On the decoding of cyclic codes with the Newton's identities

Daniel Augot

INRIA-Rocquencourt

Magali Bardet

Laboratoire LITIS
Université de Rouen

Jean-Charles Faugère

INRIA Rocquencourt, Salsa project
Université Pierre et Marie Curie-Paris 6 Équipe SPIRAL
CNRS-UMR 7606, LIP6

Abstract

We revisit in this paper the concept of decoding cyclic codes with Gröbner bases. These ideas were first introduced by Cooper, then Chen, Reed, Helleseth and Truong, and eventually by Orsini and Sala. We discuss here another way of putting the decoding problem into equations: the Newton's identities. Although these identities have been extensively used for decoding, the work was done manually, to provide formulas for the coefficients of the locator polynomial. This was achieved by Reed, Chen, Truong and others in a long series of papers, for decoding quadratic residue codes, on a case-by-case basis. It is tempting to automate these computations, using elimination theory and Gröbner bases.

Thus, we study in this paper the properties of the system defined by the Newton's identities, for decoding binary cyclic codes. This is done in two steps, first we prove some facts about the variety associated to this system, then we prove that the ideal itself contains relevant equations for decoding, which lead to formulas.

Then we consider the so-called online Gröbner bases decoding, where the work of computing a Gröbner basis is done for each received word. It is much more efficient for practical purposes than preprocessing and substituting into the formulas. Finally, we conclude with some computational results, for codes of interesting length (about one hundred).

Key words: Cyclic codes, quadratic residue codes, elimination theory, Gröbner bases, $F4$ algorithm.

1 Introduction

1.1 Introduction and Previous work

A motivation for this work is to find decoding algorithms for the *quadratic residue codes*, which are a very special and interesting family of cyclic codes. We consider only binary codes. For each prime number l, such that 2 is a square modulo l, there exists essentially one quadratic residue code of length l. These codes have a not so bad minimum distance, from the *square-root bound*, and in practice they perform even better, from compiled tables by Macwilliams and Sloane (1983); Grassl (2000). But there is no general decoding algorithm of the quadratic residue codes, and several efforts have been made in order to decode them. Let us cite the works of Chen, Chang, Reed, Helleseth, Truong etc: Reed et al. (1990a,b, 1992); Chen et al. (1994c); Lu et al. (1995); He et al. (2001); Chang et al. (2003); Truong et al. (2005), for the lengths 31, 23, 41, 73, 47, 71, 79, 97, 103 and 113. We note that for each prime l, the authors had to design a new decoding algorithm, almost from scratch each time.

These algorithms are based on the same principle: given the received word e, the set of its *syndromes* is computed, and the *error locator polynomial* has to be determined. For this, the authors write down a system of equations, whose indeterminates are 1) the syndromes, 2) the coefficients of the error locator polynomial, 3) the so-called *unknown syndromes*. This system is based on the Newton's identities. Once that this system was written, the above authors try to eliminate the unknown syndromes, and to express the coefficients of the locator polynomial as polynomials or rational functions in terms of the syndromes. Then, to decode, one only needs to substitute the actual value of the syndromes into the formulas, to get the locator polynomial. Finding the expression of the locator polynomial is tedious and error prone, as the length of the codes grows.

It makes sense to use tools from computer algebra to automate these steps. This can actually be done for *any* cyclic code, although Cooper III (1990,

Email addresses: Daniel.Augot@inria.fr (Daniel Augot),
magali.bardet@univ-rouen.fr (Magali Bardet),
Jean-Charles.Faugere@lip6.fr (Jean-Charles Faugère).
URLs: www-rocq.inria.fr/~augot (Daniel Augot),
www-calfor.lip6.fr/~bardet/ (Magali Bardet), fgbrs.lip6.fr/jcf/
(Jean-Charles Faugère).

1991b,a) considered it only for BCH codes. The system of equations introduced by Cooper III is different from the system of the Newton's identities, and can also be used for any cyclic code, see Chen et al. (1994b). The properties of these systems have been proven by Loustaunau and York (1997) and Caboara and Mora (2002), for any cyclic code. In Orsini and Sala (2005), this system is called CRHT (or more precisely, the variety associated to it is called the CRHT variety), and it is further refined in order to get what the authors call *general error locator polynomials*, which is computed offline, and then used for decoding online. Several examples are given in Orsini and Sala (2005), and exhaustive computations for all 2-error correcting cyclic codes of length less than 63 have been done by Orsini and Sala (2007).

1.2 Our contributions

We consider another system of equations than the CRHT one and its derivative. We consider the system based on the Newton's identities, as was already done by Chen et al. (1994a) (see also de Boer and Pellikaan (1999a,b)). We have already discussed the use of Gröbner bases for decoding cyclic codes in Augot et al. (2003), but for another system, and also, for doing *online* Gröbner bases computation. In the present paper, we prove that the system of the Newton's identities can be used for *offline* Gröbner bases computation, (called One Step Decoding in de Boer and Pellikaan (1999a,b)), to find formulas for the coefficients of the locator polynomial, which are of the form:

$$\sigma_i = \frac{q_i}{p_i}.$$

It is not clear how these formulas relate to the general error locators polynomials of Orsini and Sala (2005). But we think that the approach of precomputing formulas for the decoding is rather inefficient for two reasons: the computation of these formulas is rather intractable, and even when the formulas are obtained, they are to huge to be practical.

Our second contribution is to show that it is much better to perform *online* Gröbner bases computations: for each received word, one writes down the system of the Newton's identities with the known syndromes of the errors, the unknown syndromes, and the locators. We show in this paper that the elimination of the unknown syndromes by a computation of a Gröbner basis leads directly to the value of the coefficients of the locator polynomial. This is in practice much faster.

Thanks to fast algorithms for computing Gröbner bases Faugère J.C. (1999); Faugère J.C. (2002) and fast implementation (FGb or Magma for instance), we get a reasonable number of operations for decoding cyclic codes, even for codes of length one hundred or more. We will also show how the speed of the decoding can be improved using code generation techniques.

1.3 Outline of the paper

The paper is organized as follows. In Section 2, we recall the properties of Gröbner bases (elimination and specialization) that we need in the sequel. In Section 3, we recall the definition of cyclic codes, and some important properties of the Fourier Transform. In Section 4, we determine the variety associated to the Newton's identities. Section 5 is devoted to One Step Decoding (i.e. finding formulas for decoding), while Section 6 deals with online computation of Gröbner bases. Section 7 explains how to use a single Gröbner basis computation on one set of syndromes to derive the other computations on the other sets of syndromes, using code generation techniques. Section 8 presents some Figures and Tables.

2 Background on Gröbner bases

2.1 Definition

Let $\mathbb{F}[X_1, \ldots, X_n]$ be considered, where $\mathbb{F}$ is a field and $X_1, \ldots, X_n$ are indeterminates. A monomial ordering $<$ over the set of monomials $X_1^{i_1} \cdots X_n^{i_n}$ is a total ordering, compatible with multiplication by a monomial, which is also a well ordering (see (Cox et al., 1992, Chapter2, Definition 1)). Given a polynomial $f \in K[X_1, \ldots, X_n]$, the leading monomial, leading term, and leading coefficient of f are then defined (Cox et al. (1992)). The classical definition of a Gröbner basis is the following.

Definition 1 *A Gröbner basis of an ideal $I \subset \mathbb{F}[X_1, \ldots, X_n]$ is a set of polynomial $G = \{g_1, \ldots, g_r\} \subset I$ such that the leading monomials of the g_i's generate by monomial-wise multiplication all the leading monomials of the polynomials in I.*

We postpone the discussion on the algorithms to compute Gröbner bases to Section 6.

2.2 Gröbner bases and elimination

Definition 2 *(Eisenbud (1995) p.357) An* elimination ordering *with two blocks* $[X_1, \ldots, X_i] > [X_{i+1}, \ldots, X_n]$ *is a monomial order such that any monomial involving one of the* $X_1, \ldots, X_i$ *is greater than any monomial involving only monomials from* $\{X_{i+1}, \ldots, X_n\}$.

