

# Efficient Interpolation in the Guruswami-Sudan Algorithm

Peter V. Trifonov, *Member, IEEE*

**Abstract**—A novel algorithm is proposed for the interpolation step of the Guruswami-Sudan list decoding algorithm. The proposed method is based on the binary exponentiation algorithm, and can be considered as an extension of the Lee-O’Sullivan method. The algorithm is shown to achieve both asymptotical and practical performance gain compared to the case of iterative interpolation algorithm. Further complexity reduction is achieved by employing the re-encoding transformation. The key contribution of the paper, which enables the complexity reduction, is a novel randomized ideal multiplication algorithm.

**Index Terms**—Gröbner basis, Guruswami-Sudan algorithm, ideal multiplication, interpolation, list decoding, re-encoding, Reed-Solomon codes.

## I. INTRODUCTION

The Guruswami-Sudan list decoding algorithm [1] is one of the most powerful decoding methods for Reed-Solomon codes. Its complexity is known to be polynomial. However, the degree of the polynomial turns out to be too high. Therefore, computationally efficient algorithms are needed in order to obtain a practical implementation of this method.

The most computationally intensive step of the Guruswami-Sudan algorithm is construction of a bivariate polynomial passing through a number of points with a given multiplicity. In this paper a novel reduced complexity interpolation algorithm is presented. It is based on the well-known binary exponentiation method, so we call it binary interpolation algorithm. The algorithm exploits the relationship between the Gröbner bases of zero-dimensional ideals and appropriate modules. The key component of the proposed method is a novel fast randomized ideal multiplication algorithm (see Figure 3). We show also that the interpolation complexity can be further reduced by employing the re-encoding transformation [2], [3].

The paper is organized as follows. Section III presents a simple derivation of the Guruswami-Sudan algorithm and all necessary background. Section IV introduces the novel interpolation algorithm. Numeric performance results are given in Section V. Finally, some conclusions are drawn.

## II. NOTATION

- $\langle Q_i(x, y), 0 \leq i \leq v \rangle = \left\{ \sum_{i=0}^v p_i(x, y) Q_i(x, y) \mid p_i(x, y) \in \mathbb{F}[x, y] \right\}$  is the ideal generated by  $Q_i(x, y)$ .
- $[Q_i(x, y), 0 \leq i \leq v] = \left\{ \sum_{i=0}^v p_i(x) Q_i(x, y) \mid p_i(x) \in \mathbb{F}[x] \right\}$  is the module generated by  $Q_i(x, y)$ .

P.V. Trifonov is with the Distributed Computing and Networking Department, Saint-Petersburg State Polytechnic University, Russia. e-mail:petert@dcn.ftk.spbstu.ru

- $Q^{[j_1, j_2]}(x_i, y_i) = \sum_{j'_1 \geq j_1} \sum_{j'_2 \geq j_2} \binom{j'_1}{j_1} \binom{j'_2}{j_2} q_{j'_1 j'_2} x_i^{j'_1 - j_1} y_i^{j'_2 - j_2}$  is the Hasse derivative of  $Q(x, y)$  at point  $(x_i, y_i)$ .
- $Q(x_i, y_i) = 0^r$  means that  $Q(x, y)$  has a root of multiplicity at least  $r$  in  $(x_i, y_i)$ , i.e.  $Q^{[j_1, j_2]}(x_i, y_i) = 0, j_1 + j_2 < r$ .
- $I_r = \{Q(x, y) \in \mathbb{F}[x, y] \mid Q(x_i, y_i) = 0^r, 1 \leq i \leq n\}$  is the ideal of polynomials having roots of multiplicity at least  $r$  at points  $(x_i, y_i), 1 \leq i \leq n$ .
- $M_{r, \rho} = \{Q(x, y) \in I_r \mid \text{wdeg}_{(0,1)} Q(x, y) < \rho\}$ .
- $\text{LT } Q(x, y)$  is the leading term of  $Q(x, y)$  with respect to some term ordering.
- $\text{ydeg } Q(x, y) = j$  iff  $\text{LT } Q(x, y) = ax^q y^j$  for some  $a \in \mathbb{F}$  and  $q \in \mathbb{Z}$ .
- $|\mathcal{B}|$  is the dimension of vector  $\mathcal{B}$ .
- $\Delta(\mathcal{B}) = \sum_{j=0}^s b_j$ , where  $\mathcal{B} = (B_0(x, y), \dots, B_s(x, y))$  is a Gröbner basis of some module, and  $\text{LT } B_j(x, y) = a_j x^{b_j} y^j$ .

## III. PRELIMINARIES

This section introduces some background information on the Guruswami-Sudan list decoding method, associated computational algorithms, and various algebraic concepts used in this paper.

### A. Term orderings

Multivariate polynomials are extensively used in this paper, so one needs to introduce monomial orderings to deal with them.  $(a, b)$ -weighted degree of a monomial  $cx^i y^j$  equals  $ai + bj$ .  $(a, b)$ -weighted degree  $\text{wdeg}_{(a,b)} Q(x, y)$  of a polynomial  $Q(x, y)$  equals to the maximum of  $(a, b)$ -weighted degrees of its non-zero terms. Weighted degree can be used to define a term ordering.  $(a, b)$ -weighted degree lexicographic ordering is defined as  $cx^i y^j \prec dx^p y^q \Leftrightarrow (ai + bj < ap + bq) \vee (ai + bj = ap + bq) \wedge (cx^i y^j \prec_{\text{lex}} dx^p y^q)$ . Lexicographic ordering is defined as  $cx^i y^j \prec_{\text{lex}} dx^p y^q \Leftrightarrow (j < q) \vee (j = q) \wedge (i < p)$ . Leading term  $\text{LT } Q(x, y)$  of a polynomial  $Q(x, y) = \sum_{q_{ij} \neq 0} q_{ij} x^i y^j$  is given by  $\arg \max_{q_{ij} \neq 0} q_{ij} x^i y^j$ . Multivariate polynomials can be ordered according to their leading terms.

### B. Guruswami-Sudan algorithm

The Guruswami-Sudan algorithm addresses the problem of list decoding of  $(n, k, n - k + 1)$  Reed-Solomon code over field  $\mathbb{F}$ . That is, given a received vector  $(y_1, \dots, y_n)$ , it finds all message polynomials  $f(x)$ , such that  $\deg f(x) < k$  and  $f(x_i) = y_i$  for at least  $\tau$  distinct code locators  $x_i$  [1]. This is

ITERATIVEINTERPOLATION( $n, \{(x_i, y_i), 1 \leq i \leq n\}, r, \rho$ )

```

1  for  $i \leftarrow 0$  to  $\rho - 1$ 
2  do  $Q_i(x, y) \leftarrow y^i$ ;
3  for  $i \leftarrow 1$  to  $n$ 
4  do for  $\beta \leftarrow 0$  to  $r - 1$ 
5      do for  $\alpha \leftarrow 0$  to  $r - \beta - 1$ 
6          do  $\Delta_j \leftarrow Q_j^{[\alpha, \beta]}(x_i, y_i), 0 \leq j \leq \rho - 1$ 
7               $m \leftarrow \arg \min_{j: \Delta_j \neq 0} Q_j(x, y)$ 
8              for  $j \neq m$ 
9                  do  $Q_j(x, y) \leftarrow Q_j(x, y) - \frac{\Delta_j}{\Delta_m} Q_{j_0}(x, y)$ 
10                  $Q_m(x, y) \leftarrow Q_m(x, y)(x - x_i)$ ;
11  return  $(Q_0(x, y), \dots, Q_{\rho-1}(x, y))$ 
    
```

Fig. 1. Iterative interpolation algorithm (IIA)

accomplished by constructing a polynomial  $Q(x, y)$ , such that  $Q(x_i, y_i) = 0^r$ ,  $\text{wdeg}_{(1, k-1)} Q(x, y) \leq l$ ,  $\text{wdeg}_{(0, 1)} Q(x, y) < \rho$ , and factoring it.

It is possible to show that the parameters of this algorithm must satisfy [4]

$$\frac{\rho(\rho - 1)}{2} \leq \frac{nr(r + 1)}{2(k - 1)} < \frac{\rho(\rho + 1)}{2}, \quad (1)$$

$$l = \left\lfloor \frac{nr(r + 1)}{2\rho} + \frac{(\rho - 1)(k - 1)}{2} \right\rfloor, \quad (2)$$

$$\tau = \left\lfloor \frac{l}{r} \right\rfloor + 1 > \sqrt{n(k - 1)}. \quad (3)$$

### C. Interpolation

Construction of a polynomial  $Q(x, y)$  turns out to be the most computationally expensive step of the Guruswami-Sudan algorithm. This section presents an overview of two existing algorithms for the interpolation problem. The first one will be used to derive some important properties of the underlying algebraic structures, and the second will be used as a component of the proposed method.

Observe that the set of polynomials  $I_r = \{Q(x, y) \in \mathbb{F}[x, y] \mid Q(x_i, y_i) = 0^r, 1 \leq i \leq n\}$  is an ideal. The smallest non-zero polynomial of this ideal with respect to  $(1, k - 1)$ -weighted degree lexicographic ordering must satisfy the constraints of the Guruswami-Sudan algorithm. Such a polynomial is guaranteed to appear in the Gröbner basis of  $I_r$  with respect to this term ordering [5]. However, it turns out to be easier to construct a Gröbner basis of the module  $M_{r, \rho} = \{Q(x, y) \in I_r \mid \text{wdeg}_{(0, 1)} Q(x, y) < \rho\}$ .

