

On decoding up to error correcting capacity of linear error-correcting codes with Gröbner bases

Stanislav Bulygin ^{*} and Ruud Pellikaan [†]

December 20, 2006

Abstract

The problem of decoding up to error correcting capacity of arbitrary linear codes with the use of Gröbner bases is addressed. A new method is proposed, which is based on reducing an initial decoding problem to solving some system of polynomial equations over a finite field. The peculiarity of this system is that, when we want to decode up to half the minimum distance, it has a unique solution even over the algebraic closure of the considered finite field, although field equations are not added. The equations in the system have degree at most 2. Some experimental results for the method are presented.

1 Introduction

In this paper we consider bounded distance decoding of arbitrary linear codes with the use of Gröbner bases. In recent years a lot of attention was devoted to this question for cyclic codes that is a particular subclass of linear codes. In this introduction we give some background on decoding with Gröbner bases for cyclic codes and sketch several approaches that exist for arbitrary codes.

^{*}bulygin@mathematik.uni-kl.de, Department of Mathematics, Technical University of Kaiserslautern, P.O. Box 3049, 67653 Kaiserslautern, Germany

[†]g.r.pellikaan@tue.nl, Department of Mathematics and Computing Science, Eindhoven University of Technology, P.O. Box 513, NL-5600 MB Eindhoven, The Netherlands

The reader is assumed to be familiar with the basics of error-correcting codes and Gröbner bases theory. Introduction material can be taken for instance from [5, 19] and [11, 13], respectively. Next we give some remarks on finding the minimum distance by techniques based on Gröbner bases. At the end we present some background on the complexity of algorithms of decoding and finding the minimum distance.

Quite a lot of methods exist for decoding cyclic codes and the literature on this topic is vast. We just mention [5, 19, 24]. All these methods are of polynomial complexity and efficient in practice, but do not correct up to the true error-correcting capacity. The Gröbner bases based techniques were addressed to remedy this problem, but have as a drawback that they have exponential complexity. These methods can be roughly divided into the following categories:

- Unknown syndromes: [5, pp. 231-240] and [25, 15, 16];
- Newton identities method: [2, 3, 1, 9];
- Cooper's philosophy using the power sums: [10, 8, 9, 7, 18].

Our method is a generalization of the first one of unknown syndromes for arbitrary linear codes.

This outline paper is organized as follows. In section 2 we introduce the notion of an MDS basis and MDS matrix together with some important properties. In section 3 we present the main result. The proofs in this section are just outlined, only the main idea is given. In section 4 we show some experimental results obtained with the technique we presented. We conclude and summarize in section 5. The extended version of this outline paper is [20].

Notations: A field is denoted by \mathbb{F} and its algebraic closure by $\bar{\mathbb{F}}$. The finite field with q elements is denoted by \mathbb{F}_q . If I is an ideal in the polynomial ring $\mathbb{F}[X_1, \dots, X_n]$ over the field \mathbb{F} , then a zero or a solution of I is a point $\mathbf{x} \in \bar{\mathbb{F}}^n$ such that $f(\mathbf{x}) = 0$ for all $f \in I$. The zero set of I is the set of all solutions of I in $\bar{\mathbb{F}}^n$ and is denoted by $Z(I)$.

2 Matrix in MDS form

Let \mathbb{F} be a field. Let $\bar{\mathbb{F}}$ be the algebraic closure of \mathbb{F} . Let $\mathbf{b}_1, \dots, \mathbf{b}_n$ be a basis of \mathbb{F}^n . Now B is the $n \times n$ matrix with $\mathbf{b}_1, \dots, \mathbf{b}_n$ as rows.

Definition 2.1 The (*unknown*) syndrome $\mathbf{u}(B, \mathbf{e})$ of a word \mathbf{e} with respect to B is the column vector $\mathbf{u}(B, \mathbf{e}) = B\mathbf{e}^T$. It has entries $u_i(B, \mathbf{e}) = \mathbf{b}_i \cdot \mathbf{e}$ for $i = 1, \dots, n$.