For instance, the lexicographical (Lex) order on $[X_1, \ldots, X_n]$ is an elimination order for the blocks $[X_1, \ldots, X_i]$ and $[X_{i+1}, \ldots, X_n]$ for any i. The following two properties will be useful:

Theorem 1 (Elimination Theorem, Cox et al. (1992) pp. 113) *Let* $I \subset \mathbb{F}[X_1, \ldots, X_n]$ *be an ideal, and let* G *be a Gröbner basis of* I *for an elimination order with blocks* $[X_1, \ldots, X_i] > [X_{i+1}, \ldots, X_n]$. *Then, the set*

$$G_i = G \cap \mathbb{F}[X_{i+1}, \ldots, X_n]$$

is a Gröbner basis of the i*-th elimination ideal* $I_i = I \cap \mathbb{F}[X_{i+1}, \ldots, X_n]$.

Given an ideal $I \subset \mathbb{F}[X_1, \ldots, X_n]$, we denote by $V(I)$ the variety associated to I, which is the set of solutions of I in the algebraic closure $\overline{\mathbb{F}}$ of $\mathbb{F}$, i.e.

$$V(I) = \left\{ x \in \overline{\mathbb{F}}^n \mid p(x) = 0,\ \forall p \in I \right\}.$$

Definition 3 *An ideal* I *is* zero-dimensional *if* $V(I)$ *is finite, and is of* positive dimension *otherwise.*

We have that if Π_i denote the projection on the $n - i$ last coordinates, i.e. $\Pi_i(x_1, \ldots, x_n) = (x_{i+1}, \ldots, x_n)$ then $\Pi_i(V(I)) = V(I_i)$.

2.3 Specialization

We have the following Theorem about the properties of specialization. Let $f \in \mathbb{F}[Y, X]$, with $X = (X_1, \ldots, X_n)$. We note $\mathrm{LT}(I)$ the set of the leading terms of polynomials of an ideal I, and $\mathrm{LT}_Y(f)$ the leading term of f, seen as a polynomial in $\mathbb{F}_q[Y][X]$. We will distinguish a given indeterminate X_i from an actual value given to it, that we shall denote with an asterisk $X_i^* \in \overline{\mathbb{F}}$.

Theorem 2 (Gianni (1989); Kalkbrener (1989)) *Let* $I \subset \mathbb{F}[Y, X]$ *a zero-dimensional ideal,* $X^* \in \overline{\mathbb{F}}^n$ *be given, and* φ_{X^*} *the specialization of all the variables but one*

$$\begin{aligned} \varphi_{X^*} :\ \mathbb{F}[Y, X] &\to \quad \mathbb{F}[Y] \\ f(Y, X) &\mapsto f(Y, X^*) \end{aligned} \tag{1}$$

Then there exists a polynomial $g \in I$ *such that* $\varphi_{X^*}(I) = \langle \varphi_{X^*}(g) \rangle$ *and* $\deg_Y g = \deg_Y \varphi_{X^*}(g)$.

Given an ideal $I \subset \mathbb{F}[X_1, \ldots, X_n]$, $S = \{X_{i_1} \ldots, X_{i_l}\}$ a subset of $\{X_1, \ldots, X_n\}$, and $S^* = \{X^*_{i_1} \ldots, X^*_{i_l}\} \in \overline{\mathbb{F}}^l$, we use the notation $p(S \mapsto S^*)$ for the substitution of the X_{i_j} by the $X^*_{i_j}$ in the polynomial p, and the notation $I(S \mapsto S^*)$ for the same operation on the ideal I.

3 Background on cyclic codes

3.1 Definition

We consider only binary codes. Let the reader be warned that our new results do not hold over any field, but only for this particular case. Let n be an odd integer, a cyclic code C of length n is an ideal of the algebra $\mathbb{F}_2[X]/(X^n - 1)$. We shall identify a word $c = (c_0, \ldots, c_{n-1}) \in \mathbb{F}_q^n$ with the polynomial $c(X) = c_0 + \ldots c_{n-1}X^{n-1}$. The code C is generated as an ideal by its *generating polynomial* $g(X)$, which divides $X^n - 1$. Let α be a primitive n-th root of unity, in some extension $\mathbb{F}_{2^m}$ of $\mathbb{F}_2$, a cyclic code C can be given by its defining set Q which is

$$Q = \left\{ i \in \{0 \ldots n-1\}, g(\alpha^i) = 0 \right\}.$$

We note $N = \{0 \ldots n-1\} \setminus Q$ (think of Q as the (Q)uadratic residues, and N the (N)on residues, or (N)on syndromes). We note k, d, and $t = \lfloor \frac{d-1}{2} \rfloor$ the dimension, the minimum distance of C, and the error correction radius of C.

For any word in $\overline{\mathbb{F}}_2^n$, we define its Fourier Transform, also known as the *Mattson-Solomon polynomial*. Note that we introduce the definition over the algebraic closure, because we will introduce algebraic systems whose solutions may lie in arbitrary extensions of $\mathbb{F}_2$.

Definition 4 *Let* $\overline{\mathbb{F}}_2$ *denote the algebraic closure of* $\mathbb{F}_2$*. The* Fourier transform *of the word* $c = \sum_{r=0}^{n-1} c_r x^r \in \overline{\mathbb{F}}_2[x]/(x^n - 1)$ *is the polynomial* $S(Z) = \sum_{i=1}^{n} S_i^* Z^{n-i} \in \overline{\mathbb{F}}_2[Z]$*, where* $S_i^* = c(\alpha^i)$ *for all* $i \in \{1 \ldots n\}$.

Let $y = (y_0, \ldots, y_{n-1}) \in \mathbb{F}_2^n$ the word to be decoded, and c the transmitted codeword. We write $y = c + e$, where $e \in \mathbb{F}_2^n$ is the error. Let $(A_0^*, \ldots, A_{n-1}^*)$ be the Fourier Transform of the known word y then, concerning the Fourier Transform $(S_0^*, \ldots, S_{n-1}^*)$ of e, we have that $S_i^* = A_i^*$, for $i \in Q$. The S_i, $i \in Q$, are the *syndromes* of the error, while the S_i, $i \notin Q$ are the *unknown syndromes.*

Given $\tau \in \mathbb{N}$, the *syndrome decoding* principle is, given the syndromes S_i of the received word, to find the error e of weight $w \leq \tau$ such that its syndromes are the $S_i, i \in Q$. In the case when $\tau = t = \lfloor \frac{d-1}{2} \rfloor$, we have a unique solution. We shall consider this case, but also the case when $\tau > t$, in which case we may not have a unique solution to the decoding problem.

The Fourier transform satisfies the following Theorem, sometimes known as Blahut's Theorem. Since we state the Theorem for the unusual context of the algebraic closure of $\mathbb{F}_2$, we give the proof to convince the reader.