1) *Iterative interpolation algorithm*: The algorithm shown in Figure 1 constructs  $\rho$  non-zero polynomials  $Q_j(x, y), 0 \leq j \leq \rho - 1$ , such that  $Q(x_i, y_i) = 0^r$ ,  $\text{LT } Q_j(x, y) = a_j x^{t_j} y^j$ , and  $t_j$  are the smallest possible integers [4], [6], [7]. These polynomials represent a Gröbner basis of the module  $M_{r, \rho} = \{Q(x, y) \in I_r \mid \text{wdeg}_{(0, 1)} Q(x, y) < \rho\}$  [8], [9]. In the context of list decoding one has to use the  $(1, k - 1)$ -weighted lexicographic ordering. The solution of the interpolation problem is given by the smallest polynomial in the obtained vector  $(Q_0(x, y), \dots, Q_{\rho-1}(x, y))$ . It can be seen that the complexity of IIA is given by  $O(n^2 r^4 \rho)$ .

It will be sometimes convenient to represent a vector of polynomials  $A_i(x, y) = \sum_{j=0}^t y^j a_{ji}(x), 0 \leq i \leq s$ , as

$$(1, y, \dots, y^t) \underbrace{\begin{pmatrix} a_{00}(x) & a_{01}(x) & \dots & a_{0s}(x) \\ a_{10}(x) & a_{11}(x) & \dots & a_{1s}(x) \\ \vdots & \vdots & \ddots & \vdots \\ a_{t0}(x) & a_{t1}(x) & \dots & a_{ts}(x) \end{pmatrix}}_{\mathcal{A}(x)}, \text{ where } \mathcal{A}(x)$$

is a  $(t + 1) \times (s + 1)$  polynomial matrix.

**Lemma 1.** Let  $\mathcal{Q} = (Q_0(x, y), \dots, Q_{\rho-1}(x, y))$  be a vector of polynomials constructed by IIA for the input  $(n, \{(x_i, y_i), 1 \leq i \leq n\}, r, \rho)$ . Then

$$\deg \det \mathcal{Q}(x) = \Delta(\mathcal{Q}) = n \frac{r(r + 1)}{2},$$

where  $\mathcal{Q}(x)$  is the corresponding polynomial matrix.

*Proof:* Observe that at each iteration of IIA the  $x$ -degree of exactly one polynomial is increased by one. Hence, the sum of leading term  $x$ -degrees of all polynomials after algorithm termination is equal to the number of partial Hasse derivatives forced to be zero. On the other hand, this algorithm can be interpreted as construction of the polynomial matrix

$$\mathcal{Q}(x) = \prod_{i=1}^n \prod_{\alpha + \beta < r} \delta^{(i, \alpha, \beta)}, \quad (4)$$

where

$$\delta^{(i, \alpha, \beta)} = \begin{pmatrix} 1 & 0 & \dots & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ -\frac{\Delta_0}{\Delta_m} & -\frac{\Delta_1}{\Delta_m} & \dots & x - x_i & \dots & -\frac{\Delta_{\rho-1}}{\Delta_m} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & \dots & 1 \end{pmatrix},$$

and  $m = m(i, \alpha, \beta)$  is the index of the smallest polynomial selected on line 7 of the algorithm. Obviously,  $\det \delta^{(i, \alpha, \beta)} = \gamma_{i, \alpha, \beta} (x - x_i)$  for some non-zero  $\gamma_{i, \alpha, \beta}$ , and the number of terms in (4) is again equal to the number of Hasse derivatives forced to be zero. ■

Observe that for a fixed term ordering there may exist many different Gröbner bases of a module. However, they share the following common property.

**Lemma 2.** Let  $\mathcal{B} = (B_0(x, y), \dots, B_{\rho-1}(x, y))$  be a Gröbner basis of the module  $M_{r, \rho}$ . Then  $\Delta(\mathcal{B}) = \frac{nr(r+1)}{2}$ .

*Proof:* Let  $Q_j(x, y), 0 \leq j \leq \rho - 1$  be the Gröbner basis of  $M_{r, \rho}$  constructed by IIA for the same term ordering. Then  $\text{LT } Q_j(x, y) \mid \text{LT } B_j(x, y)$  and  $\text{LT } B_j(x, y) \mid \text{LT } Q_j(x, y)$ . This means that the leading terms of  $B_j(x, y)$  and  $Q_j(x, y)$  are the same up to some constants in  $\mathbb{F}$ , and the statement follows from Lemma 1. ■

2) *Transformation of the module basis*: It was shown in [10], [11], [12], [13] that the ideal of interpolation polynomials  $I_r$  is generated by

$$\Pi_{r, j}(x, y) = (y - T(x))^j \phi^{r-j}(x), 0 \leq j \leq r, \quad (5)$$

where  $T(x_i) = y_i, 1 \leq i \leq n$ , and  $\phi(x) = \prod_{i=1}^n (x - x_i)$ . Hence, the basis of the module  $M_{r, \rho}$  is given by  $\mathcal{L} =$

```

REDUCE((S0(x, y), . . . , Si-1(x, y)), P(x, y))
1  Si(x, y) ← P(x, y)
2  while ∃j : (0 ≤ j < i) ∧ (ydeg Sj(x, y) = ydeg Si(x, y))
3  do if LT Si(x, y) | LT Sj(x, y)
4      then W(x, y) ← Sj(x, y) -  $\frac{\text{LT } S_j(x, y)}{\text{LT } S_i(x, y)} S_i(x, y)$ 
5           Sj(x, y) ← Si(x, y)
6           Si(x, y) ← W(x, y)
7      else Si(x, y) ← Si(x, y) -  $\frac{\text{LT } S_i(x, y)}{\text{LT } S_j(x, y)} S_j(x, y)$ 
8  if Si(x, y) = 0
9      then i ← i - 1
10 return (S0(x, y), . . . , Si(x, y))
    
```

Fig. 2. Multi-dimensional Euclidean algorithm

$(\Pi_{r,0}(x, y), \dots, \Pi_{r,r}(x, y), \Pi_{r,r+1}(x, y), \dots, \Pi_{r,\rho-1}(x, y))$ ,  
 where

$$\Pi_{r,r+j}(x, y) = y^j \Pi_{r,r}(x, y), 0 < j < \rho - r. \quad (6)$$

**Lemma 3.** *The polynomials  $(S_0(x, y), \dots, S_{s-1}(x, y))$  represent a Gröbner basis of the module  $M = \{\sum_{j=0}^{s-1} S_j(x, y) a_j(x) \mid a_j(x) \in \mathbb{F}[x]\}$  if  $\text{ydeg } S_i(x, y), 0 \leq i \leq s-1$ , are distinct values.*

*Proof:* The lemma follows from the Buchberger S-pair criterion [14]. ■

The above described basis  $\mathcal{L}$  has to be transformed into a Gröbner one with respect to  $(1, k-1)$ -weighted degree lexicographic monomial ordering. This can be done with the algorithm given in [11], [12], which can be considered as a simplified instance of the Buchberger algorithm. It is convenient to present it here in a slightly modified form. Namely, this algorithm takes as input some polynomial  $P(x, y)$ , a Gröbner basis  $(S_0(x, y), \dots, S_{i-1}(x, y))$  of some module  $M \subset \mathbb{F}[x, y]$ , and constructs a Gröbner basis of the module  $M' = \{Q(x, y) + a(x)P(x, y) \mid Q(x, y) \in M, a(x) \in \mathbb{F}[x]\}$ . The algorithm is shown in Figure 2.

**Lemma 4.** *Let  $S_j(x, y), 0 \leq j \leq i-1$ , be the polynomials such that  $\text{LT } S_j(x, y) = \alpha_j x^{s_j} y^j$ ,  $\text{wdeg}_{(0,1)} S_j(x, y) < i$ . Then the Reduce algorithm constructs a Gröbner basis of the module  $M = [S_0(x, y), \dots, S_{i-1}(x, y), P(x, y)]$ .*

*Proof:* This statement follows from Lemma 3 and invertibility of transformations used by the algorithm. ■

The required Gröbner basis is obtained as  $\mathcal{S}_{\rho-1}$ , where

$$S_j = \text{Reduce}(S_{j-1}, \Pi_{r,j}(x, y)), S_0 = (\Pi_{r,0}(x, y)). \quad (7)$$

The complexity of this method is given by  $O(n^4 k^{-2, \rho^5})$  [12]. Curiously, if  $(1, k-1)$ -weighted degree lexicographic ordering is used and  $r = 1, \rho = 2$ , it reduces to the Gao decoding method [15], [16], with function *Reduce* being the standard extended Euclidean algorithm with early termination condition. Therefore, *Reduce* will be referred to as the multi-dimensional Euclidean algorithm.

#### IV. BINARY INTERPOLATION ALGORITHM

This section introduces a novel interpolation algorithm. The main idea of this algorithm is to construct a sequence of ideals

and modules of polynomials having roots  $(x_i, y_i)$  with increasing multiplicity. The proposed method can be considered as an application of the well-known binary exponentiation algorithm to zero-dimensional ideals.

