(X)$, Equation (14) is rewritten:

$$\Lambda_b(X)X^{(l-b)(n-k)} = -\sum_{t=b+1}^{l} \Lambda_t(X)\binom{t}{b} X^{(l-t)(n-k)} \bar{R}(X)^{t-b} + \bar{B}_b(X)\bar{G}(X)^{s-b}, \quad (24)$$

which means that the coefficient of $\Lambda_b(X)$ are read on the N_b highest terms of the RHS of (24). These "substitutions" only involve polynomial multiplications.

IX. Solving the Reduced System

In this section we have a closer look at the reduced system:

$$\begin{pmatrix} \mathbf{S}^{b_0+1,b_0+1} & \ldots & \mathbf{S}^{b_0+1,l} \\ \vdots & \ddots & \vdots \\ \mathbf{S}^{s-1,b_0+1} & \ldots & \mathbf{S}^{s-1,l} \end{pmatrix} \begin{pmatrix} \mathbf{\Lambda}_{b_0+1} \\ \vdots \\ \mathbf{\Lambda}_l \end{pmatrix} = 0, \quad (25)$$

where each matrix $\mathbf{S}^{b,j}$ has $(s-b)n$ and N_j columns. The gain can be expressed by the number of equations. The linear system (25) consist of

$$\begin{aligned} N &= \sum_{b=b_0+1}^{s-1} (s-b)n \\ &\approx \frac{n}{2}(s-b_0)^2 \\ &\approx \frac{ns^2}{2}\left(1-\frac{\tau}{d}\right)^2 \end{aligned}$$

equations.
Assuming that one wants to reach the maximum radius, i.e. $\tau = (1-\sqrt{R})n$ and with $d=(1-R)n$, we can express the number of equations in terms of the rate:

$$N = \frac{ns^2}{2}\left(1-\frac{1-\sqrt{R}}{1-R}\right)^2. \quad (26)$$

In Fig. 2 the factor $\alpha(R)$, where $N = \frac{ns^2}{2}\cdot\alpha(R)$, is illustrated.

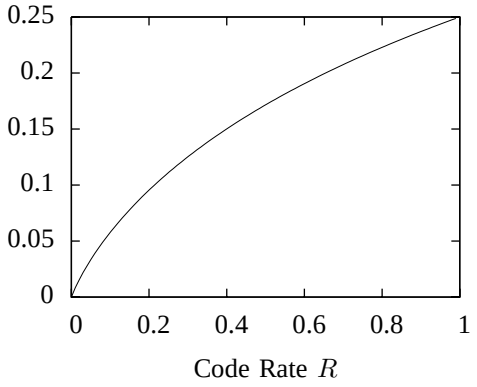

Fig. 2. The factor α in dependence of the code rate R.

It was hinted in the PHD thesis of Ruckenstein [6] that the matrix in Figure 1 has a structure of a block Hankel matrix

$$\begin{pmatrix} \mathrm{sn}\left\{\begin{bmatrix} S_{1,0}^{0,0} & \cdots & S_{1,N_0-1}^{0,0} \\ S_{2,0}^{0,0} & \cdots & S_{2,N_0-1}^{0,0} \\ \vdots & & \\ S_{sn,0}^{0,0} & \cdots & S_{sn,N_0-1}^{0,0} \end{bmatrix}\right. & \mathbf{S}^{0,1} & & & \cdots & \mathbf{S}^{0,l} \\ \mathbf{0} & \text{(s-1)n}\left\{\begin{bmatrix} S_{1,0}^{1,1} & \cdots & S_{1,N_1-1}^{1,1} \\ S_{2,0}^{1,1} & \cdots & S_{2,N_1-1}^{1,1} \\ \vdots & & \\ S_{(s-1)n,0}^{1,1} & \cdots & S_{(s-1)n,N_1-1}^{1,1} \end{bmatrix}\right. & \mathbf{S}^{1,2} & \mathbf{S}^{1,3} & \cdots & \mathbf{S}^{1,l} \\ \vdots & & \ddots & & & \vdots \\ \mathbf{0} & \cdots & \mathbf{0} & \text{(s-}b_0\text{)n}\{\mathbf{S}^{b_0,b_0} & \cdots & \mathbf{S}^{b_0,l} \\ \vdots & & & \ddots & & \vdots \\ \mathbf{0} & \cdots & \mathbf{0} & \text{n}\{\mathbf{S}^{s-1,s-1} & \cdots & \mathbf{S}^{s-1,l} \end{pmatrix}$$

