Bounded distance decoding of linear error-correcting codes with Gröbner bases

Stanislav Bulygin

Department of Mathematics, University of Kaiserslautern,P.O. Box 3049, 67653 Kaiserslautern, Germany

Ruud Pellikaan

Department of Mathematics and Computing Science, Eindhoven University of Technology, P.O. Box 513, NL-5600 MB, Eindhoven, The Netherlands

Abstract

The problem of bounded distance decoding of arbitrary linear codes using Gröbner bases is addressed. A new method is proposed, which is based on reducing an initial decoding problem to solving a certain 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. As our experiments suggest, our method is much faster than the one of Fitzgerald-Lax. It is also shown via experiments that the proposed approach in some range of parameters is superior to the generic syndrome decoding.

Key words: decoding, Gröbner basis, linear code, minimum distance, syndrome decoding, system of polynomial equations
1991 MSC: 94B05, 94B35, 13P10

⋆ The first author was funded by "Cluster of Excellence in Rhineland-Palatinate"

Email addresses: bulygin@mathematik.uni-kl.de (Stanislav Bulygin), g.r.pellikaan@tue.nl (Ruud Pellikaan).

URLs: www.mathematik.uni-kl.de/~bulygin/ (Stanislav Bulygin), www.win.tue.nl/~ruudp/ (Ruud Pellikaan).

Preprint submitted to Elsevier Science. Appeared in: Journal of Symbolic Computation 44 (2009) 1626–1643.

1. Introduction

In this paper we consider bounded distance decoding of arbitrary linear codes using Gröbner bases. In recent years a lot of attention was devoted to this question for cyclic codes which form a particular subclass of linear codes. In this paper we consider a method for decoding arbitrary linear codes. 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 Berlekamp (1968); Peterson and Weldon (1977) and Cox et al. (1997); Greuel and Pfister (2002), respectively.

Quite a lot of methods exist for decoding cyclic codes and the literature on this topic is vast. We just mention Arimoto (1961); Berlekamp (1968); Gorenstein and Zierler (1961); Massey (1969); Peterson (1960); Peterson and Weldon (1977); Sugiyama et al. (1975). All these methods are of polynomial complexity and efficient in practice, but do not correct up to the true error-correcting capacity. Techniques using the theory of Gröbner bases were addressed to remedy this problem. These methods can be roughly divided into the following categories:

- Unknown syndromes: (Berlekamp, 1968, pp. 231-240) and Tzeng et al. (1971); Hartmann (1972); Hartmann and Tzeng (1974);
- Newton identities: Augot et al. (1990, 1992, 2002, 2007); Chen et al. (1994c);
- Power sums: Cooper (1990, 1991, 1993); Chen et al. (1994a,c,b); Loustaunau and York (1997); Caboara and Mora (2002); Orsini and Sala (2005).

For arbitrary linear codes some generalizations are known, e.g. Fitzgerald (1996); Fitzgerald and Lax (1998); Borges-Quintana et al. (2005b,c,a); Giorgetti and Sala (2006); Orsini and Sala (2007). Our method is a generalization of the first one of unknown syndromes for arbitrary linear codes.

Finding a Gröbner bases has complexity that is doubly exponential in the number of variables, and it is still exponential in case of a finite number of solutions. Some experiments have been done but it is difficult to estimate the complexity of the decoding algorithms that use Gröbner bases. The existing decoding algorithms of arbitrary linear codes all have complexities that are exponential in the code length, see Barg (1998). The problem turns out to be even harder, as decoding algorithms remain exponential even if one allows unbounded preprocessing, see Bruck and Naor (1990). So far no asymptotic results of decoding algorithms with Gröbner bases are known that are better than the complexity of the existing general decoding algorithms. We continued research in this direction in Bulygin and Pellikaan (2007).

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 $\mathbb{F}[X_1, \ldots X_n]$ over $\mathbb{F}$, 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 $f \in I$. Variables are denoted by capital letters such as X, Y and U, and specific values by x, y and u, respectively. The vectors are denoted in bold, e.g. $\mathbf{u}, \mathbf{v}$. The zero set of I is the set of all solutions of I in $\bar{\mathbb{F}}^n$ and is denoted by $Z(I)$. If I is an ideal in $\mathbb{F}_q[X_1, \ldots X_n]$, then the set of solutions of I over $\mathbb{F}_q$ is denoted by $Z_q(I)$, and the ideal $I + \langle X_i^q - X_i, i = 1, \ldots, n \rangle$ is denoted by I_q. So $Z_q(I) = Z(I) \cap \mathbb{F}_q^n = Z(I_q)$.

2. Syndrome decoding with Gröbner bases

In this section we give a formulation of the well-known syndrome decoding in terms of ideals and solutions of the corresponding systems. Moreover, some results of this section (e.g. Lemma 9) are later used in Section 4, where we look closely on the structure of ideals that we need in our construction for decoding.

Let C be a linear code over $\mathbb{F}_q$ of *length* n, *dimension* k and *minimum distance* d. The parameters of C are denoted by $[n, k, d]$ and its *redundancy* by $r = n - k$. The (true) *error-correcting capacity* $\lfloor (d-1)/2 \rfloor$ of the code is denoted by e. Choose a parity-check matrix H of C. Let $\mathbf{h}_1, \ldots, \mathbf{h}_r$ be the rows of H.

Remark 1. Let $\tilde{C} = \mathbb{F}_{q^m} C$ 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 $C = \mathbb{F}_q^n \cap \tilde{C}$. And H is also a parity check matrix of $\tilde{C}$, since the rank of H does not change under the extension from $\mathbb{F}_q$ to $\mathbb{F}_{q^m}$. Furthermore C and $\tilde{C}$ have the same minimum distance, since this is equal to the minimum number of dependent columns of H, and this does not change under an extension of scalars.

Definition 2. The *(known) syndrome* $\mathbf{s}(H, \mathbf{y})$ of a word $\mathbf{y}$ with respect to H is the column vector $\mathbf{s}(H, \mathbf{y}) = H\mathbf{y}^T$. It has entries $s_i(H, \mathbf{y}) = \mathbf{h}_i \cdot \mathbf{y}$ for $i = 1, \ldots, n-k$. The abbreviations $\mathbf{s}(\mathbf{y})$ and $s_i(\mathbf{y})$ are used for $\mathbf{s}(H, \mathbf{y})$ and $s_i(H, \mathbf{y})$, respectively.

Remark 3. Let $\mathbf{y} = \mathbf{c} + \mathbf{e}$ be a *received word* with $\mathbf{c} \in C$ the codeword that was sent and $\mathbf{e}$ the *error vector*. Then $\mathbf{h}_i \cdot \mathbf{c} = 0$ for all $i = 1, \ldots, r$. So the syndromes of $\mathbf{y}$ and $\mathbf{e}$ with respect to H are equal and known:

$$s_i(\mathbf{y}) := \mathbf{h}_i \cdot \mathbf{y} = \mathbf{h}_i \cdot \mathbf{e} = s_i(\mathbf{e}).$$

Let $\mathbf{h}'_1, \ldots, \mathbf{h}'_n$ be the n columns of H. If furthermore the support of $\mathbf{e}$ is equal to $\{i_1, \ldots, i_t\}$, then

$$\mathbf{s}(\mathbf{y}) = \mathbf{s}(\mathbf{e}) = e_{i_1}\mathbf{h}'_{i_1} + \cdots + e_{i_t}\mathbf{h}'_{i_t}.$$

Therefore, if the distance of a received word to the code is t, then the syndrome vector of the received word is a linear combination of t columns of H. By *syndrome decoding* we mean an algorithm that finds such a linear combination. One way to accomplish this is to go though all possible t-subsets of $\{1, \ldots, n\}$ and see by linear algebra whether a linear combination of the corresponding columns of H gives the syndrome vector. The complexity is therefore $\mathcal{O}(\binom{n}{t}(n-k)t^2)$.
Finding the minimum distance is similar, since we take the syndrome equal to the zero vector, so we try to find the smallest number of columns of H that are linearly dependent.

Definition 4. Let $\mathbf{y} \in \mathbb{F}_q^n$ and let $d(\mathbf{y}, C)$ be the distance of $\mathbf{y}$ to C. A *nearest codeword* of $\mathbf{y}$ to C is an element $\mathbf{c} \in C$ such that $d(\mathbf{y}, \mathbf{c}) = d(\mathbf{y}, C)$. Let $\mathcal{L}(\mathbf{y}, C)$ be the list of nearest codewords of $\mathbf{y}$ to C.

Proposition 5. *Let* $\tilde{C} = \mathbb{F}_{q^m} C$. *If* $\mathbf{y} \in \mathbb{F}_q^n$, *then* $d(\mathbf{y}, C) = d(\mathbf{y}, \tilde{C})$ *and* $\mathcal{L}(\mathbf{y}, C) = \mathcal{L}(\mathbf{y}, \tilde{C})$.

Proof. (1) Now $d(\mathbf{y}, C) \geq d(\mathbf{y}, \tilde{C})$, since $C \subseteq \tilde{C}$. There are $d(\mathbf{y}, \tilde{C})$ columns of H such that an $\mathbb{F}_{q^m}$-linear combination of these columns is equal to $\mathbf{s}(H, \mathbf{y})$. But $\mathbf{y}$ and H have entries in $\mathbb{F}_q$. Hence $d(\mathbf{y}, C) \leq d(\mathbf{y}, \tilde{C})$. Therefore equality holds.