##### A. Interpolation via ideal multiplication

The main drawback of the method given by (7) is that one has to manipulate with the polynomials having large common divisors. For example,  $S_1 = \text{Reduce}((\phi^r(x)), \phi^{r-1}(x)(y - T(x))) = \phi^{r-1}(x) \text{Reduce}((\phi(x)), y - T(x))$ .

Furthermore, polynomial exponentiation is used in (5). The method proposed in this paper avoids both reducing the polynomials with large GCD, and computing large powers of polynomials. This is achieved by first constructing Gröbner bases for small root multiplicities, and using them to obtain bases for larger root multiplicities.

**Lemma 5.** *Let  $I_r = \{Q(x, y) \in \mathbb{F}[x, y] \mid Q(x_i, y_i) = 0^r, 1 \leq i \leq n\}$ . Then  $I_{r_1+r_2} = I_{r_1} \cdot I_{r_2}$ .*

*Proof:*  $I_{r_1+r_2} = \langle (y - T(x))^j \phi^{r_1+r_2-j}(x), 0 \leq j \leq r_1 + r_2 \rangle = \langle (y - T(x))^{j_1+j_2} \phi^{r_1-j_1+r_2-j_2}(x), j_1 = 0, \dots, r_1, j_2 = 0, \dots, r_2 \rangle = \langle (y - T(x))^{j_1} \phi^{r_1-j_1}(x), j_1 = 0, \dots, r_1 \rangle \cdot \langle (y - T(x))^{j_2} \phi^{r_2-j_2}(x), j_2 = 0, \dots, r_2 \rangle = I_{r_1} \cdot I_{r_2}$ . ■

This lemma implies that  $I_r = \underbrace{I_1 \cdot I_1 \cdots I_1}_{r \text{ times}} = I_1^r$ . One can

avoid repeated calculations and reduce the overall number of calls to the *Reduce* algorithm by using the binary exponentiation method [17]. Namely, one can compute

$$I_r = I_1^r = (\dots ((I_1^2 \cdot I_1^{r-m-1})^2 \cdot I_1^{r-m-2})^2 \cdot I_1^{r-m-3} \dots I_1^1)^2 \cdot I_1^0$$

where  $r = \sum_{j=0}^m r_j 2^j, r_m = 1, I^2 = I \cdot I, I^0 = \mathbb{F}[x, y]$ , and  $I \cdot \mathbb{F}[x, y] = I$ .

The key problem addressed in this paper is how to construct efficiently a Gröbner basis of the product of ideals  $I' = \langle P_0(x, y), \dots, P_u(x, y) \rangle$  and  $I'' = \langle S_0(x, y), \dots, S_v(x, y) \rangle$ . The standard way is given by

$$I' \cdot I'' = \langle P_i(x, y) S_j(x, y), 0 \leq i \leq u, 0 \leq j \leq v \rangle, \quad (8)$$

i.e. to compute pairwise products of all basis elements of the ideals being multiplied. This requires  $(u+1)(v+1)$  bivariate polynomial multiplications, and the basis of  $I' \cdot I''$  obtained in such way is extremely redundant. Furthermore, Buchberger algorithm must be used in order to obtain a Gröbner basis of  $I' \cdot I''$ .

To the best of author's knowledge, the problem of efficient ideal multiplication was not considered in the literature, except in [9], where multiplication of zero-dimensional co-prime ideals was reduced to linear convolution. However, the ideals considered in this paper are not co-prime.

This problem can be again solved by constructing at each step of the binary exponentiation algorithm a basis of the module of polynomials with limited  $(0, 1)$ -weighted degree.

**Lemma 6.** *Consider the polynomials  $P_j(x, y) : P_j(x_i, y_i) = 0^s, 1 \leq i \leq n, 0 \leq j \leq m$ , such that  $\text{LT } P_j(x, y) = a_j x^{p_j} y^j$ ,  $\text{wdeg}_{(0,1)} P_j(x, y) \leq m, p_m = 0$ , and*

$$\Delta((P_0(x, y), \dots, P_m(x, y))) = \frac{ns(s+1)}{2}. \quad (9)$$

Then  $I_s = \langle P_j(x, y), 0 \leq j \leq m \rangle$ , and the polynomials  $P_j(x, y)$  constitute a Gröbner basis of this ideal.

*Proof:* Observe that the polynomials  $P_j(x, y)$  represent a Gröbner basis of some module by lemma 3. Obviously,  $\langle P_j(x, y), 0 \leq j \leq m \rangle \subset I_s$ . Suppose that the polynomials  $P_j(x, y)$  do not constitute a Gröbner basis of  $I_s$ . That is, there exists  $S(x, y) \in I_s : S(x, y) = \sum_{j=0}^m q_j(x, y)P_j(x, y) + R(x, y)$ , where the terms of  $R(x, y)$  are not divisible by  $\text{LT } P_j(x, y)$ , i.e.  $\text{wdeg}_{(0,1)} R(x, y) < m$  and  $\text{LT } R(x, y) = \beta x^u y^v, u < p_v$ . Observe that  $R(x, y) \in M_{s,m}$ . This means that the polynomials  $P_j(x, y), 0 \leq j \leq m-1$ , do not represent a Gröbner basis of module  $M_{s,m}$ . The true Gröbner basis of this module should consist of smaller polynomials, i.e. the sum of  $x$ -degrees of their leading terms should be less than  $\frac{ns(s+1)}{2}$ . But this contradicts to Lemma 2. Hence,  $R(x, y) = 0$  and  $P_j(x, y)$  constitute a Gröbner basis of  $I_s$ . ■

Observe that there may exist Gröbner bases of  $I_s$  not satisfying the constraints of this lemma.

Let  $I_{r_1} = \langle P_j(x, y), 0 \leq j \leq u \rangle, I_{r_2} = \langle S_i(x, y), 0 \leq i \leq v \rangle$  be the ideals given by their Gröbner bases satisfying the above lemma. One can construct a Gröbner basis of the product  $I_{r_1+r_2}$  of these ideals as follows. Let  $(m'_j, m''_j), 0 \leq j \leq (u+1)(v+1) - 1$  be a sequence of distinct pairs of integers such that  $0 \leq m'_j \leq u, 0 \leq m''_j \leq v$ , and  $\text{LT} \left( P_{m'_j}(x, y) S_{m''_j}(x, y) \right) = \alpha_j x^{q_j} y^j$  for  $j \leq u+v$ . Let

$$\mathcal{Q}_{u+v} = (P_{m'_j}(x, y) S_{m''_j}(x, y), 0 \leq j \leq u+v) \quad (10)$$

be a basis of some submodule of  $M_{r_1+r_2, u+v+1}$ . By Lemma 3, it is a Gröbner basis of this submodule. It can be seen that  $\Delta(\mathcal{Q}_{u+v}) = \sum_{j=0}^{u+v} q_j \geq \frac{n(r_1+r_2)(r_1+r_2+1)}{2}$ .

Let

$$\mathcal{Q}_j = \text{Reduce}(\mathcal{Q}_{j-1}, P_{m'_j} S_{m''_j}), j > u+v. \quad (11)$$

The *Reduce* algorithm attempts to cancel the leading terms of the provided polynomials, so  $\Delta(\mathcal{Q}_{j+1}) \leq \Delta(\mathcal{Q}_j)$ . As soon as one obtains  $\Delta(\mathcal{Q}_j) = \frac{n(r_1+r_2)(r_1+r_2+1)}{2}$ ,  $\mathcal{Q}_j$  is a Gröbner basis of  $I_{r_1+r_2}$ .

**Lemma 7.**  $M_{r_1+r_2, u+v+1}$  is generated by  $\mathcal{Q}_{(u+1)(v+1)-1}$ .

*Proof:* Consider  $Q(x, y) \in I_{r_1+r_2}$ , such that  $\text{wdeg}_{(0,1)} Q(x, y) \leq u+v$ . Any such polynomial can be represented as

$$Q(x, y) = \sum_{j=0}^u P_j(x, y) \sum_{i=0}^v q_{ji}(x, y) S_i(x, y). \quad (12)$$

Inner sum is an element of  $I_{r_2}$ . Since the polynomials  $S_i(x, y), 0 \leq i \leq v$ , are a Gröbner basis of  $M_{r_2, v+1}$  and  $I_{r_2}$ , one can use the multivariate polynomial division algorithm to obtain  $Q(x, y) = \sum_{j=0}^u P_j(x, y) \left( \sum_{i=0}^{v-1} w_{ji}(x) S_i(x, y) + S_v(x, y) \sum_{i \geq v} y^{i-v} \tilde{w}_{ji}(x) \right)$ .