Definition 2.2 Define the coordinatewise star product of two vectors $\mathbf{x}, \mathbf{y} \in \mathbb{F}^n$ by

$\mathbf{x} * \mathbf{y} = (x_1y_1, \dots, x_ny_n)$. Then $\mathbf{b}_i * \mathbf{b}_j$ is a linear combination of the basis vectors $\mathbf{b}_1, \dots, \mathbf{b}_n$, that is there are constants $\mu_{ijl} \in \mathbb{F}$ such that

$$\mathbf{b}_i * \mathbf{b}_j = \sum_{l=1}^n \mu_{ijl} \mathbf{b}_l.$$

The elements $\mu_{ijl} \in \mathbb{F}$ are called the *structure constants* of the basis $\mathbf{b}_1, \dots, \mathbf{b}_n$.

Definition 2.3 Define the $n \times n$ matrix of (*unknown*) syndromes $\mathcal{U}(\mathbf{e})$ of a word \mathbf{e} by $u_{ij}(\mathbf{e}) = (\mathbf{b}_i * \mathbf{b}_j) \cdot \mathbf{e}$. The following abbreviations $\mathbf{u}(\mathbf{e})$ and $u_i(\mathbf{e})$ are used for $\mathbf{u}(B, \mathbf{e})$ and $u_i(B, \mathbf{e})$, respectively.

Remark 2.4 The relation between the entries of the matrix $\mathcal{U}(\mathbf{e})$ and the vector $\mathbf{u}(\mathbf{e})$ of unknown syndromes is given by

$$u_{ij}(\mathbf{e}) = \sum_{l=1}^n \mu_{ijl} u_l(\mathbf{e}).$$

Proposition 2.5 *The rank of $\mathcal{U}(\mathbf{e})$ is equal to the weight of \mathbf{e} .*

Proof. The proof is straightforward. See also [17, Lemma 4.7]. ◇

So there are $\text{wt}(\mathbf{e}) + 1$ columns of $\mathcal{U}(\mathbf{e})$ that are dependent and every w tuple of columns of $\mathcal{U}(\mathbf{e})$ are independent if $w \leq \text{wt}(\mathbf{e})$. We will look at the smallest t such that the first $t + 1$ columns are dependent. Consider the $v \times w$ matrix $\mathcal{U}_{vw}(\mathbf{y})$ of a word \mathbf{y} with the entries $u_{ij}(\mathbf{y})$ for $i = 1, \dots, v$ and j, \dots, w . For an arbitrary matrix B we have to go through all the $\binom{n}{w}$ of all w -tuples of columns of B with $w \leq \text{wt}(\mathbf{e}) + 1$ to find such a dependency. This is not very efficient. There is a more efficient way with the help of a B in special form.

Definition 2.6 Let $\mathbf{b}_1, \dots, \mathbf{b}_n$ be a basis of \mathbb{F}^n . Let B_r be the $r \times n$ matrix with $\mathbf{b}_1, \dots, \mathbf{b}_r$ as rows. Let $B = B_n$. We say that $\mathbf{b}_1, \dots, \mathbf{b}_n$ is an ordered MDS basis and B an MDS matrix if all the $t \times t$ submatrices of B_t have rank t for all $t = 1, \dots, n$. Let C_t be the code with B_t as parity check matrix.

Remark 2.7 Let B be an MDS matrix. Then C_t is an MDS code for all t .

Remark 2.8 Let \tilde{C} be the code over \mathbb{F}_{q^m} that is generated by C . Then C is the restriction of \tilde{C} to \mathbb{F}_q^n , that is $C = \mathbb{F}_q^n \cap \tilde{C}$. Furthermore C and \tilde{C} have the same minimum distance.

For any prime p and positive integer M there is an algorithm of polynomial computing time $(p \log M)^{\mathcal{O}(1)}$ that computes an irreducible polynomial of degree $m = M + o(M)$ over \mathbb{F}_p . See [22, 23]. Hence for a given field \mathbb{F}_q , the complexity of finding an extension \mathbb{F}_{q^m} such that $q^m \geq n$, is polynomial in n .