(2) Now $\mathcal{L}(\mathbf{y}, C) \subseteq \mathcal{L}(\mathbf{y}, \tilde{C})$ by (1). Conversely, let $\mathbf{c} \in \mathcal{L}(\mathbf{y}, \tilde{C})$ and $t = d(\mathbf{y}, \tilde{C})$. Let $\mathbf{e} = \mathbf{y} - \mathbf{c}$. Let $I = \{i_1, \ldots, i_t\}$ be the support of $\mathbf{e}$ that is the set of nonzero coordinates of $\mathbf{e}$. Let H_I be the submatrix of H consisting of the columns $h_{i_1}, \ldots, h_{i_t}$. Let $\mathbf{s} = H\mathbf{y}^T$. Then $\mathbf{s}$ is a linear combination of the columns of H_I. So H_I and the extended matrix $[H_I|\mathbf{s}]$ have the same rank. This rank is t, otherwise we would have a proper subset I' of I such that $H_{I'}$ and H_I have the same rank. But this would give an $\mathbf{e}'$ with support I' of weight $t' < t$ and $H\mathbf{e}'^T = \mathbf{s}$. This gives $\mathbf{c}' \in \tilde{C}$ with $\mathbf{y} = \mathbf{c}' + \mathbf{e}'$. So $d(\mathbf{y}, \tilde{C}) \leq t' < t$, a contraction. Hence H_I and the extended matrix $[H_I|\mathbf{s}]$ have the same rank t. So $H_I\mathbf{x}^T = \mathbf{s}$ has a unique solution $\mathbf{x} = (e_{i_1}, \ldots, e_{i_t})$ with entries in $\mathbb{F}_q$. Hence and $\mathbf{c} = \mathbf{y} - \mathbf{e} \in \mathbb{F}_q^n \cap \tilde{C} = C$. Therefore $\mathbf{c} \in \mathcal{L}(\mathbf{y}, C)$. □

Definition 6. Let $h_i(E)$ be the linear function in $\mathbb{F}_q[E_1, \ldots, E_n]$ defined by

$$h_i(E) = \sum_{j=1}^{n} h_{ij} E_j$$

Let $E(\mathbf{y})$ be the ideal in $\mathbb{F}_q[E_1, \ldots, E_n]$ generated by the elements $h_i(E) - s_i(\mathbf{y})$ for all $i = 1, \ldots, n-k$. Let $J(t, n)$ be the ideal in $\mathbb{F}_q[E_1, \ldots, E_n]$ defined by

$$J(t, n) = \bigcap_{1 \leq j_1 < \cdots < j_{n-t} \leq n} \langle E_{j_1}, \ldots, E_{j_{n-t}} \rangle.$$

Let $E(t, \mathbf{y})$ be the ideal generated by $E(\mathbf{y})$ and $J(t, n)$.

Lemma 7.
1) $\mathbf{e}$ *is a solution of* $E(\mathbf{y})$ *if and only if* $\mathbf{y} = \mathbf{c} + \mathbf{e}$ *for some positive integer* m *and* $\mathbf{c} \in \mathbb{F}_{q^m} C$.
2) $\mathbf{e}$ *is a solution of* $J(t, n)$ *if and only if* $wt(\mathbf{e}) \leq t$.
3) Let $t = d(\mathbf{y}, C)$. *Then* $E(w, \mathbf{y})$ *has no solution for all* $w < t$. *And* $\mathbf{e}$ *is a solution of* $E(t, \mathbf{y})$ *if and only if* $\mathbf{y} = \mathbf{c} + \mathbf{e}$ *for some* $\mathbf{c} \in C$ *and* $wt(\mathbf{e}) = t$.

Proof.
1) If $\mathbf{y} = \mathbf{c} + \mathbf{e}$ for some $\mathbf{c} \in \mathbb{F}_{q^m} C$, then $\mathbf{e}$ is a solution of $E(\mathbf{y})$ by Remarks 1 and 3. Conversely, if $\mathbf{e}$ is a solution of $E(\mathbf{y})$, then $\mathbf{s}(\mathbf{y}) = \mathbf{s}(\mathbf{e})$ and $\mathbf{e} \in \mathbb{F}_{q^m}^n$ for some positive integer m. So $\mathbf{s}(\mathbf{y} - \mathbf{e}) = 0$. Hence $\mathbf{c} = \mathbf{y} - \mathbf{e}$ is a codeword of $\mathbb{F}_{q^m} C$ and $\mathbf{y} = \mathbf{c} + \mathbf{e}$.
2) If $\mathrm{wt}(\mathbf{e}) \leq t$, then the support of $\mathbf{e}$ is contained in $\{k_1, \ldots, k_t\}$ for some $\mathbf{k}$. Let $\{j_1, \ldots, j_{n-t}\}$ be the complement of this support. Then $\mathbf{e}$ is a solution of the ideal $\langle E_{j_1}, \ldots, E_{j_{n-t}} \rangle$. So $\mathbf{e}$ is an element of the zero set $Z(\langle E_{j_1}, \ldots, E_{j_{n-t}} \rangle)$. Hence $\mathbf{e}$ is an element of the zero set

$$\bigcup_{1 \leq j_1 < \cdots < j_{n-t} \leq n} Z(\langle E_{j_1}, \ldots, E_{j_{n-t}} \rangle) =$$

$$Z\left(\cap_{1 \leq j_1 < \cdots < j_{n-t} \leq n} \langle E_{j_1}, \ldots, E_{j_{n-t}} \rangle\right) = Z(J(t, n)).$$

So $\mathbf{e}$ is a solution of $J(t, n)$
The converse is proved similarly and is left to the reader.
3) Is a direct consequence of (1) and (2) and Proposition 5. □

Theorem 8. *Let* H *be a parity-check matrix of the code* C. *Let* $\mathbf{y}$ *be a received word. Let* t *be the smallest positive integer such that* $E(t, \mathbf{y})$ *has a solution.*

1) Then the solutions $\mathbf{e}$ *of* $E(t, \mathbf{y})$ *correspond one-to-one to* $\mathbf{c}$ *in* $\mathcal{L}(\mathbf{y}, C)$.
2) If $\mathbf{e}$ *is a solution of* $E(t, \mathbf{y})$ *such that* $wt(\mathbf{e}) \leq (d(C) - 1)/2$, *then* $wt(\mathbf{e}) = t$ *and* $\mathbf{e}$ *is the unique solution.*

Proof. (1) is a direct consequence of Lemma 7 (3).
(2) is a consequence of (1) and the well-known fact that $\mathbf{y}$ has a unique nearest codeword in case $d(\mathbf{y}, C) \leq (d-1)/2$. □

Lemma 9. *Let*

$$I(t, n) = \langle E_{i_1} \cdots E_{i_{t+1}} | 1 \leq i_1 < \cdots < i_{t+1} \leq n \rangle.$$

Then $I(t, n) = J(t, n)$.

Proof. Let $E_{i_1} \cdots E_{i_{t+1}}$ be a generator of the ideal $I(t, n)$ and let $\mathbf{j}$ be an increasing $n-t$ tuple. Then $\{i_1, \ldots, i_{t+1}\}$ and $\{j_1, \ldots, j_{n-t}\}$ are subsets of $\{1, \ldots, n\}$ consisting of $t+1$ and $n-t$ elements, respectively. Hence their intersection is not empty, that is $i_r = j_s$ for some r and s. Hence

$$E_{i_1} \cdots E_{i_{t+1}} \in \langle E_{j_s} \rangle \subseteq \langle E_{j_1}, \ldots, E_{j_{n-t}} \rangle.$$

Hence it is proved that $I(t, n) \subseteq J(t, n)$.
Now consider $J(t, n)/I(t, n)$. Let f be a polynomial in $J(t, n)$. Modulo $I(t, n)$ we may assume that

$$f = \sum_{\mathbf{i}=(i_1,\ldots,i_t), 1 \leq i_1 < \cdots < i_t \leq n} f_{\mathbf{i}} E_{i_1}^{\alpha_{i_1}} \cdots E_{i_t}^{\alpha_{i_t}}.$$

with $f_{\mathbf{i}} \in \mathbb{F}_q$ and α_i are nonnegative integers, which depend on $\mathbf{i}$. For every $\mathbf{i}$ with $1 \leq i_1 < \cdots < i_t \leq n$ there exists exactly one $\mathbf{j}$ such that $1 \leq j_1 < \cdots < j_{n-t} \leq n$ and $\{j_1, \ldots, j_{n-t}\}$ is the complement of $\{i_1, \ldots, i_t\}$ in $\{1, \ldots, n\}$. Now $f \in J(t, n)$. So $f \in \langle E_{j_1}, \ldots, E_{j_{n-t}} \rangle$. This is only possible if $f_{\mathbf{i}} = 0$ since the sets of variables $\{E_{i_1}, \ldots, E_{i_t}\}$ and $\{E_{j_1}, \ldots, E_{j_{n-t}}\}$ are disjoint. So $f_{\mathbf{i}} = 0$ for every such $\mathbf{i}$. Hence $f = 0$. Therefore $J(t, n) \subseteq I(t, n)$. □

Remark 10. The ideal $J(t, n)$ is generated by $\binom{n}{t+1}$ monomials of degree $t+1$, and thus $E(t, \mathbf{y})$ is generated by $n - k$ linear functions and $\binom{n}{t+1}$ monomials of degree $t + 1$.

Example 11. We provide now a small example explaining Theorem 8. Consider a one-error-correcting Hamming code with parameters $[7, 4, 3]$ over $\mathbb{F}_2$. Let $\mathbf{y} = (1, 0, 1, 0, 1, 1, 1)$ be a received word. Let a parity-check matrix be

$$H = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

The ideal $E(1, \mathbf{y})$ is generated by the linear polynomials $E_1 + E_2 + E_4 + E_5, E_1 + E_3 + E_4 + E_6 + 1, E_1 + E_2 + E_3 + E_7 + 1$ and the binomials $E_i E_j, 1 \leq i < j \leq 7$. Now $E(1, \mathbf{y})$ has $(0, 0, 1, 0, 0, 0, 0)$ as the unique solution in the algebraic closure. Moreover, the same situation takes place when we consider a code with the parity-check matrix H over $\mathbb{F}_8$. In particular, one does not need to add field equations in order to avoid spurious solutions.

3. Matrix in MDS form

In this section we introduce the notions of an MDS basis and an unknown syndrome and the corresponding matrix. We establish some properties of the matrix of unknown syndromes.
Let $\mathbf{b}_1, \ldots, \mathbf{b}_n$ be a basis of $\mathbb{F}^n$. Now B is the $n \times n$ matrix with $\mathbf{b}_1, \ldots, \mathbf{b}_n$ as rows.

Definition 12. 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 $i = 1, \ldots, n$.