Similarly,  $P(x, y) = \sum_{j=0}^u P_j(x, y) \sum_{i \geq v} y^{i-v} \tilde{w}_{ji}(x)$  is in  $I_{r_1}$ , and the multivariate division algorithm leads to

$$P(x, y) = \sum_{j=0}^u w_{jv}(x) P_j(x, y) + P_u(x, y) \sum_{j>u} y^{j-u} w_{jv}(x).$$

Hence,  $Q(x, y) = \sum_{j=0}^u \sum_{i=0}^v P_j(x, y) S_i(x, y) w_{ji}(x) + P_u(x, y) S_v(x, y) y \bar{w}(x, y)$ . Last term in this expression is zero, since  $Q(x, y)$  does not contain any monomials  $ax^p y^q$  with  $q > u+v$ , so  $M_{r_1+r_2, u+v+1} = [P_j(x, y) S_i(x, y), 0 \leq j \leq u, 0 \leq i \leq v]$ . ■

The lemma states that for any suitable polynomial  $Q(x, y) \in I_{r_1} I_{r_2}$  one can replace the bivariate polynomials  $q_{ji}(x, y)$  in (12) with univariate ones  $w_{ji}(x)$ . This implies that the sequence  $\mathcal{Q}_j$  converges eventually to the required module basis. However, the convergence turns out to be quite slow. One may need to compute many bivariate polynomial products  $P_{m'_j} S_{m''_j}$  and apply the *Reduce* algorithm to them before the constraint (9) is satisfied. In many cases it appears even that  $\mathcal{Q}_{j+1} = \mathcal{Q}_j$ . That is, a significant fraction of pairs  $(m'_j, m''_j)$  is useless.

Therefore we propose to replace pairwise products  $P_j(x, y) S_i(x, y)$  in (8) with their random linear combinations

$$Q_s(x, y) = \sum_{j=0}^u \sum_{i=0}^v \chi_{sji} P_j(x, y) S_i(x, y), \quad (13)$$

where  $\chi_{sji}$  are independent random variables uniformly distributed over  $\mathbb{F}$ . Obviously, such polynomials still generate the ideal product if the linear transformation given by  $\chi_{sji}$  is invertible, i.e. if at least  $(u+1)(v+1)$  polynomials  $Q_s(x, y)$  are given. However, it turns out that in average one needs just a few such polynomials to obtain a basis of the ideal product. The reason is that  $Q_s(x, y)$  depend on all pairwise products  $P_j(x, y) S_i(x, y)$ , and a Gröbner basis construction algorithm (e.g. *Reduce*) can take them into account simultaneously. This will be discussed in more details in Section IV-B.

However, it is impractical to construct the polynomials explicitly as given by (13), since this requires one first to compute all pairwise products  $P_j(x, y) S_i(x, y)$ . More efficient way is to construct a sequence of bases

$$\mathcal{Q}'_{j+1} = \text{Reduce} \left( \mathcal{Q}'_j, \left( \sum_{i=0}^u \alpha_{ij} P_i(x, y) \right) \left( \sum_{i=0}^v \beta_{ij} S_i(x, y) \right) \right),$$

where  $j \geq u+v$ , and  $\alpha_{ij}, \beta_{ij}$  are some random values uniformly distributed over  $\mathbb{F}$ . Furthermore, we propose to construct the initial basis  $\mathcal{Q}'_{u+v} = (Q_0(x, y), \dots, Q_{u+v}(x, y))$  as  $Q_i(x, y) = P_{i-j}(x, y) S_j(x, y)$ , where for each  $i, j$  is selected so that  $\text{LT } Q_i(x, y) = a_i x^{q_i} y^i$ , and the values  $q_i, 0 \leq i \leq u+v$  are minimized. This reduces the number of iterations needed by the *Reduce* algorithm. The proposed approach is summarized in Figure 3.

**Theorem 1.** Given Gröbner bases  $\mathcal{P} = (P_0(x, y), \dots, P_u(x, y))$  and  $\mathcal{S} = (S_0(x, y), \dots, S_v(x, y))$  of ideals  $I_{r_1}$  and  $I_{r_2}$ , the result of *Merge*( $\mathcal{P}, \mathcal{S}, n^{\frac{r(r+1)}{2}}$ ) is a Gröbner basis of  $I_r$ , where  $r = r_1 + r_2$ .

*Proof:* Observe that the sequence  $\mathcal{Q}'_j$  still converges to a basis of  $M_{r_1+r_2, u+v+1}$ , since it is possible to select  $\alpha_{ij}$  and  $\beta_{ij}$  so that the linear transformation (13) given

```

MERGE(( $P_0(x, y), \dots, P_u(x, y)$ ), ( $S_0(x, y), \dots, S_v(x, y)$ ),  $\Delta_0$ )
1  for  $i \leftarrow 0$  to  $u + v$ 
2  do  $Q_i(x, y) = \min_{0 \leq j \leq v} P_{i-j}(x, y)S_j(x, y)$ 
3   $\mathcal{Q} = (Q_0(x, y), \dots, Q_{u+v}(x, y))$ 
4  while  $\Delta(\mathcal{Q}) > \Delta_0$ 
5  do  $\alpha_i \leftarrow \text{rand}(), 0 \leq i \leq u$ 
6      $\beta_j \leftarrow \text{rand}(), 0 \leq j \leq v$ 
7      $Q(x, y) \leftarrow (\sum_{i=0}^u \alpha_i P_i(x, y)) (\sum_{i=0}^v \beta_i S_i(x, y))$ 
8      $\mathcal{Q} \leftarrow \text{REDUCE}(\mathcal{Q}, Q(x, y))$ 
9  return  $\mathcal{Q}$ 

```

Fig. 3. Construction of a Gröbner basis of  $I = JK$  from the Gröbner bases of  $J = \langle P_0(x, y), \dots, P_u(x, y) \rangle$  and  $K = \langle S_0(x, y), \dots, S_v(x, y) \rangle$ .

```

INTERPOLATE((( $x_i, y_i$ ),  $1 \leq i \leq n$ ),  $r$ )
1   $\phi(x) \leftarrow \prod_{i=1}^n (x - x_i)$ 
2   $T(x) \leftarrow \sum_{i=1}^n y_i \prod_{j \neq i} \frac{x - x_j}{x_i - x_j}$ 
3   $\mathcal{G} \leftarrow (\phi(x))$ 
4   $j \leftarrow 0$ 
5  repeat
6      $\mathcal{G} \leftarrow \text{REDUCE}(\mathcal{G}, y^j(y - T(x)))$ 
7      $j \leftarrow j + 1$ 
8  until  $\text{LT } G_j(x, y) = y^j$ 
9   $\mathcal{B} \leftarrow \mathcal{G}$ 
10  $r = \sum_{j=0}^m r_j 2^j, r_j \in \{0, 1\}$ 
11  $R \leftarrow 1$ 
12 for  $j \leftarrow m - 1$  to 0
13 do  $R \leftarrow 2R$ 
14  $\mathcal{B} \leftarrow \text{MERGE}(\mathcal{B}, \mathcal{B}, nR(R + 1)/2)$ 
15 if  $r_j = 1$ 
16 then  $R \leftarrow R + 1$ 
17  $\mathcal{B} \leftarrow \text{MERGE}(\mathcal{B}, \mathcal{G}, nR(R + 1)/2)$ 
18 return  $\mathcal{B}$ 

```

Fig. 4. Construction of a Gröbner basis for  $I_r$ .

by  $\chi_{sij} = \alpha_{is}\beta_{js}$  is invertible, provided that sufficiently many polynomials are constructed. By lemma 4, the *Reduce* algorithm always produces a Gröbner basis of some module. By lemma 6, this basis is a Gröbner basis of  $I_r$ . ■

*Remark 1.* *Merge* is not guaranteed to obtain a minimal Gröbner basis of  $I_r$ . In particular, a few polynomials may have  $\text{LT } Q_j(x, y) = y^j$ . Such polynomials are redundant, and should be eliminated, except the smallest one.

The overall interpolation algorithm is shown in Figure 4.  $(1, k - 1)$ -weighted degree lexicographic ordering must be used throughout this algorithm. Observe that in most practical cases the polynomial  $T(x)$  can be constructed by using fast inverse discrete Fourier transform. FFT can be also used in the implementation of polynomial multiplication, which is extensively used by this algorithm.

**Theorem 2.** *Interpolate algorithm constructs a Gröbner basis of  $I_r$  with respect to a given term ordering.*

*Proof:* The objective of the *REPEAT* loop is to construct a Gröbner basis of  $M_{1, j+1}$ , such that it is also a Gröbner

basis of  $I_1$ . Any Gröbner basis of a zero-dimensional ideal must contain a polynomial  $G_j(x, y) : \text{LT } G_j(x, y) = ay^j$  for some  $a \in \mathbb{F}, j \in \mathbb{N}$  [14, Th. 6.54], so this loop terminates eventually, and  $\mathcal{G}$  is indeed a Gröbner basis of  $I_1$ .

Let  $r' = \sum_{i=j+1}^m r_i 2^{i-j-1}$ . By induction, the input vectors to *Merge* at line 14 are two copies of a Gröbner basis of  $I_{r'}$ . By Theorem 1 its output is a Gröbner basis of  $I_{2r'}$ . Similar argument applies to line 17. Hence, at the end of each iteration of the *FOR* loop one obtains a Gröbner basis of  $I_{2r'+r_j}$ . Observe also, that at the end of each iteration  $R = 2r' + r_j$ . ■

The interpolation polynomial needed by the Guruswami-Sudan algorithm can be found as the smallest element of the basis produced by the *Interpolate* algorithm.