Theorem 3 *Let $S^*(Z) = \sum_{i=1}^{n} S_i^* Z^{n-i}$ be the Fourier transform of some word $c \in \overline{\mathbb{F}}_2^n$. Then the weight of c is equal to rank of the following circulant matrix C_{S^*}:*

$$C_{S^*} = \begin{pmatrix} S_0^* & S_1^* & \dots & S_{n-2}^* & S_{n-1}^* \\ S_1^* & S_2^* & \dots & S_{n-1}^* & S_0^* \\ \vdots & & & & \vdots \\ S_{n-1}^* & S_0^* & \dots & S_{n-3}^* & S_{n-2} \end{pmatrix}. \tag{2}$$

Proof Let $c = (c_0, \dots, c_{n-1})$. For $i \in \{0 \dots n-1\}$, we have that

$$\begin{pmatrix} S_i^* \\ S_{i+1}^* \\ \vdots \\ S_{i+n-1}^* \end{pmatrix} = F \begin{pmatrix} c_0 \\ \alpha^i c_1 \\ \vdots \\ \alpha^{(n-1)i} c_{n-1} \end{pmatrix}, \text{with } F = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \alpha^1 & \dots & \alpha^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{n-1} & \dots & \alpha^{(n-1)(n-1)} \end{pmatrix}.$$

Then

$$\begin{aligned} \begin{pmatrix} S_0^* & S_1^* & \dots & S_{n-2}^* & S_{n-1}^* \\ S_1^* & S_2^* & \dots & S_{n-1}^* & S_0^* \\ \vdots & & & & \\ S_{n-1}^* & S_0^* & \dots & S_{n-3}^* & S_{n-2}^* \end{pmatrix} &= F \begin{pmatrix} c_0 & c_0 & \dots & c_0 \\ c_1 & \alpha c_1 & \dots & \alpha^{n-1} c_1 \\ \vdots & \vdots & \ddots & \vdots \\ c_{n-1} & \alpha^{n-1} c_{n-1} & \dots & \alpha^{(n-1)(n-1)} c_{n-1} \end{pmatrix} \\ &= F \begin{pmatrix} c_0 & 0 & & \dots \\ 0 & c_1 & 0 & \dots \\ \vdots & & \ddots & \\ 0 & \dots & 0 & c_{n-1} \end{pmatrix} F. \end{aligned}$$

Now the rank of the inner diagonal matrix is equal to the weight of c, and F is an invertible Vandermonde matrix. $\square$

3.2 The locator polynomial

Let the error e be of weight w, and let $u_1, \ldots, u_w$ the indices of the non zero coordinates of e. These indices are encoded in the *locator polynomial* $\sigma(Z)$, defined as follows:

$$\sigma(Z) = \prod_{i=1}^{w}(1 - \alpha^{u_i}Z) = \sum_{i=0}^{w} \sigma_i Z^i,$$

where $\sigma_1, \ldots, \sigma_w$ are the *elementary symmetric functions* of $\alpha^{u_1}, \ldots, \alpha^{u_w}$, which are in turn denoted $Z_1 \ldots, Z_w$, and are called the *locators* of e. Finding e is equivalent to finding $\sigma(Z)$, and the problem is considered to be solved when $\sigma(Z)$ is found, thanks to the Chien search (Chien (1964)), which is an efficient method for finding the i's such that $\sigma(\alpha^{-i}) = 0$.

3.3 The Newton's identities

The *Newton identities* relate the elementary symmetric functions of the locators of e to the coefficients of the Fourier Transform of e. They have the following form (see Macwilliams and Sloane (1983)):

$$\begin{cases} S_i + \sum_{j=1}^{i-1} \sigma_j S_{i-j} + i\sigma_i = 0, & i \leq w, \\ S_i + \sum_{j=1}^{w} \sigma_j S_{i-j} = 0, & w < i \leq n + w. \end{cases} \tag{3}$$

Note that the indices of the S_i are cyclic, i.e. $S_{i+n} = S_i$. In these equations, there are the σ_i's, that we are looking for, the S_i, $i \in Q$, that we know, and the S_i's, $i \notin Q$, that we try to eliminate.

3.4 Matricial forms of the Newton's identities

We split the Newton's identities in two part: the circulant part and the quasi-triangular part. The triangular part is the following

$$I_{T,w} = \{S_i + \sum_{j=1}^{i-1} \sigma_j S_{i-j} + i\sigma_i \quad i \in \{1 \ldots w\}\}. \tag{4}$$

and the circulant part is the following

$$I_{C,n,w} = \left\{ S_{w+i \bmod n} + \sum_{j=1}^{w} \sigma_j S_{w+i-j \bmod n}, \quad i \in \{1 \ldots n\} \right\}; \tag{5}$$

We introduce the following circulant matrix:

$$C_S = \begin{pmatrix} S_0 & S_1 & \dots & S_{n-2} & S_{n-1} \\ S_1 & S_2 & \dots & S_{n-1} & S_0 \\ \vdots & & & & \vdots \\ S_{n-1} & S_0 & \dots & S_{n-3} & S_{n-2} \end{pmatrix}. \tag{6}$$

Then $I_{C,n,w}$ can be written as

$$C_S[\sigma_w \sigma_{w-1}, \dots \sigma_1, 1, 0, \dots, 0]^t = 0. \tag{7}$$

The system $I_{C,n,w}$ can also be written in a polynomial manner as follows:

$$S(Z)\sigma_w(Z) = 0 \bmod Z^n - 1, \text{ with } S(Z) = \sum_{i=1}^{n} S_i Z^{n-i} \text{ and } \sigma_w(Z) = 1 + \sum_{i=1}^{w} \sigma_i Z^i. \tag{8}$$

3.5 The Waring's formulas

Using the triangular part and the circulant part of the Newton's identities, we can write successively the S_i's in terms of the σ_i's. Thus there exists a polynomial $W_{w,i}$ such that

$$S_i = W_{w,i}(\sigma_1, \dots, \sigma_w) \bmod I_{T,w} + I_{C,n,w}, \quad i \in \{0 \dots n-1\}. \tag{9}$$

These expressions are known as the *Waring formulas*. An explicit expression for $W_{w,i}$ is even know and can be found in Lidl and Niederreiter (1996).

3.6 Algebraic Systems

We consider the ideal $I_{N,n,v}$ generated by the Newton identities:

$$I_{N,n,v} : \left\langle \begin{array}{l} S_i + \sum_{j=1}^{i-1} \sigma_j S_{i-j} + i\sigma_i, \quad 1 \le i \le v \\ S_i + \sum_{j=1}^{v} \sigma_j S_{i-j}, \quad n+v \ge i > v \\ S_{i+n} + S_i, i \in \{1 \dots v\}. \end{array} \right\rangle. \tag{10}$$

In the above, we indicate that we use cyclic indices for the S_i by adding the relations $S_{i+n} + S_i$. Let us note by σ the set of the variables $\{\sigma_1, \dots, \sigma_v\}$, by S_Q the set $\{S_i; i \in \{1,\ldots,n+v\}, i \bmod n \in Q\}$, and S_N the set $\{S_i, i \in \{1,\ldots,n+v\}\}\backslash S_Q$. Then $I_{N,n,v}$ is an ideal in the polynomial ring $\mathbb{F}_2[\sigma, S_Q, S_N]$.

Recall that to show the difference between the indeterminates and the actual values in $\overline{\mathbb{F}}_2$, we will append an asterisk to indeterminates when speaking of values: for instance S_1^* is an actual value in $\overline{\mathbb{F}}_2$ (the first syndrome of a given error) given to the *indeterminate* S_1, which is used in equations.

We know that, if we are given S_Q^*, S_N^*, and the σ_i^*, they will satisfy the system of equations defined by the ideal $I_{N,n,w}$. We first deal with the converse: what are the solutions of the system of equations defined by the $I_{N,n,v}$. Then, we will also show that $I_{N,n,v}$ contains polynomials relevant for decoding.

Definition 5 *Let $A = \mathbb{F}_q[Z_1,\ldots,Z_v,\sigma_1,\ldots,\sigma_v,S_1,\ldots,S_n,\ldots S_{n+v}]$, let us define the following ideals. The ideal of the elementary symmetric functions:*

$$I_{\sigma,v} = \left\langle \sigma_i - \sum_{1\le j_1<\cdots<j_i\le v} Z_{j_1}\ldots Z_{j_i}; i \in \{1\ldots v\} \right\rangle; \tag{11}$$

and the ideal of the cyclic power sum symmetric functions:

$$I_{S,n,v} = \left\langle \begin{array}{ll} S_i - \sum_{j=1}^{v} Z_j^i, & i \in \{1\ldots n+v\}; \\ S_{i+n} - S_i, & i \in \{1\ldots v\} \end{array} \right\rangle. \tag{12}$$

Proposition 1 *The ideal $I_{N,n,v}$ is the elimination ideal of the Z_i's in the ideal $I_{S,n,v} + I_{\sigma,v}$:*

$$(I_{S,n,v} + I_{\sigma,v}) \cap \mathbb{F}_q[S,\sigma] = I_{N,n,v}.$$

Let us first recall the following Theorem of Machi-Valibouze Valibouze (1995).