Remark 13. The matrix B is invertible, since its rank is n. The syndrome $\mathbf{u}(B, \mathbf{e})$ determines the error vector $\mathbf{e}$ uniquely, since

$$B^{-1}\mathbf{u}(B, \mathbf{e}) = B^{-1}B\mathbf{e}^T = \mathbf{e}^T.$$

So the idea is based on finding the unknown syndrome of an error vector with respect to some specific basis B. Then finding the error vector is trivial.
The 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. We have a linear automorphism β of $\bar{\mathbb{F}}^n$, defined by $\beta(\mathbf{e}) = \mathbf{e}B^T$ with inverse map γ. This induces an isomorphism of rings

$$\beta^* : \mathbb{F}[U_1, \ldots, U_n] \longrightarrow \mathbb{F}[E_1, \ldots, E_n],$$

defined by

$$\beta^*(U_i) = \sum_{j=1}^{n} b_{ij} E_j$$

and its inverse γ^*, defined by

$$\gamma^*(E_i) = \sum_{j=1}^{n} c_{ij} U_j,$$

where the c_{ij} are the entries of B^{-1}.

Definition 14. Define the coordinatewise *star product* of two vectors $\mathbf{x}, \mathbf{y} \in \mathbb{F}^n$ by $\mathbf{x} * \mathbf{y} = (x_1 y_1, \ldots, x_n y_n)$. Then $\mathbf{b}_i * \mathbf{b}_j$ is a linear combination of the basis vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$, that is there are constants $\mu_l^{ij} \in \mathbb{F}$ such that

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

The elements $\mu_l^{ij} \in \mathbb{F}$ are called the *structure constants* of the basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$. See Kostrikin and Shafarevich (1990)

Definition 15. Define the $n \times n$ matrix of *(unknown) syndromes* $\mathcal{U}(\mathbf{e})$ of a word $\mathbf{e}$ by $u_{ij}(\mathbf{e}) = (\mathbf{b}_i * \mathbf{b}_j) \cdot \mathbf{e}$.

Remark 16. 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

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

Proposition 17. *The rank of* $\mathcal{U}(\mathbf{e})$ *is equal to the weight of* $\mathbf{e}$.

Proof. See (Høholdt et al., 1998, Lemma 4.7). See also Proposition 25. □

Remark 18. So there are $\mathrm{wt}(\mathbf{e})+1$ columns of $\mathcal{U}(\mathbf{e})$ that are dependent and every w-tuple of columns of $\mathcal{U}(\mathbf{e})$ is independent if $w \leq \mathrm{wt}(\mathbf{e})$. We will look at the smallest t such that the first $t+1$ columns are dependent. For an arbitrary matrix B we have to go through all the w-tuples of columns of $\mathcal{U}(\mathbf{e})$ with $w \leq \mathrm{wt}(\mathbf{e})+1$ 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 19. Let $\mathbf{b}_1, \ldots, \mathbf{b}_n$ be a basis of $\mathbb{F}^n$. Let B_s be the $s \times n$ matrix with $\mathbf{b}_1, \ldots, \mathbf{b}_s$ as rows, so $B = B_n$. We say that $\mathbf{b}_1, \ldots, \mathbf{b}_n$ is an ordered *MDS basis* and B an *MDS matrix* if all the $s \times s$ submatrices of B_s have rank s for all $s = 1, \ldots, n$. Let C_s be the code with B_s as parity-check matrix.

Remark 20. Let B be an MDS matrix. Then C_s is an MDS code for all s. This motivates the name in the previous definition.

Definition 21. Let $\mathbb{F} = \mathbb{F}_q$. Suppose $n \leq q$. Let $\mathbf{x} = (x_1, \ldots, x_n)$ be an n-tuple of pairwise distinct elements in $\mathbb{F}$. Define

$$\mathbf{b}_i = (x_1^{i-1}, \ldots, x_n^{i-1}).$$

Then $\mathbf{b}_1, \ldots, \mathbf{b}_n$ is called an ordered *Vandermonde basis* and the corresponding matrix is denoted by $B(\mathbf{x})$ and called a *Vandermonde matrix*.
In particular, if $\alpha \in \mathbb{F}^*$ is an element of order n and $x_j = \alpha^{j-1}$ for all j, then $\mathbf{b}_1, \ldots, \mathbf{b}_n$ is called an ordered *Reed-Solomon (RS) basis* and the corresponding matrix is called a *RS matrix* and denoted by $B(\alpha)$.

Remark 22. If $\mathbf{b}_1, \ldots, \mathbf{b}_n$ is a Vandermonde basis of $\mathbb{F}^n$, then it is an MDS basis. Note that an RS matrix is symmetric.
For a finite field and general n there is a positive integer m such that $n \leq q^m$. The above construction gives a Vandermonde basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$ of $\mathbb{F}_{q^m}^n$ over $\mathbb{F}_{q^m}$ such that

$$u_{ij}(\mathbf{e}) = u_{i+j-1}(\mathbf{e}) \quad \text{if} \quad i+j \leq n+1.$$

In case n and q are relatively prime, then n divides $q^m - 1$ for some m, and we can take an element $\alpha \in \mathbb{F}_{q^m}^*$ of order n and $x_j = \alpha^{j-1}$ for $i = 1, \ldots, n$ like for cyclic codes. In that case $u_{ij}(\mathbf{e}) = u_{i+j-1}(\mathbf{e})$ for all i, j modulo n.

Remark 23. Let $\tilde{C} = \mathbb{F}_{q^m} C$ 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 by Remark 1.
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 Shparlinski (1993, 1999). 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.
Thus the code $\tilde{C}$ can be efficiently realized for a given C.

Definition 24. Let M be a matrix with entry m_{ij} in row i and column j. Then M_v is the submatrix of M consisting of the first v columns, and M_{uv} is the $u \times v$ submatrix of M given by

$$M_{uv} = \begin{pmatrix} m_{11} & m_{12} & \dots & m_{1v} \\ m_{21} & m_{22} & \dots & m_{2v} \\ \vdots & \vdots & \ddots & \vdots \\ m_{u1} & m_{u2} & \dots & m_{uv} \end{pmatrix}.$$

Proposition 25. *Suppose that B is an MDS matrix. Let $w = wt(\mathbf{e})$. Then*

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

Proof. We have that

$$u_{ij}(\mathbf{e}) = (\mathbf{b}_i * \mathbf{b}_j) \cdot \mathbf{e} = \sum_{l=1}^{n} b_{il} e_l b_{jl}.$$

Hence

$$\mathcal{U}_{nv}(\mathbf{e}) = BD(\mathbf{e})B_v^T,$$

where $D(\mathbf{e})$ is the diagonal matrix with $\mathbf{e}$ on the diagonal. This triple product implies that $\text{rank}(\mathcal{U}_{nv}(\mathbf{e})) \leq \min\{v, w\}$, since $\text{rank}(B) = n$, $\text{rank}(B_v) = v$ and $\text{rank}(D(\mathbf{e})) = w$. We may assume without loss of generality that the nonzero entries of $\mathbf{e}$ are at the beginning, since B stays an MDS matrix after a permutation of its columns. So the non-zero entries are $e_1, \dots, e_w$. Let $\mathbf{e}' = (e_1, \dots, e_w)$. Then $BD(\mathbf{e})B_v^T$ has $B_w D(\mathbf{e}')B_{vw}^T$ as a submatrix. Now $D(\mathbf{e}')$ is invertible, since all the coordinates of $\mathbf{e}'$ are nonzero. Hence $B_w D(\mathbf{e})B_v^T$ has the same rank as $B_w B_{vw}^T$. Now B_{ww} is invertible, since B is an MDS matrix. Hence $B_w B_{vw}^T$ has the same rank as B_{vw}^T. But $\text{rank}(B_{vw}) = \min\{v, w\}$, again since B is MDS. Therefore $\text{rank}(\mathcal{U}_{nv}(\mathbf{e})) \geq \min\{v, w\}$. □

4. Determinantal variety of syndromes

In the previous section it is shown that $\mathcal{U}_{nv}(\mathbf{e})$ has rank v if $v \leq \text{wt}(\mathbf{e})$, and its rank is $\text{wt}(\mathbf{e})$ if $v > \text{wt}(\mathbf{e})$. We see that the first moment of stabilization of the rank of $\mathcal{U}_{nv}(\mathbf{e})$ yields the weight of $\mathbf{e}$. We would like to be able to find this moment. For this we change all the entries of $\mathcal{U}_{nv}(\mathbf{e})$ to variables and search for linear dependence of columns, see Definitions 26 and 39. The corresponding results are developed in this section. It turns out that the study of the corresponding ideal also gives an opportunity to find a vector of unknown syndromes $\mathbf{u}$.

Definition 26. Let B be an MDS matrix with structure constants μ_l^{ij}. Define the linear functions U_{ij} in the variables $U_1, \dots, U_n$ by

$$U_{ij} = \sum_{l=1}^{n} \mu_l^{ij} U_l.$$

Let $\mathcal{U}$ be the $n \times n$ matrix with entries U_{ij}.

Remark 27. If $U_i = u_i(\mathbf{e})$ for all i, then $U_{ij} = u_{ij}(\mathbf{e})$ for all i, j. So the matrix above exactly reflects the idea stated at the beginning of this section.