Definition 2.9 Let M be an $m \times n$ matrix. Let $\mathbf{i} = (i_1, \dots, i_u)$ with $1 \leq i_1 < \dots < i_u \leq m$ and $\mathbf{j} = (j_1, \dots, j_v)$ with $1 \leq j_1 < \dots < j_v \leq n$. Then $M[\mathbf{i}, \mathbf{j}]$ is the $u \times v$ submatrix of M consisting of rows indexed by \mathbf{i} and the columns indexed by \mathbf{j} . Define furthermore $M[u, \mathbf{j}] = M[(1, \dots, u), \mathbf{j}]$ and $M[\mathbf{i}, v] = M[\mathbf{i}, (1, \dots, v)]$.

Proposition 2.10 Suppose that B is an MDS matrix. Let $w = wt(\mathbf{e})$. If $u \geq w$, then

$$\text{rank}(\mathcal{U}_{uv}(\mathbf{e})) = \min\{v, w\}.$$

Proof. The triple product $\mathcal{U}_{uv}(\mathbf{e}) = B_u D(\mathbf{e}) B_v^T$ implies that

$$\text{rank}(\mathcal{U}_{uv}(\mathbf{e})) \leq \min\{v, w\},$$

since $\text{rank}(B_u) = u$, $\text{rank}(B_v) = v$ and $\text{rank}(D(\mathbf{e})) = w \leq u$.

Let $\mathbf{j} = (j_1, \dots, j_w)$ be the w positions of the support of \mathbf{e} in increasing order. Let $\mathbf{e}' = (e_{j_1}, \dots, e_{j_w})$. Then $B[v, \mathbf{j}]$ is the submatrix of B_v consisting of the columns indexed by \mathbf{j} . So $B_u D(\mathbf{e}) B_v^T$ has $B[u, \mathbf{j}] D(\mathbf{e}') B[v, \mathbf{j}]^T$ as submatrix and with zeros in the complementary entries. Now $D(\mathbf{e}')$ is invertible, since all the coordinates of \mathbf{e}' are nonzero. Hence $B_u D(\mathbf{e}) B_v^T$ has the same rank as $B[u, \mathbf{j}] B[v, \mathbf{j}]^T$.

It is assumed that $w \leq u$. Hence $B[w, \mathbf{j}]$ is an invertible submatrix of $B[u, \mathbf{j}]$, since B is an MDS matrix. Hence $B[u, \mathbf{j}] B[v, \mathbf{j}]^T$ has the same rank as $B[v, \mathbf{j}]^T$

If $w \leq v$, then $B[w, \mathbf{j}]$ is an invertible $w \times w$ submatrix of $B[v, \mathbf{j}]$. Therefore the rank of \mathcal{U}_{uv} is equal to w .

If $w > v$, then $B[v, \mathbf{j}]^T$ is a generator matrix of an MDS code of length w and dimension v . Therefore the rank of \mathcal{U}_{uv} is equal to v . \diamond

Hence $\mathcal{U}_{nv}(\mathbf{e})$ has rank v if $v \leq \text{wt}(\mathbf{e})$, and its rank is $\text{wt}(\mathbf{e})$ if $v > \text{wt}(\mathbf{e})$.

3 Decoding up to half the minimum distance

Without loss of generality we may assume, after a finite extension of the finite field \mathbb{F}_q , that $n \leq q$. Let $\mathbf{b}_1, \dots, \mathbf{b}_n$ be a basis of \mathbb{F}_q^n . From now on we assume that the corresponding matrix B is an MDS matrix.