Theorem 4 *Let $f(Z) = Z^v + \sum_{i=1}^{v} \sigma_i Z^{v-i} \in \mathbb{F}[\sigma][Z]$. Let the f_i polynomials, $i \in \{1\ldots v\}$, be iteratively constructed as follows (Cauchy Modules):*

$$f_1(Z_1) = f(Z_1), \tag{13}$$

$$f_{i+1}(Z_1,\ldots,Z_{i+1}) = \frac{f_i(Z_1,\ldots,Z_{i-1},Z_i) - f_i(Z_1,\ldots,Z_{i-1},Z_{i+1})}{Z_i - Z_{i+1}}. \tag{14}$$

Then, for every $i \in \{1\ldots v\}$, $f_i \in \mathbb{F}_q[\sigma][Z_1,\ldots,Z_i]$. Furthermore, with the lexicographical ordering $Z_v > Z_{v-1} > \cdots > Z_1 > \sigma_v > \cdots > \sigma_1$, f_i has a leading term equals to Z_i, and $G_{\sigma,v} = \{f_1,\ldots,f_v\}$ is a Gröbner basis of $I_{\sigma,v}$.

Proof of Proposition 1 Since n and v are fixed, let us write $I_N = I_{N,n,v}$, $I_\sigma = I_{\sigma,v}$, and $I_S = I_{S,n,v}$. We can infer the Newton's identities (triangular and circular) from the definition of the elementary and power-sum symmetric functions. We thus have:

$$I_N \subset (I_S + I_\sigma) \cap \mathbb{F}_q[\sigma_1, \dots, \sigma_v, S_1, \dots, S_n, \dots, S_{n+v}]. \tag{15}$$

To prove the reverse inclusion, we proceed in two steps: first we prove that $I_S + I_\sigma = I_N + I_\sigma$, then that

$$(I_N + I_\sigma) \cap \mathbb{F}_q[\sigma_1, \dots, \sigma_v, S_1, \dots, S_{n+v}] = I_N. \tag{16}$$

The Waring formulas are obtained from the Newton's identities, thus:

$$S_i - W_{v,i}(\sigma_1, \dots, \sigma_v) = 0 \bmod I_N, \quad i \in \{1 \dots n+v\}. \tag{17}$$

We note (as a short hand notation) s_i, $i \in \{1 \dots v\}$, for the polynomial

$$s_i = \sum_{1 \le j_1 < \dots < j_i \le v} Z_{j_1} \dots Z_{j_i},$$

then $\sigma_i - s_i \in I_\sigma$, and $S_i - W_{v,i}(s_1, \dots, s_v) \in I_N + I_\sigma$.

Last, let us write (also as a short hand notation) p_i, $i \in \{1 \dots n+v\}$, for the polynomial $\sum_{j=1}^{v} Z_j^i$, then, from the Waring formulas, we have that $p_i = W_{v,i}(s_1, \dots, s_v)$, which implies

$$S_i - p_i \in I_N + I_\sigma, \quad i \in \{1 \dots n+v\},$$

i.e. $I_S \subset I_N + I_\sigma$. Thus $I_S + I_\sigma \subset I_N + I_\sigma$ and the equality $I_S + I_\sigma = I_N + I_\sigma$ follows.

We now prove (16). Let G_N be a Gröbner basis of I_N, for any ordering, and let G_σ be the Gröbner basis of I_σ described in Theorem 4. Then $G_N \cup G_\sigma$ is a Gröbner basis of $I_N + I_\sigma$. Indeed, from Theorem 4, G_σ does not contain any polynomial whose leading term contains one of the σ_i's. Then, the leading terms of the polynomials in G_N and of the polynomials in G_σ are relatively prime, a fact which implies that $G_N \cup G_\sigma$ is Gröbner basis. The elimination properties of Gröbner bases imply that

$$(G_N \cup G_\sigma) \cap \mathbb{F}_q[\sigma_1, \dots, \sigma_n, S_1, \dots, S_{n+v}] \tag{18}$$

is a Gröbner basis of $(I_N + I_\sigma) \cap \mathbb{F}_q[\sigma_1, \dots, \sigma_v, S_1, \dots, S_{n+v}]$. Since, from Theorem 4, $G_\sigma \cap \mathbb{F}_q[\sigma_1, \dots, \sigma_v] = \{0\}$, the elimination properties of Gröbner bases also imply that G_N is a Gröbner basis of $(I_N + I_\sigma) \cap \mathbb{F}_q[\sigma_1, \dots, \sigma_v, S_1, \dots, S_{n+v}]$. □

4 The variety associated to the Newton's identities

Theorem 5 *Let $\mathbb{F}_q$ be the finite field with q elements. Let e be a word in $\overline{\mathbb{F}}_q^n$, of weight w, $\sigma^*(Z)$ its locator polynomial, and $S^* = (S_0^*, \dots, S_{n-1}^*)$ its Fourier*

Transform. Let us consider $I_{N,n,v}$ the Newton's identities written for a given weight $v \neq w$. Then:

1. The circulant part of the Newton Identities, when specialized on S^* has a solution

$$\rho^* = (\rho_1^*, \dots, \rho_v^*) \in \overline{\mathbb{F}}_q^v,$$

if and only if the weight w of e is less than or equal to v.

2. Suppose that $w \leq v$ and let ρ^* be as previously, then the polynomial $\rho^*(Z) = 1 + \sum_{i=1}^{v} \rho_i^* Z^i$, is a multiple of $\sigma^*(Z)$.

3. If the characteristic of $\mathbb{F}_q$ is 2, and if furthermore S^* and ρ^* are solutions of the triangular part of the Newton Identities, then e has indeed coordinates in $\mathbb{F}_2$, and there exists $G(Z) \in \overline{\mathbb{F}}_2[Z]$ and an integer $l \geq 0$ such that

$$\rho^*(Z) = \sigma^*(Z) G(Z)^2 Z^l. \tag{19}$$

Proof *1* . Suppose there exists a solution ρ^* to $I_{C,n,v}(S \mapsto S^*)$. Let C_{S^*} be the circulant matrix constructed from S^* as in (2). From the solution $(\rho_1^*, \dots, \rho_v^*)$, it is seen that the $(v+1)$-th column of C_{S^*} can be linearly expressed in terms of the v first columns. The circulant properties of the matrix C_{S^*} then imply that the $(v+2)$-th column can be expressed in terms of the v previous columns, and so on. Thus the v first columns generate the column space of C_{S^*}, which must have a rank less than or equal to v. From Theorem 3, $w \leq v$.

Conversely, if the weight of e is less than v, then the elementary symmetric functions of e, $\sigma_1^*, \dots, \sigma_w^*$ are solutions of the circulant part of the Newton Identities $I_{C,w}$ written for the weight w, specialized on S^*. One checks that

$$(\sigma_1^*, \dots, \sigma_w^*, \sigma_{w+1}^* = 0 \dots, \sigma_v^* = 0)$$

is solution of $I_{C,n,v}(S \mapsto S^*)$.