### B. Complexity analysis

Let us first estimate the convergence speed of the *Merge* algorithm. Recall, that this algorithm constructs a Gröbner basis of  $M_{r_1+r_2, u+v+1}$  given Gröbner bases of  $M_{r_1, u+1}$  and  $M_{r_2, v+1}$  (in fact,  $I_{r_1}$  and  $I_{r_2}$ ). For the sake of simplicity we will estimate the probability of  $M_{r_1+r_2, u+v+1}$  being generated by  $u + v + 1 + \delta$  polynomials given by (13), such that  $\text{LT } Q_s(x, y) = \gamma_s x^{q_s} y^s$  for  $s \leq u + v$ , and leading terms of summands do not cancel. The difference in the behavior of the actual algorithm *Merge* with respect to this impractical ideal multiplication method will be discussed below.

The polynomials  $Q_0(x, y), \dots, Q_{u+v+\delta}(x, y)$  can be represented as a  $(u + v + 1) \times (u + v + 1 + \delta)$  polynomial matrix  $\mathcal{Q}(x)$ . If they indeed generate  $M_{r_1+r_2, u+v+1}$ , then the  $(u+v+1) \times (u+v+1)$  polynomial matrix  $\mathcal{B}(x)$  corresponding to the Gröbner basis  $B_0(x, y), \dots, B_{u+v}(x, y)$  of this module satisfies

$$\mathcal{Q}(x)\mathcal{A}(x) = \mathcal{B}(x),$$

where  $\mathcal{Q}(x)$  is the polynomial matrix corresponding to  $Q_i(x, y)$ , and  $\mathcal{A}(x)$  is some transformation matrix. On the other hand,  $Q_j(x, y) \in M_{r_1+r_2, u+v+1}$ , i.e.  $\mathcal{Q}(x) = \mathcal{B}(x)\Lambda(x)$ , where the elements  $\lambda_{ji}(x)$  of  $\Lambda(x)$  matrix can be obtained by the multivariate division algorithm. Hence,

$$\mathcal{B}(x)\Lambda(x)\mathcal{A}(x) = \mathcal{B}(x). \quad (14)$$

Since  $\text{LT } B_j(x, y) = x^{b_j} y^j, 0 \leq j \leq u + v$ , the polynomials  $B_j(x, y)$  are linearly independent over  $\mathbb{F}[x]$ , and  $\mathcal{B}(x)$  is invertible over the field of rational functions, so it can be cancelled in (14). Therefore, the problem reduces to estimating the probability of existence of a polynomial matrix  $\mathcal{A}(x)$  satisfying

$$\Lambda(x)\mathcal{A}(x) = I. \quad (15)$$

This is a system of linear equations in terms of  $\mathcal{A}(x)$ . Observe that  $\Lambda(x)$  is a full-rank matrix over  $\mathbb{F}[x]$ . Polynomial solution exists if and only if the scalar matrix equations

$$\Lambda(x_w)\mathcal{A}(x_w) = I \quad (16)$$

are solvable for any  $x_w \in \mathbb{F}^*$ , i.e.  $\Lambda(x_w)$  matrices have rank  $u + v + 1$ , where  $\mathbb{F}^*$  is the algebraic closure of  $\mathbb{F}$ . It is sufficient to consider only such  $x_w$  that some fixed  $(u+v+1) \times (u+v+1)$  submatrix  $\hat{\Lambda}(x)$  of  $\Lambda(x)$  loses rank for  $x = x_w$ , i.e. the roots

of  $\det \widehat{\Lambda}(x)$ . Such roots are called eigenvalues of polynomial matrix  $\widehat{\Lambda}(x)$  [18].

Let  $\widehat{\Lambda}(x)$  be a matrix consisting of first  $u + v + 1$  columns of  $\Lambda(x)$ . This matrix satisfies

$$\mathcal{B}(x)\widehat{\Lambda}(x) = \widehat{\mathcal{Q}}(x),$$

where the polynomial matrix  $\widehat{\mathcal{Q}}(x)$  corresponds to  $Q_0(x, y), \dots, Q_{u+v}(x, y)$ . For each eigenvalue  $x_w \in \mathbb{F}^*$  of  $\widehat{\Lambda}(x)$  one can identify  $n_w$  linearly independent left eigenvectors, i.e. vectors  $z^{(w,1)}, \dots, z^{(w,n_w)}$ , such that  $z^{(w,l)}\widehat{\Lambda}(x_w) = 0, 1 \leq l \leq n_w$ . The geometric multiplicity  $n_w$  of eigenvalue  $x_w$  is upper-bounded by its algebraic multiplicity  $r_w$ , which is defined as the multiplicity of root  $x_w$  of  $\det \widehat{\Lambda}(x)$ . Equation (16) is solvable if for each  $l \sum_{j=0}^{u+v} z_j^{(w,l)} \lambda_{ji}(x_w) \neq 0$  for at least one  $i: u + v < i \leq u + v + \delta$ , i.e. if  $\Lambda(x_w)$  is a full-rank matrix. The total number of such pairs  $(x_w, z^{(w,l)})$  is upper-bounded by  $N = \deg \det \widehat{\Lambda}(x) = \deg \det \widehat{\mathcal{Q}}(x) - \deg \det \mathcal{B}(x)$ . The polynomials  $Q_i(x, y), 0 \leq i \leq u + v$  represent a Gröbner basis of some submodule of  $M_{r_1+r_2, u+v+1}$ , and could be obtained from those given by  $\mathcal{B}(x)$  by executing lines 6–10 of IIA for a few additional points  $(x_i, y_i)$  and/or pairs  $(\alpha, \beta)$ . Hence, by lemma 1,  $\Delta_1 = \deg \det \widehat{\mathcal{Q}}(x) = \Delta((Q_0(x, y), \dots, Q_{u+v}(x, y)))$  and  $\Delta_0 = \deg \det \mathcal{B}(x) = n \frac{(r_1+r_2)(r_1+r_2+1)}{2}$ .

Let polynomials  $Q_i(x, y), 0 \leq i \leq w$  be a Gröbner basis with respect to  $(1, k-1)$ -weighted degree lexicographic ordering of  $I_R$  and  $M_{R, w+1}$  for some  $R$  and  $w$ . Then  $\text{LT } Q_i(x, y) = x^{q_i} y^i, 0 \leq i \leq w$ , where<sup>1</sup>  $q_i \approx l_R - i(k-1), 0 \leq i \leq w-1$  for some  $l_R, q_w = 0$ , and  $\sum_{i=0}^w q_i = n \frac{R(R+1)}{2}$ . Hence<sup>2</sup>  $(w+1)l_R - (k-1) \frac{w(w+1)}{2} \approx n \frac{R(R+1)}{2}$ , and

$$l_R = l_R(w) \approx \frac{(k-1)w(w+1) + nR(R+1)}{2(w+1)}.$$

Since the polynomials  $P_i(x, y)$  and  $S_j(x, y)$  represent Gröbner bases of  $M_{r_1, u+1}$  and  $M_{r_2, v+1}$ ,  $\text{LT } P_i(x, y) = x^{p_i} y^i$ ,  $\text{LT } S_j(x, y) = x^{s_j} y^j$ , where  $p_i \approx l_{r_1}(u) - i(k-1)$  and  $s_j \approx l_{r_2}(v) - j(k-1)$ . Then  $q_i \approx l_{r_1}(u) + l_{r_2}(v) - i(k-1), 0 \leq i \leq u + v$ ,  $q_{u+v} = 0$  and  $N = \Delta_1 - \Delta_0 = \sum_{i=0}^{u+v} q_i - n \frac{(r_1+r_2)(r_1+r_2+1)}{2} \approx (l_{r_1}(u) + l_{r_2}(v))(u + v + 1) - (k-1) \frac{(u+v)(u+v+1)}{2} - n \frac{(r_1+r_2)(r_1+r_2+1)}{2}$ . Hence,

$$N \approx \frac{n}{2} \left( \frac{v}{u+1} r_1(r_1+1) + \frac{u}{v+1} r_2(r_2+1) - 2r_1r_2 \right). \quad (17)$$

Let us assume that the elements of  $\Lambda(x)$  are univariate polynomials with independent coefficients uniformly distributed over  $\mathbb{F}$ . Then  $\bar{\lambda}_{iwl} = \sum_{j=0}^{u+v} z_j^{(w,l)} \lambda_{ji}(x_w)$  are random variables uniformly distributed over  $\mathbb{F}^s$ , where  $\mathbb{F}^s$  is the smallest

<sup>1</sup>There is no formal proof for this approximation. However, one can argue that the polynomials in a Gröbner basis of  $M_{R, w+1}$  should have approximately the same  $(1, k-1)$ -weighted degree, since the IIA, which can be used to construct them, always increases the degree of the smallest polynomial. Numerical experiments confirm this claim. Alternatively, if the received sequence is not a codeword, a Gröbner basis of zero-dimensional ideal  $I_R$  must contain the polynomials with  $(1, k-1)$ -weighted degree both below and above the value given by (2), and the approximate expression for  $l_R$  derived below coincides with that one.