Definition 28. Let $\mathbf{b}'_1, \ldots, \mathbf{b}'_n$ be the columns of B. Let $\mathbf{i} = (i_1, \ldots, i_t)$ with $1 \leq i_1 < \cdots < i_t \leq n$. Let $L(\mathbf{i})$ be the linear subspace of the vector space $\bar{\mathbb{F}}^n$ generated by $\mathbf{b}'_{i_1}, \ldots, \mathbf{b}'_{i_t}$. That is

$$L(\mathbf{i}) = \{\ x_1\mathbf{b}'_{i_1} + \cdots + x_t\mathbf{b}'_{i_t} \mid x_1, \ldots, x_t \in \bar{\mathbb{F}}\ \}.$$

Let $I(\mathbf{i})$ be the defining ideal of $L(\mathbf{i})$ in $\mathbb{F}[U_1, \ldots, U_n]$. That is

$$I(\mathbf{i}) = \{\ f(U) \in \mathbb{F}[U_1, \ldots, U_n] \mid f(\mathbf{u}) = 0 \text{ for all } \mathbf{u} \in L(\mathbf{i})\ \}.$$

Lemma 29. *Let $\mathbf{k}$ be a t-tuple of increasing entries and let $\{j_1, \ldots, j_{n-t}\}$ be the complement of $\{k_1, \ldots, k_t\}$ in $\{1, \ldots, n\}$. Then $L(\mathbf{k})$ has dimension t and the ideal $I(\mathbf{k})$ is a radical ideal generated by the $n-t$ linear functions $\gamma^*(E_{j_1}), \ldots, \gamma^*(E_{j_{n-t}})$ in the variables $U_1, \ldots, U_n$.*

Proof. The dimension of $L(\mathbf{k})$ follows form Definition 28 and the fact that $\mathbf{b}'_1, \ldots, \mathbf{b}'_n$ are independent. Now $\mathbf{u} = \mathbf{u}(\mathbf{e}) = B\mathbf{e}^T = e_1\mathbf{b}'_1 + \cdots + e_n\mathbf{b}'_n$. Furthermore $\mathrm{wt}(\mathbf{e}) \leq t$ if and only if the support of $\mathbf{e}$ is contained in $\{k_1, \ldots, k_t\}$ for some $\mathbf{k}$ with $1 \leq k_1 < \cdots < k_t \leq n$. Let β and γ be the maps of Remark 13. Then $\mathbf{u} \in I(\mathbf{k})$ if and only if $\mathbf{e} = \gamma(\mathbf{u})$ and $e_{j_1} = \cdots = e_{j_{n-t}} = 0$. So $\beta^*(I(\mathbf{k})) = \langle E_{j_1}, \ldots, E_{j_{n-t}} \rangle$ is a radical ideal. Hence the ideal $I(\mathbf{k})$ is also radical and generated by the $n-t$ linear functions $\gamma^*(E_{j_1}), \ldots, \gamma^*(E_{j_{n-t}})$ in the variables $U_1, \ldots, U_n$, since β^* is an isomorphism with inverse γ^*. $\square$

Remark 30. If $\mathbf{i} = (i_1, \ldots, i_t)$, $\mathbf{j} = (j_1, \ldots, i_u)$ and $\mathbf{k} = (k_1, \ldots, k_v)$ consist of increasing entries such that $\{i_1, \ldots, i_t\} \cap \{j_1, \ldots, i_u\} = \{k_1, \ldots, k_v\}$, then $L(\mathbf{i}) \cap L(\mathbf{j}) = L(\mathbf{k})$. This fact is left to the reader to check.

Definition 31. Let $\mathcal{V}$ be an $l \times m$ matrix with entries in $\mathbb{F}[U_1, \ldots, U_n]$. 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 $\bar{\mathbb{F}}^n$.

Remark 32. The ideal $I(t, \mathcal{V})$ is invariant under elementary row operations and elementary column operations on the first $t+1$ columns. In particular $I(t, \mathcal{V}) = I(t, \mathcal{S}\mathcal{V})$ if $\mathcal{V}$ is an $l \times m$ matrix and $\mathcal{S}$ is an invertible $l \times l$ matrix. See Bruns and Vetter (1988).

Remark 33. Let $\mathbf{u} \in \bar{\mathbb{F}}^n$. The rank of $\mathcal{V}_{l,t+1}$ at $\mathbf{u}$ is at most t if and only if $\mathbf{u} \in Z(t, \mathcal{V})$. See Bruns and Vetter (1988).

Theorem 34. *The variety $Z(t,\mathcal{U})$ is the union of the $\binom{n}{t}$ irreducible components $L(\mathbf{k})$ with $1 \leq k_1 < \cdots < k_t \leq n$. Furthermore $I(t,\mathcal{U})$ is a radical ideal with*

$$I(t,\mathcal{U}) = \bigcap_{1 \leq k_1 < \cdots < k_t \leq n} I(\mathbf{k}).$$

Proof. Let $\mathbf{u} \in \bar{\mathbb{F}}^n$ and $U_i = u_i$ for all i. Then $\mathbf{u} = \mathbf{u}(\mathbf{e})$ for some $\mathbf{e} \in \bar{\mathbb{F}}^n$ by Remark 13. Hence $U_{ij} = u_{ij}(\mathbf{e})$ by Remark 27. Now $\mathbf{u} \in Z(t,\mathcal{U})$ if and only if $\operatorname{rank}(\mathcal{U}_{n,t+1}(\mathbf{e})) \leq t$. But $\operatorname{rank}(\mathcal{U}_{n,t+1}(\mathbf{e}))$ is equal to $\min\{t+1, \operatorname{wt}(\mathbf{e})\}$ by Proposition 25. Hence $\mathbf{u} \in Z(t,\mathcal{U})$ if and only if $\operatorname{wt}(\mathbf{e}) \leq t$. Now $\mathbf{u} = \mathbf{u}(\mathbf{e}) = B\mathbf{e}^T = e_1\mathbf{b}'_1 + \cdots + e_n\mathbf{b}'_n$. Furthermore $\operatorname{wt}(\mathbf{e}) \leq t$ if and only if the support of $\mathbf{e}$ is contained in $\{k_1, \ldots, k_t\}$ for some $\mathbf{k}$ with $1 \leq k_1 < \cdots < k_t \leq n$. Therefore $\mathbf{u} \in Z(t,\mathcal{U})$ if and only if $\mathbf{u} \in L(\mathbf{k})$ for some t-tuple $\mathbf{k}$ with increasing entries by Lemma 29. Note that a linear space is irreducible. Hence $Z(t,\mathcal{U})$ is the union of the $\binom{n}{t}$ irreducible components $L(\mathbf{k})$.
Let $D(E)$ be the diagonal matrix with the variables $E_1, \ldots, E_n$ on the diagonal. Then the componentwise application of β^* to the entries of $\mathcal{U}$ yields

$$\beta^*(\mathcal{U}) = BD(E)B^T,$$

because

$$\beta^*(U_{ij}) = \beta^*\left(\sum_{l=1}^{n} \mu_l^{ij} U_l\right) = \sum_{l=1}^{n}\sum_{l'=1}^{n} \mu_l^{ij} b_{ll'} E_{l'} = \sum_{l'=1}^{n} b_{il'} b_{jl'} E_{l'},$$

since $\mathbf{b}_i * \mathbf{b}_j = \sum_{l=1}^{n} \mu_l^{ij} \mathbf{b}_l$.
Remark 32 yields

$$I(t,\mathcal{U}) = I(t,\mathcal{U}_{n,t+1}) = I(t, B^{-1}\mathcal{U}_{n,t+1}).$$

Now $\beta^*(\mathcal{U}_{n,t+1}) = BD(E)B_{t+1}^T$. So $\beta^*(B^{-1}\mathcal{U}_{n,t+1}) = D(E)B_{t+1}^T$. Let $\mathbf{i}$ be an $(t+1)$-tuple with $1 \leq i_1 < \cdots < i_{t+1} \leq n$. Then the $(t+1) \times (t+1)$ minor of $\beta^*(B^{-1}\mathcal{U}_{n,t+1})$ consisting of the rows indexed by $\mathbf{i}$ is up to a nonzero scalar equal to $E_{i_1} \cdots E_{i_{t+1}}$, since all the $(t+1) \times (t+1)$ submatrices of B_{t+1} have rank $t+1$. Therefore $\beta^*(I(t,\mathcal{U}))$ is generated by all $(t+1)$-fold products $E_{i_1} \cdots E_{i_{t+1}}$. So

$$\beta^*(I(t,\mathcal{U})) = \bigcap_{1 \leq j_1 < \cdots < j_{n-t} \leq n} \langle E_{j_1}, \ldots, E_{j_{n-t}} \rangle$$

by Lemma 9. The inverse of the map β^* is γ^* by Remark 13. Hence

$$I(t,\mathcal{U}) = \bigcap_{1 \leq j_1 < \cdots < j_{n-t} \leq n} \langle \gamma^*(E_{j_1}), \ldots, \gamma^*(E_{j_{n-t}}) \rangle = \bigcap_{1 \leq k_1 < \cdots < k_t \leq n} I(\mathbf{k})$$

by Lemma 29. Therefore $I(t,\mathcal{U})$ is radical, since it is an intersection of radical ideals. □

Remark 35. The ideal $I(t,\mathcal{U})$ is equal to $\gamma^*(I(t,n))$ and is generated by $\binom{n}{t+1}$ homogeneous polynomials of degree $t+1$. See also Lemma 9 and Remark 10.

Remark 36. 1) For definitions and properties of determinantal ideals, rings and varieties we refer to the early work of Room (1938) and the more recent books Bruns and Vetter (1988); Eisenbud (1995). Determinantal rings are Cohen-Macaulay by Eagon and Hochster, see (Eisenbud, 1995, Theorem 18.18). Consequently determinantal ideals are unmixed (Eisenbud, 1995, Corollary 18.14), that is all associated primes are minimal and have the same codimension, in particular there are no embedded primes (Eisenbud, 1995, §3.1).
2) In the case of Theorem 34 the ideal $I(t,\mathcal{U})$ is generated by the $t+1$ minors of a the $n \times (t+1)$ matrix $\mathcal{U}_{n,t+1}$ Hence the codimension of its zero set $Z(t,\mathcal{U})$ is at most $n - (t+1) - 1$. But all components of $Z(t,\mathcal{U})$ have in fact codimension $n - t$. Hence

$I(t,\mathcal{U})$ is a determinantal ideal and therefore Cohen-Macaulay and unmixed. The associated primes of $I(t,\mathcal{U})$ are minimal and have the same codimension $n-t$. The minimal primes are the ideals $I(\mathbf{k})$.
3) The $(t+1)\times(t+1)$ minors of a generic matrix $m\times n$ matrix X form a reduced Gröbner basis of the ideal generated by these minors, with respect to a certain lexicographic term order. See Sturmfels (1990). We think that a similar statement holds for $I(t,\mathcal{U})$ and leave this as an open question.
4) The case that the matrix $\mathcal{U}$ is "Hankel", "Toeplitz" or "Catalecticant", that is where the entries of $\mathcal{U}$ are constant along diagonals: $U_{ij} = U_{i+j-1}$, is treated in Eisenbud (1988).