2. Let $F \subset \overline{\mathbb{F}}_q^v$ be the set of solutions $\underline{\rho}^* = (\underline{\rho}_1^*, \dots, \underline{\rho}_v^*)$ of $I_{C,n,v}(S \mapsto S^*)$ as in (7), i.e. the set of $\underline{\rho}^*$ such that ${C_{S^*}}^T \underline{\rho}^* = 0$. Then, since the rank of C_{S^*} is w, F is an affine space of dimension $v - w$. Let F' be the space

$$F' = \left\{ \rho^* = (\rho_1^*, \dots, \rho_v^*) \in \overline{\mathbb{F}}_q^v \mid \sigma^*(Z) \text{ divides } \rho^*(Z) = 1 + \sum_{i=1}^{v} \rho_i^* Z^i \right\}.$$

Then F' is also an affine space, of dimension $v - w$. Let $\rho^* \in F'$ and $\rho^*(Z)$ constructed from ρ^*. Since $\sigma^*(Z) | \rho^*(Z)$, and since, from (8), $S^*(Z)\sigma^*(Z) = 0 \bmod Z^n - 1$, we also have:

$$S^*(Z)\rho^*(Z) = 0 \bmod Z^n - 1,$$

i.e. $(\rho_1^*, \dots, \rho_v^*) \in F$. Thus $F' \subset F$. Since they have the same dimension, they are equal.

3. Let $\sigma^*(Z)$ be the locator polynomial of e, and $\rho^*(Z)$ as in the Theorem. Then, from statement *2.* of the Theorem, $\sigma^*(Z)|\rho^*(Z)$. Let then $Z_1^*, \dots, Z_w^*$ be the locators of e, and $Z_{w+1}^* \dots, Z_v^*$ the roots of $\rho^*(Z)$ which are not locators. Since S^* and ρ^* satisfy the Newton's Identities, they satisfy the Waring formulas

$$S_i^* = W_{v,i}(\rho_1^*, \dots, \rho_v^*), \quad i \in \{1 \dots n\}, \tag{20}$$

and since the ρ_i^*'s are the elementary symmetric functions of $Z_1^*, \dots, Z_v^*$:

$$S_i^* = \sum_{j=0}^{v} Z_j^{*i}, \quad i \in \{1 \dots n\}. \tag{21}$$

On the other hand, S^* is the Fourier Transform of e. Let Y_j^*, $j \in \{1 \dots w\}$ be the coefficient of e corresponding to the locator Z_j^*, with $Y_j^* \neq 0$. Computing the Fourier Transform in terms of the Y_i's and the Z_i's leads to

$$S_i^* = \sum_{j=1}^{w} Y_j^* Z_j^{*i}, i \in \{1 \dots n\}. \tag{22}$$

By equality of the right-hand sides of (21) and (22), we get the matricial relation

$$\begin{bmatrix} Z_1^* & \dots & Z_w^* & Z_{w+1}^* & \dots & Z_v^* \\ Z_1^{*2} & \dots & Z_w^{*\,2} & Z_{w+1}^{*\;\;2} & \dots & Z_v^{*2} \\ \vdots & & & & & \vdots \\ Z_1^{*n} & \dots & Z_w^{*\,n} & Z_{w+1}^{*\;\;n} & \dots & Z_v^{*n} \end{bmatrix} Y_{w,v}^{*\;\;t} = 0 \tag{23}$$

where $Y_{w,v}^*$ is the vector $(Y_1^* + 1, \dots, Y_w^* + 1, 1, \dots, 1)$. Considering the matrix consisting only in the first v rows of the left-hand matrix, we get a Vander-Monde matrix, whose determinant Δ_v^* is

$$\Delta_v^* = \left(\prod_{i=1}^{v} Z_i^* \right) \left(\prod_{1 \le j_1 < j_2 \le v} (Z_{j_2}^* - Z_{j_1}^*) \right). \tag{24}$$

Now there are two alternatives. Either the vector $Y_{w,v}^*$ is zero, or the determinant Δ_v^* is zero. In the first case, we get the result: $w = v$, and all the Y_i^* satisfy $Y_i^* + 1 = 0$. In the second case, they are three possibilities:

(1) one of the Z_j^*'s is zero, for $w + 1 \le j \le v$;
(2) $Z_{j_1}^* = Z_{j_2}^*$, for $w + 1 \le j_1, j_2 \le v$;
(3) $Z_{j_1}^* = Z_{j_2}^*$, with $1 \le j_1 \le w$ and $w + 1 \le j_2 \le v$.

In case (1), we can rewrite (23), and withdraw the j-th column of the matrix. Note that we get a factor Z of the polynomial $\rho^*(Z)$.

In case (2), the effect of the characteristic 2 is that the terms $Z^*_{j_1}$ and $Z^*_{j_2}$ in the equation (23) will collapse. We can rewrite the equation (23) without the j_1-th and j_2-th columns. Note that the equality $Z^*_{j_1} = Z^*_{j_2}$ contributes as a square factor in $\rho^*(Z)$.

In case (3), the j_1-th and j_2-th columns will sum up, and we get a relation

$$\begin{bmatrix} Z_1^* & \dots & Z_w^* & Z_{w+1}^* & \dots & Z_v^* \\ Z_1^{*2} & \dots & Z_w^{*\,2} & {Z_{w+1}^*}^2 & \dots & Z_v^{*2} \\ \vdots & & & & & \vdots \\ Z_1^{*n} & \dots & Z_w^{*\,n} & {Z_{w+1}^*}^n & \dots & Z_v^{*n} \end{bmatrix} Y^{*'}_{w,v} = 0, \tag{25}$$

where the j_2-th row of the matrix in (23) has disappeared, and $Y^{*'}_{w,v} = (Y_1^* + 1, \dots, Y^*_{j_1} + 1 + 1, \dots, Y_w^* + 1, 1, \dots, 1)$ is a vector of length $v - 1$.

In each of the cases (1), (2) and (3), the matrix of (23) has shrunk, eliminating columns where one of the Z_j^* occurs, $w + 1 \leq j \leq v$. Repeating the process, we eventually get a relation

$$\begin{bmatrix} Z_1^* & \dots & Z_w^* \\ Z_1^{*2} & \dots & Z_w^{*\,2} \\ \vdots & \vdots & \\ Z_1^{*n} & \dots & Z_w^{*\,n} \end{bmatrix} \begin{bmatrix} Y_1^* + \epsilon_1 \\ \vdots \\ Y_w^* + \epsilon_w \end{bmatrix} = 0, \tag{26}$$

containing only the Z_j^*, $1 \leq j \leq w$, and where $\epsilon_i = 0$ or 1, from the effect of the characteristic 2. Now the Vandermonde matrix of (26) is non singular, since the Z_i^*'s, $1 \leq i \leq w$ are different. Thus the vector $Y_1^* + \epsilon_1, \dots, Y_w^* + \epsilon_w$ is zero, which implies $Y_i^* = 1$, $i \in \{1 \dots w\}$, since they are non zero. Keeping track of the square factors, and of the Z factors of $\rho^*(Z)$ leads to the form (20). $\square$

5 One-step decoding

5.1 Zero dimensional ideals

We consider the following ideal, which is the ideal generated by the Newton's identities, augmented with the so-called "field equations":

$$I^0_{N,n,v} = I_{N,n,v} + \left\langle \begin{matrix} S_i^{2^m} + S_i, i \in \{1, \dots, n\}, \\ \sigma_i^{2^m} + \sigma_i, i \in \{1, \dots, v\} \end{matrix} \right\rangle. \tag{27}$$

The addition of these field equations ensures that the solutions of this algebraic system all lie in the field $\mathbb{F}_{2^m}$, which is the splitting field of $X^n - 1$ over $\mathbb{F}_2$. Furthermore, from (Cox et al., 2005, Chapter2, Proposition 2.7), we have that $I^0_{N,n,v}$ is a radical ideal, since it contains a univariate square-free polynomial in each indeterminate. It is also a zero-dimensional ideal, since all the solutions lie in $\mathbb{F}_{2^m}$.

From the NullStellenSatz Cox et al. (1992), we have the following Corollary of Theorem 5.