<sup>2</sup>The author thanks V. Miloslavskaya for pointing an error in this expression in the printed version of this paper.

algebraic extension of  $\mathbb{F}$ , such that  $x_w \in \mathbb{F}^s$ , and  $s$  is the extension degree. Then the probability of  $\bar{\lambda}_{iwl}$  being non-zero for at least one  $i \in \{u + v + 1, \dots, u + v + \delta\}$  is given by  $\theta_{s\delta} = 1 - \frac{1}{|\mathbb{F}|^{s\delta}}$ .

Consider factorization  $\det \widehat{\Lambda}(x) = \alpha \prod_i \phi_i(x)$ , where  $\alpha \in \mathbb{F} \setminus \{0\}$ , and  $\phi_i(x) \in \mathbb{F}[x]$  are some monic irreducible polynomials. Each eigenvalue  $x_w$  is a root of at least one of  $\phi_i(x)$ , so  $x_w \in \mathbb{F}^{\sigma_i}, \sigma_i = \deg \phi_i(x)$ , and  $N = \sum_i \sigma_i$ . Let  $\omega_j = |\{i: \sigma_i = j\}|, 1 \leq j \leq N$ . Observe that  $\phi_i(x)$  has  $\sigma_i$  distinct roots in  $\mathbb{F}^{\sigma_i}$ . Assuming the worst case, where the geometric and algebraic multiplicities of eigenvalues are the same, one obtains the following expression for the probability of (16) being solvable for all eigenvalues  $x_w$ :

$$\theta_\delta(\omega) = \prod_{j=1}^N \theta_{j\delta}^{j\omega_j} = \prod_{j=1}^N \left( 1 - \frac{1}{|\mathbb{F}|^{j\delta}} \right)^{j\omega_j}. \quad (18)$$

Assuming that  $\det \widehat{\Lambda}(x)$  is a polynomial with independent coefficients uniformly distributed over  $\mathbb{F}$ , one can estimate the probability of obtaining a particular factorization of  $\det \widehat{\Lambda}(x)$  as  $P_\omega = \frac{1}{|\mathbb{F}|^N} \prod_{j=1}^N \binom{\mu_j + \omega_j - 1}{\omega_j} [19]$ , where  $\mu_j$  is the number of monic irreducible polynomials of degree  $j$ . Hence, the probability of (15) being solvable is given by

$$\Theta(\delta) = \sum_{\omega} \theta_\delta(\omega) P_\omega,$$

where summation is performed over all partitions  $\omega$  of  $N$ .

Exact evaluation of this expression does not seem to be feasible. However, it can be seen that the value of (18) is dominated by the first multiple, and it is known that a random polynomial over a finite field  $\mathbb{F}$  has in average one root in it [20]. Hence, the probability of (15) being unsolvable decreases exponentially fast with  $\delta$ . Thus, for sufficiently large  $\mathbb{F}$  one can assume that a Gröbner basis of  $I_{r_1+r_2}$  can be derived from  $u + v + 1 + \delta, \delta = O(1)$  polynomials given by (13).

The above analysis was performed for an impractical version of the proposed randomized ideal multiplication method. It turns out that the polynomial matrix corresponding to the actual polynomials  $Q_0(x, y), \dots, Q_{u+v}(x, y)$  constructed on line 2 of the *Merge* algorithm has usually more than one eigenvalue in  $\mathbb{F}$  with high algebraic multiplicity. But the geometric multiplicity of the corresponding eigenvectors appears to be much less than the algebraic one (although still greater than 1), so the algorithm still quickly converges.

Let us now estimate the number of iterations of *Reduce* algorithm called on line 8 of *Merge*. To do this observe that the objective of *Reduce* is to decrease  $(1, k-1)$ -weighted degrees of polynomials constructed on lines 2 and 7 of *Merge* from approximately  $l_{r_1} + l_{r_2}$  to approximately  $l_{r_1+r_2}$ , i.e. to cancel the monomials with too high  $(1, k-1)$ -weighted degree. For each polynomial approximately  $(l_{r_1} + l_{r_2} - l_{r_1+r_2})(u + v + 1)$  monomials should be eliminated. The total number of monomials to be eliminated can be estimated as<sup>3</sup>  $\sum_{i=0}^{u+v} (l_{r_1} + l_{r_2} - l_{r_1+r_2})(u + v) = \sum_{i=0}^{u+v} (l_{r_1} + l_{r_2} - i(k-1) - (l_{r_1+r_2} - i(k-1)))(u + v + 1) = N(u + v + 1)$ . At least one monomial is

<sup>3</sup>Observe that the objective of minimization at line 2 of *Merge* is to decrease the number of monomials to be cancelled, i.e. decrease the number of iterations in *Reduce*.

cancelled during each iteration of *Reduce*. Taking into account (17), one obtains that the number of iterations in *Reduce* is given by  $O(\tilde{r}(n - \sqrt{nk}))$ , where  $\tilde{r} = r_1 + r_2$ . The algorithm operates with polynomials containing  $O(n(2\tilde{r})^2)$  terms, i.e. its complexity is given by  $O(n(n - \sqrt{nk})\tilde{r}^3)$ .

It can be seen from (1) that the number of polynomials in the basis of  $I_{\tilde{r}}$ ,  $\tilde{r} \leq r$  is  $O(\tilde{r}\sqrt{n/k})$ . The degrees of these polynomials can be estimated as  $\text{wdeg}_{(0,1)} Q_i(x, y) = O(\tilde{r}\sqrt{n/k})$  and  $\text{wdeg}_{(1,0)} Q_i(x, y) = O(n\tilde{r})$ . Computing a product of two such polynomials requires  $O(n\tilde{r}^2\sqrt{n/k}\log(\tilde{r}\sqrt{n/k})\log(n\tilde{r}))$  operations. The analysis given above suggests that the number of iterations performed by *Merge* is  $O(1)$ . Therefore, the complexity of polynomial multiplications needed to construct the Gröbner basis of  $I_{2\tilde{r}}$  from the basis of  $I_{\tilde{r}}$  is  $O(\frac{n^2}{k}\tilde{r}^3\log(\tilde{r}\sqrt{n/k})\log(n\tilde{r}))$ . Hence, one call to *Merge* at line 11 of the interpolation algorithm requires  $O(n\tilde{r}^3(a\log(\tilde{r}\sqrt{n/k})\log(n\tilde{r}) + b(n - \sqrt{nk})))$  operations for some positive  $a$  and  $b$ .

Obviously, the complexity of *Interpolate* algorithm is dominated by the FOR loop. The number of calls to *Merge* in this loop is given by

$$M = \lfloor \log_2 r \rfloor + \sum_{i=0}^{\lfloor \log_2 r \rfloor} r_i. \quad (19)$$

The second term in this expression corresponds to line 17 of the algorithm. The complexity of the whole algorithm is dominated by the last iteration, so the overall complexity is given by  $O(nr^3(a\log(r\sqrt{n/k})\log(nr) + b(n - \sqrt{nk})))$ . Observe that this is better than the complexity of IIA.

### C. Re-encoding

The proposed binary interpolation algorithm can be integrated with the re-encoding transformation [2], [3], [21]. As it was shown in section III-C2,  $M_{r,\rho} = [(y - T(x))^j \phi^{r-j}(x), y^s(y - T(x))^r, 0 \leq j \leq r, 1 \leq s \leq \rho - r]$ . Let  $\psi(x) = \prod_{i=1}^k (x - x_i)$ . Dividing  $T(x)$  by  $\psi(x)$ , one obtains

$$T(x) = h(x)\psi(x) + g(x),$$

where  $g(x_i) = y_i, 1 \leq i \leq k$  and  $h(x_i) = \frac{y_i - g(x_i)}{\psi(x_i)}$ ,  $i = k + 1, \dots, n$ . Substituting  $y = g(x) + z\psi(x)$  and dividing<sup>4</sup> all polynomials in  $M_{r,\rho}$  by  $\psi^r(x)$ , one obtains the module

$$\widehat{M}_{r,\rho} = \left\{ P(x, z) \in \mathbb{F}[x, y] \mid P\left(x_i, \frac{y_i - g(x_i)}{\psi(x_i)}\right) = 0^r, \right. \\ \left. i = k + 1, \dots, n, \text{wdeg}_{(0,1)} P(x, z) < \rho \right\},$$

which is generated by  $\widehat{\Pi}_{r,j}(x, z) = (z - h(x))^j \theta^{r-j}(x), 0 \leq j \leq r$  and  $\widehat{\Pi}_{r,r+j} = z^j \psi^j(x)(z - h(x))^r, 1 \leq j \leq \rho - r$ , where  $\theta(x) = \frac{\phi(x)}{\psi(x)}$ . There is a one-to-one correspondence between the polynomials in  $M_{r,\rho}$  and  $\widehat{M}_{r,\rho}$ , and the smallest polynomial with respect to  $(1, k - 1)$ -weighted degree lexicographic ordering in  $M_{r,\rho}$  corresponds to the smallest polynomial with respect to  $(1, -1)$ -weighted degree lexicographic ordering in  $\widehat{M}_{r,\rho}$ . If the leading term of a polynomial in  $M_{r,\rho}$  is  $a.x^i y^j$ ,

```

REENCODEINTERPOLATE(((x_i, y_i), 1 ≤ i ≤ n), r, k)
1  ψ(x) ← ∏_{i=1}^k (x - x_i), θ(x) = ∏_{i=k+1}^n (x - x_i)
2  T(x) ← ∑_{i=1}^n y_i ∏_{j≠i}^{(x-x_j)} / ∏_{j≠i}^{(x-x_j)}
3  Compute h(x) : T(x) = h(x)ψ(x) + g(x), deg g(x) < k
4  G ← (θ(x))
5  j ← 0
6  repeat
7      G ← REDUCE(G, (ψ(x)z)^j (z - h(x)))
8      j ← j + 1
9  until LT G_j = x^{(j-1)k} z^j
10 B ← G
11 Let r = ∑_{j=0}^m r_j 2^j, r_j ∈ {0, 1}
12 R ← 1
13 for j ← m - 1 to 0
14 do R ← 2R
15   B ← MERGE(B, B, δ(|B|, |B|, R))
16   if r_j = 1
17     then R ← R + 1
18     B ← MERGE(B, G, δ(|B|, |G|, R))
19 return B
    
```