Let C be an \mathbb{F}_q -linear code with parameters $[n, k, d]$. Choose a parity check matrix H of C . The redundancy is $r = n - k$. Let $\mathbf{h}_1, \dots, \mathbf{h}_r$ the the rows of H . The row \mathbf{h}_i is a linear combination of the basis $\mathbf{b}_1, \dots, \mathbf{b}_n$, that is there are constants $a_{ij} \in \mathbb{F}_q$ such that

$$\mathbf{h}_i = \sum_{j=1}^n a_{ij} \mathbf{b}_j.$$

In other words $H = AB$ where A is the $r \times n$ matrix with entries a_{ij} .

Remark 3.1 Let $\mathbf{y} = \mathbf{c} + \mathbf{e}$ be a received word with $\mathbf{c} \in C$ a codeword and \mathbf{e} an error vector. The syndromes of \mathbf{y} and \mathbf{e} with respect to H are equal and known: $s_i(\mathbf{y}) := \mathbf{h}_i \cdot \mathbf{y} = \mathbf{h}_i \cdot \mathbf{e} = s_i(\mathbf{e})$ and they can be expressed in the unknown syndromes of \mathbf{e} with respect to B :

$$s_i(\mathbf{y}) = \sum_{j=1}^n a_{ij} u_j(\mathbf{e}),$$

since $\mathbf{h}_i = \sum_{j=1}^n a_{ij} \mathbf{b}_j$ and $\mathbf{b}_j \cdot \mathbf{e} = u_j(\mathbf{e})$.

Definition 3.2 The ideal $I(t, \mathcal{U}, V)$ in the ring $\mathbb{F}[U_1, \dots, U_n, V_1, \dots, V_t]$ is generated by the elements

$$\sum_{j=1}^t U_{ij} V_j - U_{it+1} \quad \text{for } i = 1, \dots, n$$

Let $Z(t, \mathcal{U}, V)$ be the zero set of $I(t, \mathcal{U}, V)$ over $\bar{\mathbb{F}}$.

Definition 3.3 The ideal $J(\mathbf{y})$ in the ring $\mathbb{F}_q[U_1, \dots, U_n]$ is generated by the elements

$$\sum_{l=1}^n a_{jl}U_l - s_j(\mathbf{y}) \quad \text{for } j = 1, \dots, r$$

Let $J(t, \mathbf{y})$ be the ideal in $\mathbb{F}_q[U_1, \dots, U_n, V_1, \dots, V_t]$ generated by $J(\mathbf{y})$ and $I(t, \mathcal{U}, V)$ from Definition 3.2.

Remark 3.4 The ideal $J(t, \mathbf{y})$ is generated by $n - k$ linear functions and n quadratic polynomials.

Now we state several lemmas that are used in the proof of the main theorem: Theorem 3.8. They are quite elementary, so we omit the proofs.

Lemma 3.5 *If $\mathbf{y} = \mathbf{c} + \mathbf{e}$ for some $\mathbf{c} \in C$ and $\text{wt}(\mathbf{e}) = t$, then there is a \mathbf{v} such that $(\mathbf{u}(\mathbf{e}), \mathbf{v})$ is a solution of $J(t, \mathbf{y})$.*

Lemma 3.6 *Let (\mathbf{u}, \mathbf{v}) be a solution of $J(t, \mathbf{y})$. Then there is a unique \mathbf{e} such that $\mathbf{u} = \mathbf{u}(\mathbf{e})$, furthermore $\mathbf{y} = \mathbf{c} + \mathbf{e}$ for some $\mathbf{c} \in C$ and $\text{wt}(\mathbf{e}) \leq t$.*

Lemma 3.7 *If (\mathbf{u}, \mathbf{v}) and (\mathbf{u}, \mathbf{w}) are distinct solutions of $J(t, \mathbf{y})$, then there is a solution (\mathbf{u}, \mathbf{z}) of $J(t', \mathbf{y})$ for some t' with $t' < t$. If furthermore $t' = 0$, then \mathbf{y} is a codeword.*