Corollary 6 *Let $I_{N,n,v} \cap \mathbb{F}_2[S_Q, S_N]$ be the elimination ideal of the σ_i's in $I_{N,n,v}$. If $I_{N,n,v}$ is radical, then $I_{N,n,v} \cap \mathbb{F}_2[S_Q, S_N]$ is the set of all the relations between the coefficients of the Fourier Transform of the binary words of weight less than v. Furthermore, if we eliminate the S_i's, $i \notin Q$, then $I_{N,n,v} \cap \mathbb{F}_2[S_Q]$ is the set of all the relations between the syndromes of the words (in the algebraic closure) of weight less than v.*

Concerning the zero-dimensional ideals, since they are radical, we get:

Corollary 7 *Let $I^0_{N,n,v} \cap \mathbb{F}_2[S_Q, S_N]$ be the elimination ideal of the σ_i's in $I^0_{N,n,v}$. Then $I^0_{N,n,v} \cap \mathbb{F}_2[S_Q, S_N]$ is the set of all relations between the coefficients of the Fourier Transform of words of weight less than or equal to v, whose Fourier Transform lie in $\mathbb{F}_{2^m}$.*

Computing a Gröbner basis of $I_{N,n,w}$, then eliminating the σ_i's, we get a criteria which helps to determine the weight of the error.

Corollary 8 *Let S^*_Q be the set of syndromes of some word e of weight w. Let T_v be a Gröbner basis of $I_{N,n,v} \cap \mathbb{F}_2[S_Q]$, then e has a weight w less than or equal of v if and only if*

$$t(S^*_Q) = 0, \textit{for all } t \in T_v. \tag{28}$$

We can use the condition 28 as a criterion to find the weight w of some error e, by successively checking the conditions

$$t(S^*_Q) = 0, \text{for all } t \in T_v$$

for $v = 1, 2, \ldots$ until we find the first v such that the conditions (28) are satisfied.

Theorem 9 *For each binary word e of weight w less than t, for each $i \in \{1, \ldots, w\}$, the ideal $I^0_{N,n,w}$ contains a polynomial*

$$p_i \sigma_i + q_i,$$

with $p_i, q_i \in \mathbb{F}_2[S_Q]$ such that $p_i(S^*_{Q,e}) \neq 0$, where $S^*_{Q,e}$ is the set of syndromes of e.

Proof Consider I^0_j the ideal $I^0_{N,n,w} \cap [\sigma_j, S_Q]$. First note that I^0_j is a zero-dimensional radical ideal. Let e be an error of weight w, S^*_Q the set of its syndromes, and σ^*_j its j-th elementary symmetric function. Then, from Theorem 5, the variety $V(I_{N,n,w})$ is exactly $\{\sigma^*_1, \ldots, \sigma^*_w\}$, and the variety $V(I_j(S_Q \mapsto S^*_Q))$ is $\{\sigma_j - \sigma^*_j\}$. Since the ideal is radical, one has

$$I_j(S_Q \mapsto S^*_Q) = \left\langle \sigma_j - \sigma^*_j \right\rangle. \tag{29}$$

Now, considering the specialization map $\varphi_{S^*_Q} : (\sigma_j, S_Q) \mapsto (\sigma_j, S^*_Q)$, Theorem 2 shows that there exists a polynomial $g_j = g_j(\sigma_j, S_Q) \in I^0_j$ such that $\varphi_{S^*_Q}(I^0_j) = \left\langle \varphi_{S^*_Q}(g_j) \right\rangle$ and $\deg_{\sigma_j} g_j = \deg_{\sigma_j} \varphi_{S^*_Q}(g_j) = 1$. Thus the degree of g_j in σ_j is one. Also the initial $p_j(S_Q)$ of g_j does not vanish under the specialization. □

Thus the decoding algorithm is:

(1) (precomputation) For each $w \in \{1, \ldots, t\}$, compute a Gröbner basis G_w of $I^0_{N,n,w}$, for an ordering such that the S_i, $i \notin Q$, are greater than the σ_i's which in turn are greater than the S_i's, $i \in Q$;
(2) (precomputation) from each Gröbner basis G_w, collect the polynomials in $G_w \cap \mathbb{F}_2[S_Q]$, call T_w this set of polynomials;
(3) (precomputation) For each $w \in \{1, \ldots, t\}$, for each $i \in \{1 \ldots w\}$, find all the polynomials $p_i \sigma_i + q_i$, with $p_i, q_i \in \mathbb{F}_2[S_Q]$. This can be done using relevant orderings. Call $\Sigma_{w_e,i}$ this set of polynomials.
(4) (online) for each received word y, compute the syndromes $S^*_{Q,y} = S^*_{Q,e}$, where e is the error to be found;
(5) (online) find the weight w_e of e using the criterion (28).
(6) (online) for each $i \in \{1, \ldots, w_e\}$:
   (a) find the relation $p_i \sigma_i + q_i \in \Sigma_{w_e,i}$ such that $p_i(S^*_{Q_e}) \neq 0$
   (b) solve for σ^*_i:

$$\sigma^*_i = \frac{p_i(S^*_{Q_e})}{q_i(S^*_{Q_e})}$$

There are two difficulties with this approach. First, the Gröbner basis can contain many polynomials of the form $p_i \sigma_i + q_i$, $i \in \{1, \ldots, w\}$, as we have observed on examples. Second, the field equations of the type $\sigma_i^{2^m} + \sigma_i$, and $S_i^{2^m} + S_i$ can be of large degree, even though the length of the code is moderate. For instance, in the case of the quadratic residue code of length 41, the splitting field is $\mathbb{F}_{2^{20}} = \mathbb{F}_{1048576}$. This means that $I^0_{N,n,w}$ contains equations of degree more than one million, and the computation of the Gröbner basis is intractable. It is natural to try to remove the field equations, and to consider the ideal $I_{N,n,w}$ without the field equations.

5.3 Ideals of positive dimension

The main problem with the ideal $I_{N,n,v}$ is that it is an ideal of positive dimension. Thus we can not use the Specialization Theorem 2, and we were not able to prove that there exists polynomials of the form $p_i\sigma_i + q_i$ in $I_{N,n,v} \cap \mathbb{F}_2[\sigma_i, S_Q]$, although we think they do exist in all cases. However, in practice, the offline computation of the Gröbner bases of the ideal $I_{N,n,v}$ or $I^0_{N,n,v}$ are quite impractical. We were able to compute the Gröbner only for very short examples, and the yielded formulas are too large to be evaluated efficiently online. We will yet consider these systems for computation of Gröbner bases online.

6 Online computation of the Gröbner bases

6.1 Decoding up to half the minimum distance

In the case decoding with online computation of Gröbner bases, we first specialize with the syndromes, then we compute the Gröbner basis. We have the following Theorem, which describes the ideal $I_{N,n,v}(S_Q \mapsto S_Q ast)$.

Theorem 10 *Let S_Q^* be the set of syndromes of an error e of weight w, such that e is the only error of weight less than or equal to v admitting S_Q^* as syndromes (it is always the case when $v \leq t$). Let I be the ideal*

$$I = I_{N,n,v}(S_Q \mapsto S_Q^*) + \langle \sigma_{w+1}, \dots, \sigma_v \rangle \,, \tag{30}$$

then

$$I = \left\langle \sigma_1 - \sigma_1^*, \dots, \sigma_w - \sigma_w^*, \sigma_{w+1}, \dots, \sigma_v, S_j - S_j^*, j \in N \right\rangle . \tag{31}$$

Proof The proof is in two steps: we first show that the two varieties associated to the ideals of each side of (31) are equal, then that I is radical. Since the ideal in the right-hand side of (31) is radical, equality will follow.