Proposition 37. *If $t < n$, then the singular locus of $Z(t,\mathcal{U})$ is $Z(t-1,\mathcal{U})$.*

Proof. For the notion of singular and regular point we refer to (Eisenbud, 1995, §16.6). Every component $L(\mathbf{i})$ of $Z(t,\mathcal{U})$ is nonsingular, since it is a linear subspace. Hence the singular locus of $Z(t,\mathcal{U})$ is the union of all the intersections of two distinct components. If $\mathbf{i} = (i_1,\ldots,i_t)$ and $\mathbf{j} = (j_1,\ldots,i_t)$ consist of increasing entries, such that $\{i_1,\ldots,i_t\}\cap\{j_1,\ldots,i_t\} = \{k_1,\ldots,k_v\}$ with $\mathbf{k} = (k_1,\ldots,k_v)$, then $L(\mathbf{i})\cap L(\mathbf{j}) = L(\mathbf{k})$ by Remark 30. If moreover $\mathbf{i}\neq\mathbf{j}$, then $v \leq t-1$ and $L(\mathbf{i})\cap L(\mathbf{j}) \subseteq Z(t-1,\mathcal{U})$.
Conversely, let $L(\mathbf{k})$ be a component of $Z(t-1,\mathcal{U})$ with $\mathbf{k} = (k_1,\ldots,k_{t-1})$. Then $\{i_1,\ldots,i_t\}\cap\{j_1,\ldots,i_t\} = \{k_1,\ldots,k_{t-1}\}$ for some $\mathbf{i} = (i_1,\ldots,i_t)$ and $\mathbf{j} = (j_1,\ldots,i_t)$, since $t < n$. Hence $L(\mathbf{k}) = L(\mathbf{i})\cap L(\mathbf{j})$ is in the singular locus of $Z(t,\mathcal{U})$. □

Example 38. Let α be an element of $\mathbb{F}_4^*$ of order 3. Let B be the RS matrix with rows $\mathbf{b}_1 = (1,1,1)$, $\mathbf{b}_2 = (1,\alpha,\alpha^2)$ and $\mathbf{b}_3 = (1,\alpha^2,\alpha)$. The matrix $\mathcal{U}$ is of the form (cf. Remark 22)

$$\begin{pmatrix} U_1 & U_2 & U_3 \\ U_2 & U_3 & U_1 \\ U_3 & U_1 & U_2 \end{pmatrix}.$$

If $t = 0$, then $Z(0,\mathcal{U})$ consists of the origin and indeed

$$I(0,\mathcal{U}) = \langle U_1, U_2, U_3\rangle.$$

For $t = 1$ we have that $Z(1,\mathcal{U})$ is the union of the lines $L(1)$, $L(2)$ and $L(3)$ through the origin with directions $\mathbf{b}_1'$, $\mathbf{b}_2'$ and $\mathbf{b}_3'$, respectively, given by the columns of B. And

$$I(1,\mathcal{U}) = \langle U_2^2 - U_1U_3, U_1^2 - U_2U_3, U_3^2 - U_1U_2\rangle.$$

In case $t = 2$ we have that $Z(2,\mathcal{U})$ is the union of the planes $L(1,2)$, $L(1,3)$ and $L(2,3)$, where $L(i,j)$ is the plane through the origin generated by $\mathbf{b}_i'$ and $\mathbf{b}_j'$. The corresponding ideals are $I(1,2) = \langle U_1 + \alpha U_2 + \alpha^2 U_3\rangle$, $I(1,3) = \langle U_1 + \alpha^2 U_2 + \alpha U_3\rangle$ and $I(2,3) = \langle U_1 + U_2 + U_3\rangle$, respectively. Furthermore

$$I(2,\mathcal{U}) = \langle U_1^3 + U_2^3 + U_3^3 + U_1U_2U_3\rangle.$$

Indeed we have that

$$I(2,\mathcal{U}) = I(1,2)\cap I(1,3)\cap I(2,3),$$

since

$$U_1^3 + U_2^3 + U_3^3 + U_1U_2U_3 = (U_1 + \alpha U_2 + \alpha^2 U_3)(U_1 + \alpha^2 U_2 + \alpha U_3)(U_1 + U_2 + U_3).$$

Definition 39. The ideal $I(t,\mathcal{U},V)$ in the ring $\mathbb{F}_q[U_1,\ldots,U_n,V_1,\ldots,V_t]$ is generated by the elements

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

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

Remark 40. For every $\mathbf{u}$ there is a unique $\mathbf{e}$ such that $\mathbf{u}=\mathbf{u}(\mathbf{e})$ by Remark 13. By evaluating $\mathcal{U}$ at $\mathbf{u}(\mathbf{e})$ we see that $(\mathbf{u},\mathbf{v})$ is an element of $Z(t,\mathcal{U},V))$ for some $\mathbf{v}$ if and only if the $(t+1)$-th column of $\mathcal{U}(\mathbf{e})$ is a linear combination of the first t columns of $\mathcal{U}(\mathbf{e})$.

Lemma 41. *Let $\mathbf{u}=\mathbf{u}(\mathbf{e})$. If $\mathbf{u}\in Z(t,\mathcal{U})$, then there is a $t'\le t$ and a $\mathbf{v}$ such that $(\mathbf{u},\mathbf{v})\in Z(t',\mathcal{U},V)$.*

Proof. Suppose $\mathbf{u}\in Z(t,\mathcal{U})$. Then $\operatorname{rank}(\mathcal{U}_{n,t+1}(\mathbf{e}))\le t$ by Remark 33. So the first $t+1$ columns of $\mathcal{U}(\mathbf{e})$ are linearly dependent. Hence there is a $t'\le t$ such that the $(t'+1)$-th column of $\mathcal{U}(\mathbf{e})$ is a linear combination of the first t' columns of $\mathcal{U}(\mathbf{e})$. Therefore $(\mathbf{u},\mathbf{v})$ is an element of $Z(t',\mathcal{U},V)$ for some $\mathbf{v}$, by Remark 40. □

Proposition 42.

$$I(t,\mathcal{U})\subseteq I(t,\mathcal{U},V).$$

Proof. Let R_t be the factor ring $\mathbb{F}[U_1,\ldots,U_n,V_1,\ldots,V_t]/I(t,\mathcal{U},V)$. Then the following equations hold in the ring R_t

$$\sum_{l=1}^{t} U_{il}V_l - U_{it+1}=0 \quad \text{for all } i=1,\ldots,n.$$

Let Δ_l be the determinant of the $t\times t$ submatrix of $\mathcal{U}_{t,t+1}$ obtained by deleting the l-th column. Then

$$\Delta_{t+1}V_l=(-1)^{t+l}\Delta_l \quad \text{for all } l=1,\ldots,t,$$

by Cramer's rule, which holds in this form for a system of linear equations with entries in any commutative ring with unit element (Lang, 1993, XIII, §4). Now $\det(\mathcal{U}_{t+1,t+1})$ is a generating element of $I(t,\mathcal{U})$ and the cofactor expansion this determinant along the last row is

$$\det(\mathcal{U}_{t+1,t+1})=\sum_{l=1}^{t} U_{t+1,l}(-1)^{t+1+l}\Delta_l + U_{t+1,t+1}\Delta_{t+1}$$

which is equal to

$$\sum_{l=1}^{t} -U_{t+1,l}\Delta_{t+1}V_l + U_{t+1,t+1}\Delta_{t+1} = -\Delta_{t+1}\left(\sum_{l=1}^{t} U_{t+1,l}V_l - U_{t+1,t+1}\right)=0$$

in R_t. Hence $\det(\mathcal{U}_{t+1,t+1})\in I(t,\mathcal{U},V)$.
This holds similarly for any $(t+1)\times(t+1)$ minor of $\mathcal{U}_{n,t+1}$. □

Example 43. This is a continuation of Example 38. Suppose that $(\mathbf{u}, \mathbf{v})$ is a solution of the following system of equations.

$$\begin{cases} U_1V_1 + U_2V_2 = U_3 \\ U_2V_1 + U_3V_2 = U_1 \\ U_3V_1 + U_1V_2 = U_2 \end{cases}$$

0) If $\mathbf{u} \in Z(0,\mathcal{U})$, then $\mathbf{u} = 0$. In this case $\mathbf{v}$ is free to choose and the component of $Z(t,\mathcal{U},V)$ above $Z(0,\mathcal{U})$ is the set $\{0\} \times \bar{\mathbb{F}}^2$, where $\mathbb{F} = \mathbb{F}_4$.
1) If $\mathbf{u} \in Z(1,\mathcal{U}) \setminus Z(0,\mathcal{U})$, then $u_i \neq 0$ and $u_i^2 = u_{i-1}u_{i+1}$ for all i where the indices are counted modulo 3. Gaussian elimination of the extended matrix associated with the system of equations gives

$$\left(\begin{array}{cc|c} u_1 & u_2 & u_3 \\ u_2 & u_3 & u_1 \\ u_3 & u_1 & u_2 \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & u_2/u_1 & u_3/u_1 \\ 0 & (u_1u_3 - u_2^2)/u_1 & (u_1^2 - u_2u_3)/u_1 \\ 0 & (u_1^2 - u_2u_3)/u_1 & (u_1u_2 - u_3^2)/u_1 \end{array}\right).$$

The last two rows are in fact zero. Hence $v_1 = (u_3 - u_2v_2)/u_1$, where v_2 is free to choose.
2) Now suppose that $\mathbf{u} \in Z(2,\mathcal{U}) \setminus Z(1,\mathcal{U})$. Let $d_i = u_i^2 - u_{i-1}u_{i+1}$ and $d = u_1d_1 + u_2d_2 + u_3d_3$. Then $d = 0$ and $d_i \neq 0$ for some i. Suppose for instance that $d_2 \neq 0$. Then Gaussian elimination yields

$$\left(\begin{array}{cc|c} u_1 & u_2 & u_3 \\ u_2 & u_3 & u_1 \\ u_3 & u_1 & u_2 \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & 0 & -d_3/d_2 \\ 0 & 1 & -d_1/d_2 \\ 0 & 0 & d/d_2 \end{array}\right).$$

The element in the right lower corner is $d/d_2 = 0$. Hence the unique solution for $\mathbf{v}$ is given by $v_1 = -d_3/d_2$ and $v_2 = -d_1/d_2$.

5. 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 $\mathbf{b}_1, \ldots, \mathbf{b}_n$ 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 an $r \times n$ parity-check matrix H of C with $r = n - k$. The row $\mathbf{h}_i$ of H is a linear combination of the basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$, 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 44. 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 as noted in Remark 3 and they can be expressed in the unknown syndromes of $\mathbf{e}$ with respect to B:

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

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

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

Let $J(t, \mathbf{y})$ be the ideal in $\mathbb{F}_q[U_1, \ldots, U_n, V_1, \ldots, V_t]$ generated by $J(\mathbf{y})$ and $I(t,\mathcal{U},V)$ from Definition 39.