Theorem 3.8 *Let B be an MDS matrix with structure constants μ_{ijl} and linear functions U_{ij} . Let H be a parity check matrix of the code C such that $H = AB$. Let $\mathbf{y} = \mathbf{c} + \mathbf{e}$ be a received word with \mathbf{c} in C the codeword sent and \mathbf{e} the error vector. Suppose that the weight of \mathbf{e} is not zero and at most $(d(C) - 1)/2$. Let t be the smallest positive integer such that $J(t, \mathbf{y})$ has a solution (\mathbf{u}, \mathbf{v}) over $\bar{\mathbb{F}}_q$. Then $\text{wt}(\mathbf{e}) = t$ and the solution is unique satisfying $\mathbf{u} = \mathbf{u}(\mathbf{e})$.*

Proof. 1) There is a solution $(\mathbf{u}(\mathbf{e}), \mathbf{v})$ of $J(\text{wt}(\mathbf{e}), \mathbf{y})$ by Lemma 3.5.
2) Suppose that t is the smallest positive integer such that $J(t, \mathbf{y})$ has a solution over $\bar{\mathbb{F}}_q$. Then $t \leq \text{wt}(\mathbf{e})$ by (1).
Suppose that $(\mathbf{u}', \mathbf{v}')$ is a solution. Then there is a unique $\mathbf{e}' \in \mathbb{F}_{q^m}^n$ for some m such that $\mathbf{u}' = \mathbf{u}(\mathbf{e}')$ and $\mathbf{y} = \mathbf{c}' + \mathbf{e}'$ for some $\mathbf{c}' \in \tilde{C}$ and $\text{wt}(\mathbf{e}') \leq t$ by Lemma 3.6. Now $\mathbf{s}(\mathbf{e}') = \mathbf{s}(\mathbf{y}) = \mathbf{s}(\mathbf{e})$. Hence $\mathbf{e}' - \mathbf{e}$ is a codeword of \tilde{C} . Now C and \tilde{C} have the same minimum distance by Remark 2.8. By assumption we have that $\text{wt}(\mathbf{e}) \leq (d(\tilde{C}) - 1)/2$. The minimality of t implies

$\text{wt}(\mathbf{e}') \leq t \leq \text{wt}(\mathbf{e})$. Hence $\mathbf{e}' - \mathbf{e}$ is a codeword \tilde{C} of weight strictly smaller than $d(\tilde{C})$. So $\mathbf{e}' = \mathbf{e}$. Therefore $\mathbf{u}' = \mathbf{u}(\mathbf{e})$ is unique if $(\mathbf{u}', \mathbf{v}')$ is a solution. Now suppose that (\mathbf{u}, \mathbf{v}) and (\mathbf{u}, \mathbf{w}) are distinct solutions of $J(t, \mathbf{y})$. Then there is a solution (\mathbf{u}, \mathbf{z}) of $J(t', \mathbf{y})$ for some $1 \leq t' < t$ by Lemma 3.7, since \mathbf{y} is not a codeword. This contradicts the minimality of t . Hence the solution is unique. \diamond

Definition 3.9 Let \mathcal{V} be an $l \times m$ matrix with entries in $\mathbb{F}[U_1, \dots, U_n]$. Let \mathcal{V}_{uv} be the submatrix of \mathcal{V} consisting of the first u rows and the first v columns. Let $I(t, \mathcal{V})$ be the ideal generated by the determinants of all $(t+1) \times (t+1)$ submatrices of $\mathcal{V}_{l,t+1}$. Let $Z(t, \mathcal{V})$ be the zero set of $I(t, \mathcal{V})$ in $\bar{\mathbb{F}}^n$.

Corollary 3.10 *Let $\mathbf{y} = \mathbf{c} + \mathbf{e}$ be a received word with \mathbf{c} in C the codeword sent and \mathbf{e} the error vector. Suppose that the weight of \mathbf{e} is not zero and at most $(d(C) - 1)/2$. Let t be the smallest positive integer such that $J(t, \mathbf{y})$ has a solution. Then the solution is unique and the reduced Gröbner basis G for the ideal $J(t, \mathbf{y})$ with respect to any monomial ordering will be*

$$\begin{aligned} U_i - u_i(\mathbf{e}), i = 1, \dots, n, \\ V_j - v_j, j = 1, \dots, t, \end{aligned}$$

where $(\mathbf{u}(\mathbf{e}), \mathbf{v})$ is the unique solution.