Fig. 5. Construction of a Gröbner basis for  $\widehat{M}_{r,\rho}$

then the leading term of the corresponding polynomial in  $\widehat{M}_{r,\rho}$  is  $a.x^{i+jk-rk} z^j, a \in \mathbb{F}$ . This transformation essentially reduces the number of interpolation points. For high-rate codes this significantly decreases the number of terms in the polynomials, reducing thus the overall algorithm complexity.

The Gröbner basis of  $\widehat{M}_{r,\rho}$  can be constructed by a modified version of the *Interpolate* algorithm, as shown in Figure 5.  $(1, -1)$ -weighted degree lexicographic ordering must be used throughout this algorithm. The algorithm first constructs a Gröbner basis of  $\widehat{M}_{1,j+1}$ . The corresponding loop in the original algorithm terminates as soon as a polynomial with leading term  $y^j$  is discovered. After change of variables and term ordering the termination condition transforms to  $LTG_j = x^{(j-1)k} z^j$ . Then the algorithm proceeds with increasing root multiplicity in the same way as the original algorithm. However, the termination threshold  $\Delta_0$  of *Merge* algorithm has to be changed. For root multiplicity  $R$ , after the change of variables the basis polynomials should have leading terms  $x^{\widehat{t}_i} z^i, 0 \leq i \leq u - 1$ , such that  $\widehat{t}_i = t_i + (i - R)k$ , where  $x^{t_i} y^i$  are the leading terms of the corresponding polynomials which would be obtained without re-encoding. Therefore, the termination threshold in the modified algorithm should be set to  $\widehat{\Delta}_0 = \sum_{i=0}^{u-1} (t_i + (i - R)k) = \Delta_0 - Rku + k \frac{(u-1)u}{2} = \Delta_0 - k \frac{R(R+1)}{2} + k \frac{(u-1-R)(u-R)}{2}$ , where  $\Delta_0$  is the termination threshold derived from (9). If the sizes of the bases supplied to *Merge* are  $u_1$  and  $u_2$ , then  $u = u_1 + u_2 - 1$ . Hence, the termination threshold for *Merge* is given by  $\delta(u_1, u_2, R) = (n - k) \frac{R(R+1)}{2} + k \frac{(u_1+u_2-2-R)(u_1+u_2-1-R)}{2}$ .

## V. NUMERIC RESULTS

This section presents simulation results illustrating the performance of the proposed algorithm. Karatsuba fast univariate

<sup>4</sup>This operation prevents one from using the concept of ideal here.

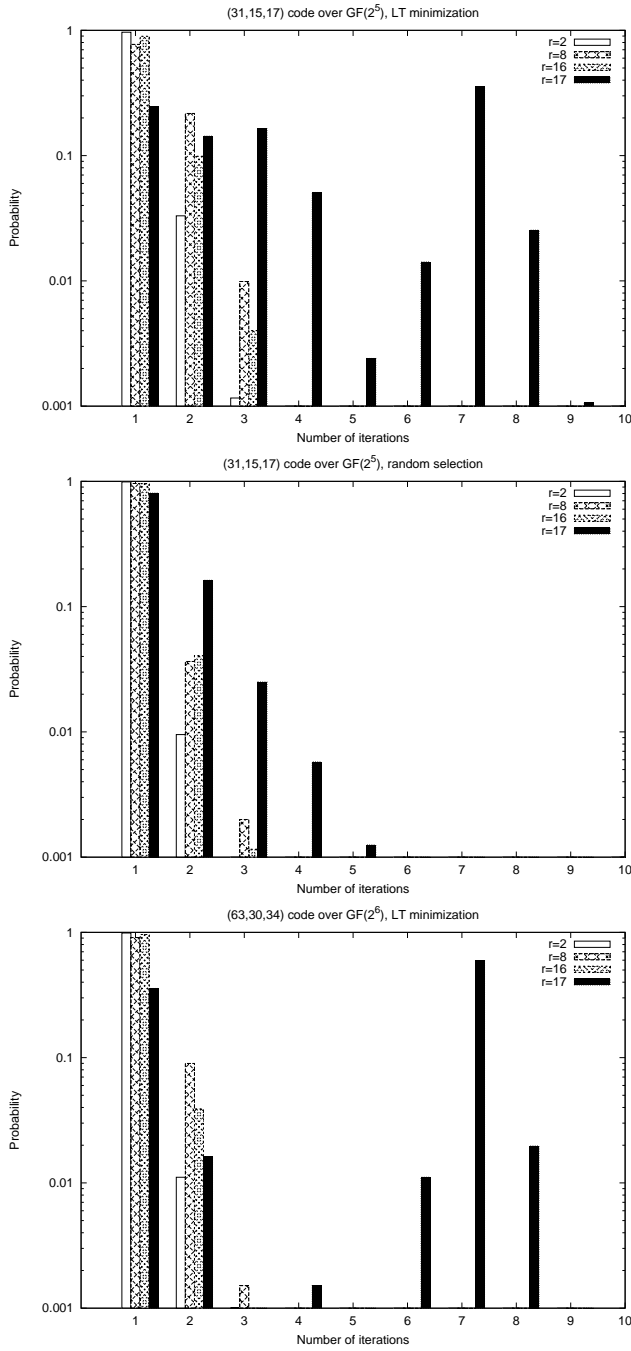


Fig. 6. Probability distribution of the number of iterations in Merge algorithm

polynomial multiplication algorithm [17] was used at steps 2 and 7 in Merge algorithm.

Figure 6 illustrates the probability distribution of the number of iterations performed by Merge algorithm while constructing Gröbner bases of  $I_r$  for different values of  $r$ . (31, 15, 17) code over  $GF(2^5)$  and (63, 30, 34) code over  $GF(2^6)$  were considered. First and third plots were obtained with the algorithm presented in Figure 3. The second plot was obtained by replacing leading term minimization on line 2 of the algorithm with random selection of  $Q_i(x, y)$  from the set  $\{P_i(x, y)S_0(x, y), \dots, P_{i-v}(x, y)S_v(x, y)\}$ . It can be seen

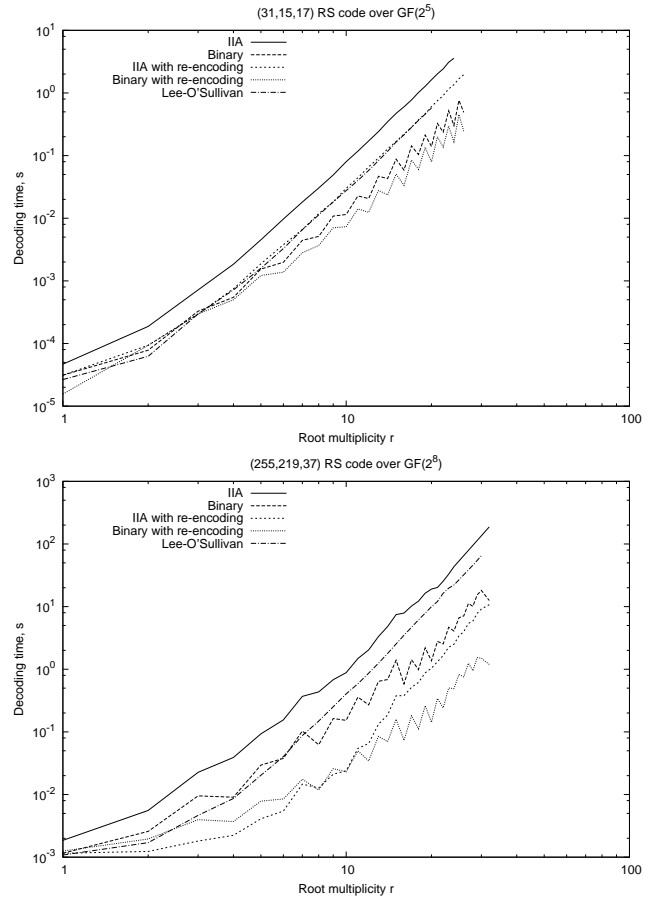


Fig. 7. Performance comparison of interpolation algorithms

that in this case the algorithm indeed converges exponentially fast. In the first and third cases the convergence is still exponential for  $r = 2^m$ , although a bit slower than in the case of random polynomial selection. However, for the case of  $r = 17$  up to 8 iterations may be needed with high probability. The reason is that constructing a Gröbner basis of  $I_{17} = I_{16} \cdot I_1$  requires processing two different collections of polynomials  $P_i(x, y), 0 \leq i \leq u$  and  $S_j(x, y), 0 \leq j \leq v$  with  $v \ll u$ . There is high probability that the smallest polynomial  $S_{j_0}(x, y)$  is used almost for all  $i$  on line 2 of the Merge algorithm. In this case the coefficients of  $\det \hat{\Lambda}(x)$  are no longer independent. In particular, this causes the most probable partitions  $\omega$  in (18) to be those with large  $\omega_1$ . This results in high algebraic and geometric multiplicity of  $\hat{\Lambda}(x)$  eigenvalues in  $\mathbb{F}$ . Hence, more correction polynomials (i.e. iterations of WHILE loop) are needed to eliminate them. This effect is partially compensated by reduction of the total number of iterations in Reduce algorithm. Observe also that for  $r = 2^m$  the algorithm converges faster for the case of  $|\mathbb{F}| = 64$  compared to  $|\mathbb{F}| = 32$ , as predicted by (18).