Let thus (ρ^*, S_N^*) be a solution of I. Then, from Theorem 5, the weight of the Inverse Fourier Transform e' of (S_N^*, S_Q^*) is less than or equal to v. Since we assumed that e is the only error of weight less than or equal to v admitting S_Q^* as syndromes, we must have $e' = e$, and (S_Q^*, S_N^*) is the Fourier Transform of e. Furthermore, Theorem 5 ensures that the polynomial $\rho^*(Z)$, constructed from ρ^* is a multiple of $\sigma^*(Z)$. Since that terms $\rho_{w+1}^*, \dots, \rho_v^*$ are zero, we have $\rho^*(Z) = \sigma^*(Z)Z^{v-w}$, and we conclude that the associated varieties are equal.

Now we prove that the ideal I is radical. Using the ideal $I_{S,n,w}$ defining the power-sum symmetric functions, we construct the ideal

$$J = I_{N,n,v}(S_Q \mapsto S_Q^*) + I_{S,n,w} + \langle \sigma_{w+1}, \dots, \sigma_v \rangle \in \mathbb{F}_1[Z, \sigma, S_N], \qquad (32)$$

which is such that $J \cap \mathbb{F}_2[\sigma, S_N] = I$ (from Theorem 4). Then J has dimension zero, and the only solution $Z^* = (Z_1^*, \dots, Z_w^*)$ such that

$$(Z_w^*, \sigma^*, \sigma_{w+1}^* = 0, \dots, \sigma_v^* = 0, S_Q^*) \in V(J)$$

is the set of the roots of the locator polynomial $\sigma^*(Z)$ of e.

Let Δ_w be defined as in Equation (24) in the proof of Theorem 5. The locators of e are such that $\Delta_w(Z_1^*, \dots, Z_w^*) \neq 0$. Using the equations $S_{i+n} - S_i = 0$, $i \in \{1 \dots n\}$, and the definition of the power-sum symmetric functions, the ideal J contains the following system of equations:

$$\sum_{j=0}^{w} (Z_j^{i+n} - Z_j^i) = 0, \quad i \in \{1 \dots n\}, \qquad (33)$$

which is equivalent to the following matricial expression:

$$M \begin{pmatrix} Z_1^n - 1 \\ \vdots \\ Z_w^n - 1 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \bmod J, \qquad (34)$$

where M is the $v \times v$ square matrix $(M_{i,j}) = \left(Z_j^i\right)$. The determinant of M is $\Delta_w(Z_1, \dots, Z_w)$ which is non zero on $Z_1^*, \dots, Z_w^*$. Then, from the Weak NullStellenSatz, there exists u such that $1 + u\Delta \in J$, i.e. $\Delta_w(Z_w)$ is invertible $\bmod J$. This implies that the matrix M is invertible $\bmod J$, and that $Z_i^n - 1 \in J$, $i \in \{1 \dots w\}$. Since the polynomials $Z_i^n - 1 \in J$ are square-free, we have that J is radical. Now the intersection of two radical ideals is radical, thus I is radical. $\square$

We can decode as follows, using the previous property. Given a code C, with defining set Q, and t its decoding radius, do the following:

(1) For each received word y, compute the set S_Q^* of its syndromes;

(2) compute a Gröbner basis G_w of $I_{N,n,t}(S_Q \mapsto S_Q^*) + \langle \sigma_{w+1}, \ldots, \sigma_v \rangle$ with $w = 1, \ldots$ until $G_w \neq \{1\}$. Then w is the weight of the error, and the Gröbner basis G_w contains the polynomials $\sigma_1 - \sigma_1^*, \ldots, \sigma_w - \sigma_w^*$.

6.2 Decoding above half the the minimum distance

We can decode using the following algorithm, with $v > t$:

(1) For each received word y, compute the set S_Q^* of its syndromes;
(2) Test $v = 1 \ldots$ incrementally until the system

$$I_{N,n,v}(S_Q \mapsto S_Q^*) + \langle \sigma_{w+1}, \ldots, \sigma_v \rangle \,, \tag{35}$$

has solutions. Note that for the first value v such it has solutions, the number of solutions if finite. If this number is one, then Theorem 10, applies. If not, then one either declares a decoding error, or can try to solve the zero-dimensional Gröbner basis, which has been obtained.

7 Efficiency considerations

7.1 The Waring system

The main problem with the system $I_{N,n,v}(S_Q \mapsto S_Q^*)$ is that it contains the S_i, $i \notin Q$, that must be eliminated. This can be a heavy computation, when the number of non syndroms is high. We introduce a new system, $I_{W,v,Q}$, constructed with the Waring formulas, given in Equation (9):

$$I_{W,v,Q} : \langle S_i + W_{v,i}(\sigma_1, \ldots, \sigma_v), \quad i \in Q \rangle \subset \mathbb{F}_2[\sigma, S_Q], \tag{36}$$

which can be specialized in the syndroms of each received word

$$I_{W,v,Q}(S_Q \mapsto S_Q^*) = \langle S_i^* + W_{v,i}(\sigma_1, \ldots, \sigma_v), \quad i \in Q \rangle \subset \mathbb{F}_{2^m}[\sigma]. \tag{37}$$

The specialized system presents the advantage that only the σ_i's appear as indeterminates in the system. We prove that this approach is well founded.

Proposition 2 *Consider the ideal* $I_{W,v} : \langle S_i + W_{v,i}(\sigma_1, \ldots, \sigma_v), \quad i \in \{1 \ldots n+v\} \rangle$. *Then the following equalities between ideals hold:*

$$I_{W,v} + \langle S_{i+n} - S_i, \quad i \in \{1 \ldots v\} \rangle + I_{\sigma,v} = I_{S,n,v} + I_{\sigma,v}, \tag{38}$$

where $I_{S,n,v}$ and $I_{\sigma,v}$ are as in Definition 5. Eliminating the Z_i's, we have:

$$I_{W,v} + \langle S_{i+n} - S_i, \quad i \in \{1 \dots v\}\rangle = I_{N,n,v}. \tag{39}$$

Proof To prove (38), write again (as a short hand notation) s_i, $i \in \{1 \dots v\}$, for the polynomial $s_i = \sum_{1 \leq j_1 < \cdots < j_i \leq v} Z_{j_1} \dots Z_{j_i}$, we have

$$\begin{aligned} I_{W,v} + \langle S_{i+n} - S_i, \quad i \in \{1 \dots v\}\rangle + I_{\sigma,v} = \\ \langle S_i + W_{v,i}(\sigma_1, \dots, \sigma_v), i \in \{1 \dots n+v\}\rangle + \langle S_{i+n} - S_i, \sigma_i + s_i, i \in \{1 \dots v\}\rangle = \\ \langle S_i + W_{v,i}(s_1, \dots, s_v), i \in \{1 \dots n+v\}\rangle + \langle S_{i+n} - S_i, \sigma_i + s_i, i \in \{1 \dots v\}\rangle = \\ \left\langle S_i + \sum_{j=1}^{w} Z_j^i, i \in \{1 \dots n+v\}; S_{i+n} - S_i, i \in \{1 \dots v\} \right\rangle + I_{\sigma,v} = I_{S,n,v} + I_{\sigma,v}. \end{aligned}$$

Now to prove (39), let G_W be a Gröbner basis of $I_{W,v} + \langle S_{i+n} - S_i, \quad i \in \{1 \dots v\}\rangle$, for any ordering such that the S_i's are greater than the σ_j's. Let $G_{\sigma,v}$ be the Gröbner basis of $I_{\sigma,v}$, given in Theorem 4, for an ordering such that Z_i's are greater than the σ_i's. Then $G_W \cup G_{\sigma,v}$ is a Gröbner basis of $I_{S,n,v} + I_{\sigma,v}$. By the Elimination Property of Gröbner bases, we have that G_W is a Gröbner basis of $I_{N,n,v}$. This proves (39). $\square$

In the remaining of the paper, the computational results that we present are obtained with the Waring system. But since we have equalities of ideals, the theoretical results of previous section holds.