Proof. The corollary states that the unique solution of Theorem 3.8 has multiplicity one. Let us first give a sketch of the proof. If (\mathbf{u}, \mathbf{v}) is the unique solution of $J(t, \mathbf{y})$, then $\mathbf{u} \in \bar{\mathbb{F}}^n$ is the unique element in the intersection of the linear affine spaces $Z(J(\mathbf{y}))$ and $Z(t, \mathcal{U})$. We show that $Z(t, \mathcal{U})$ is the finite union of linear spaces. The solution is unique. Hence $Z(J(\mathbf{y}))$ intersects exactly one of the components of $Z(t, \mathcal{U})$. The intersection of linear spaces is transversal, since the intersection consists of exactly one point. Hence $J(\mathbf{y}) + I(t, \mathcal{U})$ is equal to the maximal ideal $\langle U_1 - u_1, \dots, U_n - u_n \rangle$. The V_j satisfy linear equations in the U_{ij} which we now may assume to be constants. The solution for the V_j is unique and equal to v_j . Gaussian elimination gives that $V_j - v_j$ is an element of $J(t, \mathbf{y})$. \diamond

Remark 3.11 We note that in [1] Augot et al. also prove the uniqueness result for cyclic codes. Still they did not succeed to prove that their unique solution has multiplicity one. Our Corollary 3.10 states exactly this for arbitrary linear codes.

4 Simulations and experimental results

All computations in this section were undertaken on AMD Athlon 64 Processor 2800+ (1.8MHz), 512MB RAM under Linux. The computations of Gröbner bases were realized in SINGULAR 3-0-1 [14]. The command `std` was chosen as more effective than `slingb`.

Here we present some results on decoding with the use of Theorem 3.8 for binary random codes. First we determine the minimum distance of a random code with the method from [6] and then perform decoding of some given number of received words. The number of errors that occur in these received words equals the error capacity of the code. The results are given in the following table, with the columns: the parameters of the code, the error-correcting capacity, time to compute the minimum distance, total time to decode with Gröbner bases, the number of received words, and the average time to decode with Gröbner bases, respectively. The time is provided in seconds.

Code	err. cap.	mindist.	GB dec.	no. of rec.	average
[25,11,4]	1	2.99	1.10	300	0.0037
[25,11,5]	2	21.58	2.89	300	0.0096
[25,8,5]	2	0.99	1.84	300	0.0061
[25,8,6]	2	3.38	1.79	300	0.0060
[25,8,7]	3	12.26	6.94	300	0.0231
[31,15]	2	-	10.76	300	0.0359
[31,15]	3	-	11.19	10	1.119

We only cite the time needed for GB computations in the decoding. They are responsible for approximately 90% of the overall decoding time. The rest is spent on auxiliary operations and manipulations. The bar "-" means that a computation took more than 1000 sec. and we were not able to actually compute min.dist. in a short time, so we have just assumed the error capacity.

We are able to correct even more errors in larger codes. Next table shows timings for binary [120, 10], [120, 20], [120, 30] and [150, 10] codes, where 1 means one second or less. As the behavior of decoding seems to be more or less the same for all error-vectors of the given weight, we have used only 1

received word in the table below.

no. of err.	[120,40]	[120,30]	[120,20]	[120,10]	[150,10]
2	1	1	1	1	1
3	13	1	1	1	1
4	313	9	1	1	1
5	-	62	1	1	1
6	-	200	5	1	3
7	-	933	14	1	4
8	-	-	32	1	4
9	-	-	74	1	4
10	-	-	183	2	6
11	-	-	633	3	6
12	-	-	-	4	6
13	-	-	-	5	8
14	-	-	-	6	8
15	-	-	-	14	10
16	-	-	-	20	11
17	-	-	-	29	16
18	-	-	-	71	16
19	-	-	-	139	34
20	-	-	-	327	53
21	-	-	-	-	84
22	-	-	-	-	133
23	-	-	-	-	241
24	-	-	-	-	513

Remark 4.1 For a method for speeding up the above computations see [6]. There we also compare our method with the one of Fitzgerald-Lax [12]. The simulations indicate that when dealing with random (binary) codes the Fitzgerald-Lax method has problems starting already at 3 errors [20, 6].