Remark 46. The ideal $J(t, \mathbf{y})$ is generated by $n - k$ linear functions and n quadratic polynomials. In principle, we can also express some $n - k$ variables, say $U_{k+1}, \ldots, U_n$, via k others, say $U_1, \ldots, U_k$, using the parity-check matrix H, and then substitute in the quadratic part. In this way we obtain an ideal generated by n quadratic polynomials in $k + t$ variables.

Lemma 47. *If $\mathbf{y} = \mathbf{c} + \mathbf{e}$ for some $\mathbf{c} \in C$ and $wt(\mathbf{e}) = t$, then there is a $\mathbf{v}$ such that $(\mathbf{u}(\mathbf{e}), \mathbf{v})$ is a solution of $J(t, \mathbf{y})$.*

Proof. Let $\mathbf{y} = \mathbf{c} + \mathbf{e}$ for some $\mathbf{c} \in C$ and $\mathbf{u} = \mathbf{u}(\mathbf{e})$. Then $\mathbf{u}$ is a solution of $J(\mathbf{y})$ by Remark 44. If we evaluate $\mathcal{U}$ at $\mathbf{u}(\mathbf{e})$ we see that $\operatorname{rank}(\mathcal{U}_{nv}(\mathbf{e})) = \min\{v, \operatorname{wt}(\mathbf{e})\}$ by Proposition 25. Let $\operatorname{wt}(\mathbf{e}) = t$. Then $\operatorname{rank}(\mathcal{U}_{nv}) = v$ if $v < t$ and $\operatorname{rank}(\mathcal{U}_{nv}) = t$ if $v \geq t$. So the $(t + 1)$-th column of $\mathcal{U}_{n,t+1}$ is a linear combination of the first t columns of $\mathcal{U}$. Hence there is a $\mathbf{v}$ such that $(\mathbf{u}, \mathbf{v})$ is a solution of $I(t,\mathcal{U},V)$, by Remark 40. Hence $(\mathbf{u}, \mathbf{v})$ is a solution of $J(t, \mathbf{y})$. □

Lemma 48. *Let $(\mathbf{u}, \mathbf{v})$ be a solution of $J(t, \mathbf{y})$. Then there is a unique $\mathbf{e}$ of weight at most t such that $\mathbf{u} = \mathbf{u}(\mathbf{e})$, furthermore $\mathbf{y} = \mathbf{c} + \mathbf{e}$ for some $\mathbf{c}$ in $\mathbb{F}_{q^m}C$.*

Proof. Let $(\mathbf{u}, \mathbf{v})$ be a solution of $J(t, \mathbf{y})$. Then there is a unique $\mathbf{e}$ such that $\mathbf{u} = \mathbf{u}(\mathbf{e})$ by Remark 13.
The element $\mathbf{u}$ in $\mathbb{F}_{q^m}^n$ is a solution of $J(\mathbf{y})$. Hence $s_i(\mathbf{y}) = \sum_{j=1}^{n} a_{ij} u_j(\mathbf{e})$ for all i. But $s_i(\mathbf{e}) = \sum_{j=1}^{n} a_{ij} u_j(\mathbf{e})$ for all i, and $\mathbf{u} = \mathbf{u}(\mathbf{e})$. So $\mathbf{s}(\mathbf{y} - \mathbf{e}) = 0$. Hence there is a $\mathbf{c}$ in $\mathbb{F}_{q^m}C$ such that $\mathbf{y} = \mathbf{c} + \mathbf{e}$.
Now $(\mathbf{u}, \mathbf{v})$ is a solution of $I(t,\mathcal{U},V)$. Hence the $(t + 1)$-th column of $\mathcal{U}(\mathbf{e})$ is a linear combination of the first t columns of $\mathcal{U}(\mathbf{e})$, by Remark 40. Therefore $\operatorname{rank}(\mathcal{U}_{n,t+1}(\mathbf{e})) \leq t$. But $\operatorname{rank}(\mathcal{U}_{n,t+1}(\mathbf{e})) = \min\{t + 1, \operatorname{wt}(\mathbf{e})\}$ by Proposition 25. Hence $\operatorname{wt}(\mathbf{e}) \leq t$. □

Lemma 49. *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 $\mathbf{y}$ in $\mathbb{F}_{q^m}C$ for some m.*

Proof. Let $(\mathbf{u}, \mathbf{v})$ and $(\mathbf{u}, \mathbf{w})$ be distinct solutions of $J(t, \mathbf{y})$. Then $\mathbf{u}$ is a solution of $J(\mathbf{y})$ and $(\mathbf{u}, \mathbf{v})$ and $(\mathbf{u}, \mathbf{w})$ are solutions of $I(t, \mathcal{U}, V)$. There is a unique $\mathbf{e}$ such that $\mathbf{u} = \mathbf{u}(\mathbf{e})$. Hence

$$\sum_{j=1}^{t} u_{ij} v_j = u_{i,t+1} \quad \text{and} \quad \sum_{j=1}^{t} u_{ij} w_j = u_{i,t+1} \quad \text{for all } i.$$

So

$$\sum_{j=1}^{t} u_{ij}(v_j - w_j) = 0 \text{ for all } i,$$

and $\mathbf{v} - \mathbf{w} \neq 0$, since $\mathbf{v} \neq \mathbf{w}$. Hence the first t columns of the matrix $\mathcal{U}(\mathbf{e})$ are linearly dependent. Therefore there is a $t' < t$ such that column $t' + 1$ is a linear combination of the first t' columns. In other words there is a solution $(\mathbf{u}, \mathbf{z})$ of $J(t', \mathbf{y})$ by Remark 40. If $t' = 0$, then $\mathbf{u} = \mathbf{u}(\mathbf{e})$ for a unique $\mathbf{e}$ and $\mathbf{y} = \mathbf{c} + \mathbf{e}$ for some $\mathbf{c}$ in $\mathbb{F}_{q^m} C$ and $\mathrm{wt}(\mathbf{e}) \leq 0$, by Lemma 48. Hence $\mathbf{y}$ in $\mathbb{F}_{q^m} C$ for some m. $\square$

Theorem 50. *Let B be an MDS matrix with structure constants μ_l^{ij} and linear functions U_{ij}. Let H be a parity-check matrix of the code C. Let A be the matrix 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 $wt(\mathbf{e})$ 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 $wt(\mathbf{e}) = t$ 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 $J(\mathrm{wt}(\mathbf{e}), \mathbf{y})$ by Lemma 47.
2) Suppose that t is the smallest positive integer such that $J(t, \mathbf{y})$ has a solution over $\bar{\mathbb{F}}_q$. Then $t \leq \mathrm{wt}(\mathbf{e})$ by (1).
Suppose that $(\tilde{\mathbf{u}}, \tilde{\mathbf{v}})$ is a solution. Then there is a unique $\tilde{\mathbf{e}} \in \mathbb{F}_{q^m}^n$ for some m such that $\tilde{\mathbf{u}} = \mathbf{u}(\tilde{\mathbf{e}})$. Let $\tilde{C} = \mathbb{F}_{q^m} C$. Then $\mathbf{y} = \tilde{\mathbf{c}} + \tilde{\mathbf{e}}$ for some $\tilde{\mathbf{c}} \in \tilde{C}$ and $\mathrm{wt}(\tilde{\mathbf{e}}) \leq t$ by Lemma 48. Now $\mathbf{s}(\tilde{\mathbf{e}}) = \mathbf{s}(\mathbf{y}) = \mathbf{s}(\mathbf{e})$. Hence $\tilde{\mathbf{e}} - \mathbf{e}$ is a codeword of $\tilde{C}$. Now C and $\tilde{C}$ have the same minimum distance by Remark 1. By assumption we have that $\mathrm{wt}(\mathbf{e}) \leq (d(\tilde{C}) - 1)/2$. The minimality of t implies $\mathrm{wt}(\tilde{\mathbf{e}}) \leq t \leq \mathrm{wt}(\mathbf{e})$. Hence $\tilde{\mathbf{e}} - \mathbf{e}$ is a codeword $\tilde{C}$ of weight strictly smaller than $d(\tilde{C})$. So $\tilde{\mathbf{e}} = \mathbf{e}$. Therefore, for every solution $(\tilde{\mathbf{u}}, \tilde{\mathbf{v}})$ we have $\tilde{\mathbf{u}} = \mathbf{u}(\mathbf{e})$. Thus we have proved that the $\mathbf{u}$-part is unique.
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 49, since $\mathbf{y}$ is not a codeword. This contradicts the minimality of t. Hence the solution is unique. $\square$

Theorem 51. *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 $wt(\mathbf{e})$ 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 is*

$$\begin{aligned} &U_i - u_i(\boldsymbol{e}), i = 1, \ldots, n, \\ &\quad V_j - v_j, j = 1, \ldots, t, \end{aligned}$$

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

Proof. There is a unique solution $(\mathbf{u}, \mathbf{v})$ with $\mathbf{u} = \mathbf{u}(\mathbf{e})$ and $\mathrm{wt}(\mathbf{e}) = t$, by Theorem 50. So $(\mathbf{u}, \mathbf{v}) \in Z(t,\mathcal{U}, V)$. Hence $\mathbf{u} \in Z(t,\mathcal{U})$ by Proposition 42. So there is a $\mathbf{k}$ with $1 \leq k_1 < \cdots < k_t \leq n$ such that $\mathbf{u} \in L(\mathbf{k})$ by Theorem 34. If there is another such $\mathbf{k}'$ with $\mathbf{u} \in L(\mathbf{k}')$, then $\mathbf{u} \in Z(t-1,\mathcal{U})$, by Proposition 37. Hence there is a $t' < t$ and a $\mathbf{v}'$ such that $(\mathbf{u}, \mathbf{v}') \in Z(t',\mathcal{U}, V)$, by Lemma 41. But this contradicts the minimality of t. So $\mathbf{u}$ is not an element of $Z(t-1,\mathcal{U})$ and the $\mathbf{k}$ is unique. Hence

$$L(\mathbf{k}) \cap Z(J(\mathbf{y})) = \{\mathbf{u}\}.$$

In other words $Z(J(\mathbf{y}))$ is a linear affine space, $Z(t,\mathcal{U})$ is a union of linear spaces, and $Z(J(\mathbf{y}))$ intersects exactly one of the components of $Z(t,\mathcal{U})$. The intersection of these 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 $\langle U_1 - u_1, \ldots, U_n - u_n \rangle$. The V_j satisfy linear equations in the U_{ij} which after evaluation at u_{ij} become 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 $J(t, \mathbf{y})$. $\square$

Remark 52. We note that in Augot et al. (2002) the authors also prove the uniqueness result for cyclic codes. Still they did not succeed to prove that their unique solution has multiplicity one. Our Theorem 51 states exactly this for arbitrary linear codes.