Figure 7 presents average list decoding time obtained with IIA, Lee-O'Sullivan algorithm, proposed binary interpolation algorithm, IIA with re-encoding transformation, and binary interpolation algorithm with re-encoding. (31,15,17) and (255, 219, 37) Reed-Solomon codes were considered. It can be seen that the proposed algorithm provides up to 12 times lower



complexity than IIA for the case of (31, 15, 17) code, and up to 15 times lower complexity for the case of (255, 219, 37) code. Observe that the complexity of the proposed method increases slower than for the case of IIA, confirming thus the conclusion of Section IV-B. The complexity of the Lee-O'Sullivan algorithm turns out to be essentially the same as the one of IIA with re-encoding for rate-1/2 code, and exceeds it considerably for high-rate code. Observe also, that in some cases increasing the root multiplicity reduces the complexity of the proposed interpolation method. This represents the impact of the second term in (19), i.e. line 17 of the proposed algorithm.

Observe also that the proposed algorithm outperforms the re-encoding method in the case of low-rate code. For the high-rate code the re-encoding method turns out to be better. However, employing re-encoding jointly with the proposed method further reduces the complexity. The overall gain with respect to IIA is up to 22 times for the case of (31, 15, 17) code, and up to 157 times for the case of (255, 219, 37) code.

## VI. CONCLUSIONS

In this paper a novel algorithm was proposed for the interpolation step of the Guruswami-Sudan list decoding algorithm. It is based on the binary exponentiation algorithm, and can be considered as an extension of the Lee-O'Sullivan method. The proposed algorithm was shown to achieve significant asymptotical and practical gain compared to the case of iterative interpolation algorithm. Furthermore, it can be integrated with the re-encoding transformation, achieving thus additional complexity reduction.

An important advantage of the new approach is that its first step (first iteration of the WHILE loop in *Interpolate* algorithm) coincides with the Gao decoding algorithm, which is able to correct up to  $(n - k)/2$  errors. Since the most likely error patterns can be corrected with this algorithm, one should invoke the remaining computationally expensive part of the proposed method only if the Gao algorithm does not produce a valid codeword. It is an open problem if it is possible to terminate the interpolation algorithm as soon as it produces a bivariate polynomial containing all the solutions of a particular instance of the decoding problem, and avoid construction of  $I_r$  basis for the worst-case  $r$  given by (1)-(3). Another interesting problem is to generalize the proposed algorithm to the case rational curve fitting problem considered in [22].

For the sake of simplicity, the proposed method was presented for the case of all interpolation points having the same multiplicity. However, it can be extended to the case of weighted interpolation, allowing thus efficient implementation of soft-decision decoding.

## ACKNOWLEDGEMENTS

The author thanks Dr. V.R. Sidorenko for many stimulating discussions. The author is indebted to the anonymous reviewers, whose comments have greatly improved the quality of the paper.

This work was partially supported by the grant of the President of Russian Federation MK-1195.2009.9.

## REFERENCES

- [1] V. Guruswami and M. Sudan, "Improved decoding of Reed-Solomon and algebraic-geometric codes," *IEEE Transactions on Information Theory*, vol. 45, no. 6, pp. 1757–1767, September 1999.
- [2] R. Koetter and A. Vardy, "A complexity reducing transformation in algebraic list decoding of Reed-Solomon codes," in *Proceedings of ITW2003*, March 2003.
- [3] R. Koetter, J. Ma, A. Vardy, and A. Ahmed, "Efficient interpolation and factorization in algebraic soft-decision decoding of Reed-Solomon codes," in *Proceedings of IEEE International Symposium on Information Theory*, Yokohama, Japan, June 29 – July 4 2003, p. 365.
- [4] R. R. Nielsen and T. Hoholdt, "Decoding Reed-Solomon codes beyond half the minimum distance," in *Proceedings of the International Conference on Coding Theory and Cryptography*. Mexico: Springer-Verlag, 1998.
- [5] T. Sauer, "Polynomial interpolation of minimal degree and Gröbner bases," in *Gröbner Bases and Applications (Proceedings of the International Conference "33 Years of Gröbner Bases")*, ser. London Mathematical Society Lecture Notes, B. Buchberger and F. Winkler, Eds., vol. 251. Cambridge University Press, 1998, pp. 483–494.
- [6] R. Koetter, "Fast generalized minimum-distance decoding of algebraic-geometry and Reed-Solomon codes," *IEEE Transactions On Information Theory*, vol. 42, no. 3, May 1996.
- [7] H. O'Keefe and P. Fitzpatrick, "Gröbner basis solutions of constrained interpolation problems," *Linear Algebra and Applications*, vol. 351, pp. 533–551, 2002.
- [8] J. Ma, P. Trifonov, and A. Vardy, "Divide-and-conquer interpolation for list decoding of Reed-Solomon codes," in *Proceedings of IEEE International Symposium on Information Theory*, Chicago, USA, June 27 – July 2 2004, p. 387.
- [9] P. Trifonov, "Interpolation in list decoding of Reed-Solomon codes," *Problems of Information Transmission*, vol. 43, no. 3, pp. 190–198, 2007.
- [10] K. Lee and M. E. O'Sullivan, "An interpolation algorithm using Gröbner bases for soft-decision decoding of Reed-Solomon codes," in *Proceedings of IEEE International Symposium on Information Theory*, 2006.
- [11] M. Alekhovich, "Linear Diophantine equations over polynomials and soft decoding of Reed-Solomon codes," *IEEE Transactions On Information Theory*, vol. 51, no. 7, pp. 2257–2265, July 2005.
- [12] K. Lee and M. E. O'Sullivan, "List decoding of Reed-Solomon codes from a Gröbner basis perspective," *Journal of Symbolic Computation*, vol. 43, no. 9, September 2008.
- [13] P. Trifonov, "On the relationship of some Reed-Solomon decoding algorithms," in *Proceedings of "Coding Theory Days in Saint-Petersburg" Workshop*, 2008, pp. 83–87.
- [14] T. Becker and V. Weispfenning, *Gröbner Bases. A Computational Approach to Commutative Algebra*. New York: Springer, 1993.
- [15] S. Gao, "A new algorithm for decoding Reed-Solomon codes," in *Communications, Information and Network Security*, V. Bhargava, H. V. Poor, V. Tarokh, and S. Yoon, Eds. Kluwer, 2003, pp. 55–68.
- [16] S. Fedorenko, "A simple algorithm for decoding Reed-Solomon codes and its relation to the Welch-Berlekamp algorithm," *IEEE Transactions On Information Theory*, vol. 51, no. 3, pp. 1196–1198, March 2005.
- [17] D. E. Knuth, *The Art of Computer Programming*. Addison-Wesley, 1973, vol. 2.
- [18] I. Gohberg, P. Lancaster, and L. Rodman, *Matrix polynomials*. SIAM, 2009.
- [19] J. D. Dixon and D. Panario, "The degree of the splitting field of a random polynomial over a finite field," *The Electronic Journal of Combinatorics*, vol. 11, no. 1, 2004.
- [20] V. Leont'ev, "Roots of random polynomials over a finite field," *Mathematical Notes*, vol. 80, no. 2, pp. 300–304, 2006, translated from *Matematicheskie Zametki*, vol. 80, no. 2, 2006, pp. 313–316.
- [21] J. Ma and A. Vardy, "A complexity reducing transformation for the Lee-O'Sullivan interpolation algorithm," in *Proceedings of IEEE International Symposium on Information Theory*, 2007.
- [22] Y. Wu, "New list decoding algorithms for Reed-Solomon and BCH codes," *IEEE Transactions On Information Theory*, vol. 54, no. 8, August 2008.

**Peter Vladimirovich Trifonov** was born in St.Petersburg, USSR in 1980. He received the MSc degree in computer science in 2003, and PhD (Candidate of Science) degree from St.Petersburg State Polytechnic University in 2005.

Currently he is an Associate Professor at the Distributed Computing and Networking department of the same university. His research interests include coding theory and its applications in telecommunications and other areas. Since September, 2008 he is serving as a secretary of the IEEE Russia Joint Sections Information Theory Society Chapter.