Remark 4.2 On some comparisons for Hermitian codes see [6]. Consult the latter reference also for comparisons with the method of Augot et. al. for cyclic codes.

Remark 4.3 We note that the rate of a code is a determining factor for complexity. Indeed, we have a system with $n + t$ variables and $n + r$ equations. It was noticed by researchers that overdetermined systems of algebraic equations in general are easier to solve (cf. e.g. [4], [21]). So if, for given n , we increase redundancy r , or reduce the number of errors t we want to solve, the system becomes more overdetermined, which positively reflects on complexity. We could see on the above tables, how decrease in dimension caused better performance of the system.

5 Conclusions and final remarks

In this paper we proposed the new method for decoding arbitrary linear codes. This method is based on reducing an initial decoding problem to solving some system of polynomial equations over a finite field. The peculiarity of our system is that it has a unique solution even over the algebraic closure of the finite field we are working with, although we have not added field equations. The equations in our system have degree at most 2, which is a certain plus. Nevertheless, high density of equations provides obstacles, when working with large parameters of codes.

Here we briefly mention that the above method can also be adapted for finding the minimum distance and nearest codeword decoding. Another interesting issue to consider is to look at generic decoding, where syndromes enter as variables, rather than concrete values. For some details on all the above see [6]. We also refer to this paper for some discussions on complexity issues.

We have compared our method with other existing methods. Although, our method is slower, than e.g. the method based on Waring function designed specifically for cyclic codes [1], it is much faster, than the method of Fitzgerald-Lax for arbitrary linear codes. We also have shown that our approach in some range of parameters is superior to the generic syndrome decoding - basically the only generic decoding algorithm, except by pure exhaustion. The rough clue would be to use our method instead of syndrome decoding, when the dimension of a code is small comparing to its length, but not too small, so that exhaustion is infeasible.

As future work we see applications of the described method to crypt-analysing schemes based on error-correcting codes. The question of generic decoding and closed formulas also deserves further attention.

Acknowledgement

The first author would like to thank "Cluster of Excellence in Rhineland-Palatinate" for funding his research, and also personally his Ph.D. supervisor Prof.Dr. Gert-Martin Greuel and his second supervisor Prof.Dr. Gerhard Pfister for continuous support. The work of the first author has been partially inspired by the Special Semester on Groebner Bases, February 1 - July 31, 2006, organized by RICAM, Austrian Academy of Sciences, and RISC, Johannes Kepler University, Linz, Austria. He also would like to thank Max Sala for usefull discussions and comments.

References

- [1] D. Augot, M. Bardet, and J.-C. Faugère. Efficient decoding of (binary) cyclic codes beyond the correction capacity of the code using Gröbner bases. Technical Report 4652, INRIA, nov 2002.
- [2] D. Augot, P. Charpin, and N. Sendrier. The minimum distance of some binary codes via the Newton's Identities. In *Eurocodes'90*, volume LNCS 514, pages 65–73, 1990.
- [3] D. Augot, P. Charpin, and N. Sendrier. Studying the locator polynomial of minimum weight codewords of BCH codes. *IEEE Trans. Inform. Theory*, IT-38:960–973, may 1992.
- [4] M. Bardet, J.-C.Faugère, and B. Salvy. Complexity of Gröbner basis computation for semi-regular overdetermined sequences over $GF(2)$ with solutions in $GF(2)$. Technical Report 5049, INRIA, 2003.
- [5] E.R. Berlekamp. *Algebraic coding theory*. Mc Graw Hill, 1968.
- [6] S. Bulygin and R. Pellikaan. Decoding and finding the minimum distance of error-correcting codes with gröbner bases. Technical Report ..., TU Kaiserslautern, 2006.
- [7] M. Caboara and T. Mora. The Chen-Reed-Helleseth-Truong decoding algorithm and the Gianni-Kalkbrenner Gröbner shape theorem. *Appl. Algeb. Eng. Commum. Comput.*, (13):209–232, 2002.