So we have that the system $J(t, \mathbf{y})$, for $t = \mathrm{wt}(\mathbf{e})$, has a unique simple solution $(\mathbf{u}, \mathbf{v})$. It is known from Theorem 50 that, $\mathbf{u} = \mathbf{u}(\mathbf{e})$, the unknown syndrome of $\mathbf{e}$, which lies in $\mathbb{F}_q^n$. But then via substitution of $\mathbf{u}$ to the system $J(t, \mathbf{y})$ it is not hard to see that $\mathbf{v}$ is also from $\mathbb{F}_q^n$.

We are now ready to formulate the algorithm for decoding. In the algorithm it is assumed that the number of errors occurred does not exceed the error correcting capacity of the code as in Theorems 50 and 51.

Algorithm 53. We proceed as follows.

(1) Set $i = 1$
(2) Find the reduced Gröbner basis G of the ideal $J(i, \mathbf{y})$ with respect to any ordering chosen in advance
(3) If $G = \{1\}$, then $i := i + 1$ and go to (2)
(4) G is of the form $\{U_j - u_j, V_l - v_l\}_{1 \leq j \leq n, 1 \leq l \leq i}$. Form a vector $\mathbf{u} = (u_1, \ldots, u_n)$ of unknown syndromes of $\mathbf{y}$
(5) Compute $\mathbf{e}^T = B^{-1}\mathbf{u}$
(6) Return $\mathbf{c} := \mathbf{y} - \mathbf{e}$

Example 54. Consider the ternary Golay code of length 11 and dimension 6. The code is cyclic with defining set $\{1\}$ and complete defining set $\{1, 3, 4, 5, 9\}$. So the BCH bound implies that the minimum distance is at least 4, but it is in fact 5. So the code is 2 error-correcting. But the decoding algorithms by Peterson and Berlekamp-Massey correct only 1 error. Now $m = 5$ is the smallest degree of an extension such that $\mathbb{F}_{3^m}^*$ has an element α of order 11. The corresponding RS matrix is given by $B = (\alpha^{(i-1)(j-1)} | 1 \leq i, j \leq 11)$. Let H be the parity-check matrix over $\mathbb{F}_{243}$ that consists of the rows $\mathbf{b}_i$ for i in the complete defining set. The matrix of syndromes $\mathcal{U}$ has entries $U_{ij} = U_{i+j-1}$, where the indices i, j are taken modulo n. For a received word $\mathbf{y}$ we have that the syndromes

$s_i = y(\alpha^i) = \sum_{j=1}^{11} y_j \alpha^{i(j-1)}$ for $i = 1, 3, 4, 5, 9$ are known. Hence the ideal $J(\mathbf{y})$ is generated by the elements $U_i - s_i$, for i in the complete defining set. If there are no errors, then $s_1 = 0$. If there is one error, then $s_1^{22} = 1$ Now suppose that the received word has 2 errors. Then $s_1^{242} = 1$ and $s_1^{22} \neq 1$. The quadratic equations

$$\sum_{j=1}^{2} U_{i+j-1} V_j = U_{i+2} \quad \text{for } i = 1, \ldots, n$$

from $J(t, \mathbf{y})$ become for $i = 3, 4$

$$\begin{cases} s_3 V_1 + s_4 V_2 = s_5 \\ s_4 V_1 + s_5 V_2 = U_6 \end{cases}$$

Now $s_3 = s_1^3$, $s_4 = s_1^{81}$ and $s_5 = s_1^{27}$. Hence $\Delta = s_3 s_5 - s_4^2 = s_1^{30}(1 - s_1^{132}) \neq 0$. So V_1 and V_2 can be expressed as linear functions in U_6.

$$\begin{cases} V_1 = (s_5^2 - s_4 U_6)/\Delta \\ V_2 = (s_3 U_6 - s_4 s_5)/\Delta \end{cases}$$

The remaining equations give that U_i is a polynomial in U_6 of degree $i - 5$ for $i > 6$. In fact the U_i, V_1 and V_2 are polynomials in s_1. See Higgs and Humphreys (1993).

Remark 55. In the cryptosystem of McEliece (1978) or Niederreiter (1986) a generator matrix or parity-check matrix is scrambled by permuting the coordinate positions and is used as public key. For instance let H_1 be a ternary parity-check matrix of the ternary Golay code. Let S be an invertible 5×11 matrix and P a 11×11 permutation matrix. Then $H_2 = SH_1P$ is the public key. It is assumed that H_2 looks like a random chosen matrix for an eavesdropper. Only those decoding algorithms can be used for his attack that have arbitrary codes as input. If our method would be used, then B_2 is an 11×11 MDS matrix over $\mathbb{F}_{27}$ since this is the smallest extension of $\mathbb{F}_3$ for which such a matrix exists. The parity check matrix H_2 and the matrix B_2 do not match so nicely anymore. We could use the linear equations in $J(\mathbf{y})$ to eliminate 5 variables. Than we are left with 11 quadratic equations in the 8 variables $U_1, \ldots, U_6$ and V_1, V_2, and in general there are no linear equations among them.

6. Simulations and experimental results

All computations in this section are undertaken on AMD Opteron Processor 242 (1.6MHz), 8GB RAM under Linux. The computations of Gröbner bases are realized in SINGULAR 3-0-3 Greuel et al. (2007). The command used is `std`.

6.1. Random binary codes

Here we present some results on decoding with the use of Theorem 50 for binary random codes. First we determine the minimum distance of a random code with the method from Bulygin and Pellikaan (2007) and then perform decoding of some given number of received words. We use degree reverse lexicographic order for decoding. 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 the minimum distance in a short time, so we have just assumed the error capacity.

We are able to correct even more errors in larger codes. The following table shows timings for random binary $[120, 10], [120, 20], [120, 30]$ and $[150, 10]$ codes, where 1 means one second or less. We also present here timing for MAGMA Computational Algebra Group (2005) in order to show that our approach actually does not depend on the concrete Gröbner basis algorithm. 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, for every code the left column corresponds to SINGULAR and the right column to MAGMA.

no. of err.	[120,40]		[120,30]		[120,20]		[120,10]		[150,10]	
2	1	1	1	1	1	1	1	1	1	1
3	22	7	1	1	1	1	1	1	1	1
4	172	64	5	14	1	1	1	1	1	1
5	804	228	31	36	1	1	1	1	1	1
6	-	-	98	63	3	9	1	1	2	1
7	-	-	471	144	7	15	1	1	2	1
8	-	-	-	-	17	25	1	1	2	1
9	-	-	-	-	43	38	1	1	2	1
10	-	-	-	-	109	51	1	1	2	1
11	-	-	-	-	392	84	1	1	3	1
12	-	-	-	-	-	630	2	8	3	1
13	-	-	-	-	-	-	2	9	4	1
14	-	-	-	-	-	-	3	11	4	1
15	-	-	-	-	-	-	7	13	5	20
16	-	-	-	-	-	-	10	16	5	22
17	-	-	-	-	-	-	22	19	8	26
18	-	-	-	-	-	-	38	23	8	30
19	-	-	-	-	-	-	72	28	16	38
20	-	-	-	-	-	-	183	33	27	43
21	-	-	-	-	-	-	265	48	43	50
22	-	-	-	-	-	-	362	64	69	59
23	-	-	-	-	-	-	688	723	128	69
24	-	-	-	-	-	-	-	-	261	82
25	-	-	-	-	-	-	-	-	575	93

Remark 56. 1) For a method for speeding up the above computations see Bulygin and Pellikaan (2007).
2) Also note that here we consider a situation, when we actually know the number of errors occurred, which is not very realistic. In practice one has to compute the Gröbner bases for all the systems $J(i, \mathbf{y})$ for all $i = 1, \ldots, t-1$. In Bulygin and Pellikaan (2007) we show that actually the computation of the Gröbner basis of the last system $J(t, \mathbf{y})$

dominates or at least is comparable with all the previous work that has to be done.

Now let us compare our method with the FL method Fitzgerald and Lax (1998). Note that this method exists in both online and offline versions, see Fitzgerald and Lax (1998) Section 2 and 3 resp. Our method is an online one, i.e. we compute a Gröbner basis for every received word. Therefore we do the comparison with the online version of the FL. We will try to follow the same pattern of codes as in our experiments. First, let us take a look at "small" codes.

code	err. cap.	GB dec.	no. of rec.	average
[25,11]	1	0.32	300	0.0011
[25,11]	2	14.48	300	0.0483
[25,8]	2	6.03	300	0.0201
[25,8]	3	4.68	1	4.68
[31,15]	2	11.46	100	0.1146
[31,15]	3	112.14	1	112.14

So, we see that except for the case of $[25, 11]$ code with 1 error, our method wins, sometimes substantially (cf. $[25, 8]$, $[31, 15]$ with 2 errors, and in particular $[31, 15]$ with 3 errors).

The difference is even more striking when working with $[120, 10], [120, 20], [120, 30]$ and $[150, 10]$ codes.

no. of err.	[120,30]	[120,20]	[120,10]	[150,10]
2	5	2	1	2
3	3996	2263	1544	804

These simulations indicate that when dealing with random (binary) codes the FL method Fitzgerald and Lax (1998), has problems starting already at 3 errors.

Remark 57. On some comparisons for Hermitian codes see Bulygin and Pellikaan (2007). Consult the latter reference also for comparisons with the method of Augot et. al. for cyclic codes.

6.2. Remarks

Remark 58. 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. Bardet et al. (2003), Shamir et al. (2000)). So if, for given n, we increase redundancy r, or reduce the number of errors t we want to correct, 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.