Fig. 1. The standard matrix for determining the bivariate interpolation polynomials $Q(X,Y)$ of the Guruswami-Sudan algorithm

and can be solved with a quadratic complexity in terms of its number of rows, either with the FIA [9], [4] or with an adaptation of the Sakata's algorithm [10], [11]. As mentioned in Section II and explained in [6] a block Hankel linear system can be solved using a variant of the Fundamental Iterative Algorithm tailored for structured matrices. The main idea is to preprocess the matrix, by interleaving properly the rows and the columns. This is a combination of the idea in [2] which deals with the case where only one horizontal block of Hankel matrices is regarded and of the idea of [12], [13] dealing with one vertical band of Hankel matrices.

X. Conclusion

We have generalized Roth and Ruckenstein's approach of the Sudan decoding algorithm of Reed-Solomon codes, with multiplicity $s = 1$, to the general case of the Guruswami-Sudan algorithm, with higher multiplicities. While Roth and Ruckenstein have obtained one single key equation, which is the generalization of the classical key equation for RS codes, we obtained s key equations (one for each order of multiplicity). Although this is quite satisfactory from the mathematical point of view, we also gain in terms of the number of equations that indeed have to be solved, while the other can be solved by simple polynomial multiplications. If the code rate approaches zero, the gain in terms of the number of equations that truly need to be solved is very high.

References

[1] 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

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

[3] G.-L. Feng and K. K. Tzeng, "A generalization of the Berlekamp-Massey algorithm for multisequence shift-register synthesis with applications to decoding cyclic codes," *IEEE Transactions on Information Theory*, vol. 37, no. 5, pp. 1274–1287, 1991. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=133246

[4] G. L. Feng and K. K. Tzeng, "An iterative algorithm of shift-register synthesis for multiple sequences," *Scientia Sinica (Science in China) Series A*, vol. 28, pp. 1222–1232, November 1985.

[5] 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

[6] 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

[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] Joachim and J. Gerhard, *Modern Computer Algebra*. Cambridge University Press, July 2003. [Online]. Available: http://www.amazon.ca/exec/obidos/redirect?tag=citeulike09-20&path=ASIN/0521826462

[9] G.-L. Feng and K. K. Tzeng, "A new procedure for decoding cyclic and bch codes up to actual minimum distance," *IEEE Transactions on Information Theory*, vol. 40, no. 5, pp. 1364–1374, 1994. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=333854

[10] S. Sakata, "n-dimensional Berlekamp-Massey algorithm for multiple arrays and construction of multivariate polynomials with preassigned zeros," in *Applied algebra, algebraic algorithms and error-correcting codes (Rome, 1988)*, ser. Lecture Notes in Computer Science, T. Mora, Ed., vol. 357. Berlin: Springer, 1989, pp. 356–376. [Online]. Available: http://www.ams.org/mathscinet-getitem?mr=1008512

[11] ——, "Extension of the Berlekamp-Massey algorithm to n dimensions," *Inf. Comput.*, vol. 84, no. 2, pp. 207–239, February 1990. [Online]. Available: http://portal.acm.org/citation.cfm?id=81252

[12] G. Schmidt and V. R. Sidorenko, "Linear Shift-Register Synthesis for Multiple Sequences of Varying Length," May 2006. [Online]. Available: http://arxiv.org/abs/cs/0605044

[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