- [8] X. Chen, I.S. Reed, T. Helleseth, and T.K. Truong. Algebraic decoding of cyclic codes: a polynomial point of view. *Contemporary Math.*, 168:15–22, 1994.
- [9] X. Chen, I.S. Reed, T. Helleseth, and T.K. Truong. Use of Gröbner bases to decode binary cyclic codes up to the true minimum distance. *IEEE Trans. Inform. Theory*, IT-40:1654–1661, sep 1994.
- [10] A.B. Cooper. Toward a new method of decoding algebraic codes using Gröbner bases. In *Trans. 10th Army Conf. Appl. Math. and Comp.*, pages 1–11, 1993.
- [11] D. Cox, J.Little, and D. O’Shea. *Ideals, Varieties, and Algorithms*. Springer-Verlag, second edition, 1997.
- [12] J. Fitzgerald and R.F. Lax. Decoding affine variety codes using Gröbner bases. *Designs, Codes and Cryptography*, 13:147–158, 1998.
- [13] G.-M. Greuel and G. Pfister. *A SINGULAR Introduction to Commutative Algebra*. Springer-Verlag, 2002.
- [14] G.-M. Greuel, G. Pfister, and H. Schönemann. SINGULAR 3.0. A Computer Algebra System for Polynomial Computations, Centre for Computer Algebra, University of Kaiserslautern, 2005. <http://www.singular.uni-kl.de>.
- [15] C.R.P. Hartmann. Decoding beyond the BCH bound. *IEEE Trans. Inform. Theory*, IT-18:441–444, may 1972.
- [16] C.R.P. Hartmann and K.K. Tzeng. Decoding beyond the BCH bound using multiple sets of syndrome sequences. *IEEE Trans. Inform. Theory*, IT-20:292–295, mar 1974.
- [17] T. Høholdt, J.H. van Lint, and R. Pellikaan. *Algebraic geometry codes*, volume 1, pages 871–961. Elsevier, 1998.
- [18] E. Orsini and M. Sala. Correcting errors and erasures via the syndrome variety. *J. Pure and Appl. Algebra*, (200):191–226, 2005.
- [19] W.W. Peterson and E.J. Weldon. *Error-correcting codes*. MIT Press, 1977.

- [20] S.Bulygin and R.Pellikaan. Bounded distance decoding of linear error-correcting codes with Gröbner bases. *Journal of Symbolic Computation Special Issue Grbner Bases Techniques in Cryptography and Coding Theory*, 2006. Submitted.
- [21] A. Shamir, J. Patarin, N. Cortois, and A. Klimov. *Efficient Algorithms for solving Overdetermined Systems of Multivariate Polynomial Equations*, volume 1807, pages 392–407. 2000. Advances in cryptology - EUROCRYPT'00.
- [22] I.E. Shparlinski. Finding irreducible and primitive polynomials. *Appl. Alg. Engin. Commun. Comp.*, 4:263–268, 1993.
- [23] I.E. Shparlinski. *Finite fields: Theory and computation*, volume 477 of *Mathematics and its Applications*. Kluwer Acad. Publ., 1999.
- [24] Y. Sugiyama, M. Kasahara, S. Hirasawa, and T. Namekawa. A method for solving the key equation for decoding Goppa codes. *Information and Control*, 27:87–99, 1975.
- [25] K.K. Tzeng, C.R.P. Hartmann, and R.T. Chien. Some notes on iterative decoding. In *Proc. 9th Allerton Conf. Circuit and Systems Theory*, oct 1971.