Let us now make some remarks on the "classical" syndrome decoding. One version of syndrome decoding is implemented for example in GAP computer algebra system GAP Group (2006). There coset leaders (c.l.) are explicitly computed and stored in a table for the further decoding, see Joyner (2007), sections 4.10-1 and 4.10-9. So, the major part of time is spent during the first decoding (when the table is precomputed), whereas further it takes almost no time. Also here the method is independent on t. We have the following (for binary random codes):

code	[25,11]	[25,8]	[31,15]
time for c.l. computation, sec	1.8	15.5	8.0

Already for a random binary code $[35, 15]$ GAP is not able to perform decoding and returns an error.

Similar performance was shown by MAGMA computer algebra system Computational Algebra Group (2005). We were unable to handle syndrome decoding over $GF(2)$, when a redundancy $n-k$ exceeded 20. So as we see, the syndrome decoding can be effective only in case of small values of $n-k$, whereas our method provides a better flexibility with respect to these parameters.

7. 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. Although, during the entire paper we had in mind Gröbner bases based approach for solving such system, other methods could be possible: further work will be undertaken in this direction. 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.

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 the offline decoding, where syndromes enter as variables, rather than concrete values. For some details on all the above see Bulygin and Pellikaan (2007).

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 Augot et al. (2002), it is much faster, than the online version of 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 via precomputation of a table with coset leaders.

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

Acknowledgements

The first author would like to thank "DASMOD: 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. We thank Max Sala and the referees for useful discussions, remarks and comments.

References

Arimoto, S., nov 1961. Encoding and decoding of p-ary group codes and the correction system. Inform. Processing in Japan 2, 320–325.

Augot, D., Bardet, M., Faugère, J., 2007. On formulas for decoding binary cyclic codes. In: Proc. IEEE Int. Symp. Information Theory.

Augot, D., Bardet, M., Faugère, J.-C., nov 2002. Efficient decoding of (binary) cyclic codes beyond the correction capacity of the code using Gröbner bases. Tech. Rep. 4652, INRIA.

Augot, D., Charpin, P., Sendrier, N., 1990. The minimum distance of some binary codes via the Newton's Identities. In: Eurocodes'90. Vol. LNCS 514. pp. 65–73.

Augot, D., Charpin, P., Sendrier, N., may 1992. Studying the locator polynomial of minimum weight codewords of BCH codes. IEEE Trans. Inform. Theory IT-38, 960–973.

Bardet, M., J.-C.Faugère, Salvy, B., 2003. Complexity of Gröbner basis computation for semi-regular overdetermined sequences over $GF(2)$ with solutions in $GF(2)$. Tech. Rep. 5049, INRIA.

Barg, A., 1998. Complexity issues in coding theory. In: Pless, V., Huffman, W. (Eds.), Handbook of Coding Theory. Elsevier, pp. 649–756.

Berlekamp, E., 1968. Algebraic coding theory. Mc Graw Hill.

Borges-Quintana, M., Borges-Trenard, M., Martinez-Moro, E., 2005a. On a grobner bases structure associated to linear codes, acepted at Journal of Discrete Mathematical Sciences & Cryptography.
URL `http://arxiv.org/abs/math.AC/0506045`

Borges-Quintana, M., Borges-Trenard, M. A., Martinez-Moro, E., 2005b. A general framework for applying fglm techniques to linear codes, accepted at AAECC 16.
URL `http://arxiv.org/abs/math.AC/0509186`

Borges-Quintana, M., Borges-Trenarda, M., Fitzpatrick, P., Martinez-Moro, E., 2005c. Groebner bases and combinatorics for binary codes.
URL `http://arxiv.org/abs/math.CO/0509164`

Bruck, J., Naor, M., 1990. The hardness of decoding linear codes with preprocessing. IEEE Transactions on Information Theory 36 (2), 381–385.

Bruns, W., Vetter, U., 1988. Determinantal rings. Vol. 1327 of Lect. Notes in Math. Springer-Verlag.

Bulygin, S., Pellikaan, R., 2007. Decoding and finding the minimum distance of error-correcting codes with Gröbner bases, work in progress.

Caboara, M., Mora, T., 2002. The Chen-Reed-Helleseth-Truong decoding algorithm and the Gianni-Kalkbrenner Gröbner shape theorem. Appl. Algeb. Eng. Commum. Comput. (13), 209–232.

Chen, X., Reed, I., Helleseth, T., Truong, T., 1994a. Algebraic decoding of cyclic codes: a polynomial point of view. Contemporary Math. 168, 15–22.

Chen, X., Reed, I., Helleseth, T., Truong, T., sep 1994b. General principles for the algebraic decoding of cyclic codes. IEEE Trans. Inform. Theory IT-40, 1661–1663.

Chen, X., Reed, I., Helleseth, T., Truong, T., sep 1994c. Use of Gröbner bases to decode binary cyclic codes up to the true minimum distance. IEEE Trans. Inform. Theory IT-40, 1654–1661.

Computational Algebra Group, 2005. Magma V2.12-14.
URL `http://magma.maths.usyd.edu.au`

Cooper, A., 1990. Direct solution of BCH decoding equations. Communication, Control and Signal Processing, 281–286.

Cooper, A., 1991. Finding BCH error locator polynomials in one step. Electronic Letters 27, 2090–2091.

Cooper, A., 1993. Toward a new method of decoding algebraic codes using Gröbner bases. In: Trans. 10th Army Conf. Appl. Math. and Comp. pp. 1–11.

Cox, D., J.Little, O'Shea, D., 1997. Ideals, Varieties, and Algorithms, 2nd Edition. Springer-Verlag.

Eisenbud, D., 1988. Linear sections of determinantal varieties. Amer. J. Math. 110, 541–575.

Eisenbud, D., 1995. Commutative algebra with a view toward algebraic geometry. Vol. 150 of Grad. Texts in Math. Springer-Verlag.

Fitzgerald, J., 1996. Applications of Gröbner bases to linear codes. Ph.D. thesis, Louisiana State University.

Fitzgerald, J., Lax, R., 1998. Decoding affine variety codes using Gröbner bases. Designs, Codes and Cryptography 13, 147–158.

GAP Group, 2006. GAP – Groups, Algorithms, and Programming. Version 4.4.
URL `www.gap-system.org`

Giorgetti, M., Sala, M., 2006. A commutative algebra approach to linear codes. BCRI preprint, `www.bcri.ucc.ie`, 58, University College Cork, Boole Centre BCRI, UCC Cork, Ireland, submitted to J. Algebra.

Gorenstein, D., Zierler, N., 1961. A class of error-correcting codes in p^m symbols. Journ. SIAM 9, 207–214.

Greuel, G.-M., Pfister, G., 2002. A SINGULAR Introduction to Commutative Algebra. Springer-Verlag.

Greuel, G.-M., Pfister, G., Schönemann, H., 2007. SINGULAR 3.0. A Computer Algebra System for Polynomial Computations, Centre for Computer Algebra, University of Kaiserslautern, `http://www.singular.uni-kl.de`.

Hartmann, C., may 1972. Decoding beyond the BCH bound. IEEE Trans. Inform. Theory, IT-18, 441–444.

Hartmann, C., Tzeng, K., mar 1974. Decoding beyond the BCH bound using multiple sets of syndrome sequences. IEEE Trans. Inform. Theory IT-20, 292–295.

Higgs, R., Humphreys, J., may 1993. Decoding the ternary golay code. IEEE Trans. Inform. Theory IT-39, 1043–1046.

Høholdt, T., van Lint, J., Pellikaan, R., 1998. Algebraic geometry codes. In: Pless, V., Huffman, W. (Eds.), Handbook of Coding Theory. Elsevier, pp. 871–961.

Joyner, D., 2007. GUAVA: A GAP4 Package for computing with error-correcting codes. Version 3.1.
URL `http://www.gap-system.org/Manuals/pkg/guava3.1/htm/chap0.html`

Kostrikin, A., Shafarevich, I. (Eds.), 1990. Algebra I: Basic Notions of Algebra. Vol. 11 of Encyclopedia of Mathematical Sciences. Springer-Verlag.

Lang, S., 1993. Algebra. Addison-Wesley Publishing Company.

Loustaunau, P., York, E., 1997. On the decoding of cyclic codes using Gröbner bases. AAECC 8 (6), 469–483.

Massey, J., jan 1969. Shift-register synthesis and BCH decoding. IEEE Trans. Inform. Theory IT-15, 122–127.

McEliece, R., 1978. A public-key cryptosystem based on algebraic codig theory. Tech. Rep. 42-44, DSN Progress Report.

Niederreiter, H., 1986. Knapsack-type crypto systems and algebraic coding theory. Problems of Control and Information Theory 15 (2), 159–166,.

Orsini, E., Sala, M., 2005. Correcting errors and erasures via the syndrome variety. J. Pure and Appl. Algebra (200), 191–226.

Orsini, E., Sala, M., 2007. Improved decoding of affine–variety codes. BCRI preprint, `www.bcri.ucc.ie`, 68, University College Cork, Boole Centre BCRI, UCC Cork, Ireland.

Peterson, W., 1960. Encoding and error-correction procedures for the Bose-Chauduri codes. IRE Trans. Inform. Theory, IT-6, 459–470.

Peterson, W., Weldon, E., 1977. Error-correcting codes. MIT Press.

Room, T., 1938. The geometry of determinantal loci. Cambridge University Press.

Shamir, A., Patarin, J., Cortois, N., Klimov, A., 2000. Efficient Algorithms for solving Overdetermined Systems of Multivariate Polynomial Equations. Vol. 1807. pp. 392–407, advances in cryptology - EUROCRYPT'00.

Shparlinski, I., 1993. Finding irreducible and primitive polynomials. Appl. Alg. Engin. Commun. Comp. 4, 263–268.

Shparlinski, I., 1999. Finite fields: Theory and computation. Vol. 477 of Mathematics and its Applications. Kluwer Acad. Publ.

Sturmfels, B., 1990. Gröbner bases and Stanley decompositions of determinantal rings. Math. Zeitschrift 205, 137–144.

Sugiyama, Y., Kasahara, M., Hirasawa, S., Namekawa, T., 1975. A method for solving the key equation for decoding Goppa codes. Information and Control 27, 87–99.

Tzeng, K., Hartmann, C., Chien, R., oct 1971. Some notes on iterative decoding. In: Proc. 9th Allerton Conf. Circuit and Systems Theory.