7.1.0.1 Further tricks Even with the Waring polynomials, the systems can be hard to solve. We have to use several tricks. One of them is derived from Reed et al. (1992). Let us define $\tilde{Z}_j = Z_j^{-1}$, $\tilde{S}_j$ and $\tilde{\sigma}_j$ to be respectively the syndroms and elementary symmetric function associated to the $\tilde{Z}_j$. Then the following relations hold: $\tilde{S}_i = S_{n-i}$, and $\sigma_j = \sigma_v \tilde{\sigma}_{v-j}$ Then

$$S_i = W_{v,i}(\sigma_1, \dots, \sigma_v) = \tilde{S}_{n-i} = W_{v,n-i}(\frac{\sigma_{v-1}}{\sigma_v}, \dots, \frac{1}{\sigma_v}). \tag{40}$$

Clearing out denominators in (40) gives a formula $\sigma_v^{n-i} S_i = \tilde{f}_{n-i}(\sigma_1, \dots, \sigma_v)$ which has degree $n - i + 1$ instead of i.

Another practical remark is that it is not always necessary to use all the defining set. The algebraic system $I_{W_v,Q'}(S_{Q'} \mapsto S^*_{Q'})$ can also lead to the basis $\sigma_i - \sigma_i^*$, $i \in \{1 \dots v\}$ when $Q' \subsetneq Q$, yet for decoding the same code. So a strategy is to remove from the system $I_{W,v,Q}$ the equations $S_i^* = W_{v,i}(\sigma_1, \dots, \sigma_v)$ where i is large, while the number of solutions is still one.

The historical method for computing Gröbner bases is Buchberger's algorithm Buchberger B. (1965, 1970, 1976, 1979, 1985). It has several variants and it is implemented in most general computer algebra systems like Maple or Magma. The computation of Gröbner bases using Buchberger's algorithm is suffering from two problems:

- (A) arbitrary choices: the order in which the computations are done does not affect the result of the algorithm but my dramatically influence the computation time. Empirical strategies have been proposed (for instance the sugar strategy) but this is far from optimal.
- (B) useless computations: most of the time is spent reducing polynomials to 0. Criteria have been proposed by Buchberger B. (1970) to remove some useless critical pairs but still 90% of the computation is spent reducing polynomials to 0.

For problem (A), J.C. Faugère proposed (Faugère J.C. (1999) - algorithm F_4) a new generation of algorithms (Faugère J.C. (1999)) relying on the intensive use of linear algebra : the arbitrary choices are left to computational strategies related to classical linear algebra problems (computation of a row echelon form for instance). For the second problem (B), J.C. Faugère proposed (Faugère J.C. (2002)) a new criterion for detecting useless computations. Under some regularity conditions on the system, it is proved that the algorithm do never perform useless computations. A new algorithm named F_5 has been built using these two results. Even if the new algorithm still computes the same Gröbner basis, the gap with the original Buchberger's algorithm is large.

The idea of F_5 algorithm is to construct incrementally the following matrices *in degree d*:

$$A_d = \begin{array}{c} \\ t_1 f_1 \\ t_2 f_2 \\ t_3 f_3 \\ \dots \end{array} \begin{array}{c} m_1 > m_2 > m_3 \dots \\ \begin{bmatrix} \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \end{bmatrix} \end{array}$$

where the indices of the columns are the monomials m_j of degree d sorted for the admissible ordering $<$ and the rows are product of some polynomials f_i by some monomials t_j such that $\deg(t_j f_i) \leq d$. Each element of the matrix is then the coefficient of $t_i f_j$ with respect to the monomial m_k. For a regular system Bardet (2004); Bardet, Magali and Faugère, Jean-Charles and Salvy, Bruno (2005); Bardet et al. (2004) the matrices A_d are of full rank. In a second step, row echelon forms of theses matrices are computed, i.e.

$$\tilde{A}_d = \begin{array}{c} \\ t_1 f_1 \\ t_2 f_2 \\ t_3 f_3 \\ \dots \end{array} \begin{array}{c} m_1\ m_2\ m_3\ \dots \\ \begin{bmatrix} 1 & 0 & 0 & \dots \\ 0 & 1 & 0 & \dots \\ 0 & 0 & 1 & \dots \\ 0 & 0 & 0 & \dots \end{bmatrix} \end{array}$$

Next, the computation can be be pursued in degree $d + 1$.

7.3 Trace of the precomputation

In the above methods, when the CPU time is rather small (say less than 1 second) most of the time is spent generating matrices (see section 7.2); hence we further improve these timings, by using code generation techniques. More precisely, we first pick randomly an error of weight τ and then compute the Gröbner basis using FGb. For each *arithmetic operation* done in this step we translate the corresponding instruction into the C language. The next step is to compile the generated program (this is the most time consuming part of the whole computation) and we obtain a binary program. All this process can be viewed as a preprocessing and has to be done only once. Later, when a new message is received we compute the new values of the known syndromes and we have just to execute the binary program on these values. Actually, using this code generation technique we can speed up the computation by a factor of more that 1000. Let us explain how to achieve this gain.

Considering the computation of a Gröbner basis of the Waring system $I_{W,v,Q}(S_Q \mapsto S^*_{Q,0})$ where $S^*_{Q,0}$ is the set of syndroms of a given error e_0 of weight v_0, we can record the trace of this precomputation (in our case we record the trace of the construction of all the matrices, as a compiled C program).

Now let e be another error of weight v_0, we can run the C program on the syndroms S^*_Q of this error e. It successively constructs matrices, in exactly the same way as for e_0, and perform linear algebra on it, as for e_0. These considerations lead the following algorithm:

- *Preprocessing:* compute a Gröbner basis for $I_{W,v,Q}(S^*_{e_0})$ for a randomly chosen error e_0 of weight v, and record the trace of all linear algebra computations performed (for instance as a C program).
- *Decoding:* for an error e, execute the C program on $I_{W,v,Q}(S^*_e)$ and get the

values of the σ_j's.

The linear algebraic operations performed during the execution of the C program correspond in terms of polynomials to operations in the ideal $I_{W,v,Q}(S_Q \mapsto S_Q^*)$, i.e. all the polynomials we obtain are polynomials in I_e. If we get a result $G = \{g_0, \dots, g_s\}$ from the execution of the program, then we are sure that $g_i \in I_e$ for all i, and that the solutions are such that $V(\langle g_0, \dots, g_s \rangle) \supset I_{W,v,Q}(S_Q \mapsto S_Q^*)$. If the system G has only one solution, we are certain that it is the only solution of $I_{W,v,Q}(S_Q \mapsto S_Q^*)$. If $V(\langle g_0, \dots, g_s \rangle)$ contains more than one solution, we know at least that the solution of $I_{W,v,Q}(S_Q \mapsto S_Q^*)$ is one of the solutions of $V(\langle g_0, \dots, g_s \rangle)$.

The benefits of using such a C program instead of using a generic algorithm for computing Gröbner basis is the gain in efficiency. Indeed, the C program only performs linear algebra operations, in a prescribed manner. Using an analogy, it is the same as performing a Gaussian elimination with all the pivoting elements and the row operations known in advance.

Let us note that the execution of the C program succeed only if the error e has the same weight v as e_0. For a given code C correcting t errors, a decoding algorithm consists in t programs $P_1, \dots, P_t$, one for each possible weight. To decode, execute the programs in sequence, starting from P_1 to P_t, until the resulting system does not contain 1.

Note that now, contrarily to the computation of a Gröbner basis using a general algorithm, we are able to predict the time needed for the decoding. As we only perform linear algebra, we can give explicitly the number of arithmetic operations in the field $\mathbb{F}_{2^m}$ that are needed to decode a word.

8 Results and tables

We will present experimental results for seven codes, which seem to be relevant. Let us first describe the codes, the results are compiled in Table 1. We also compare our experimental running times with estimation of the number operations of Information Set Decoding, that could be used for instance for the codes presented here, except the BCH codes.

8.1 Quadratic residue codes

We pick quadratic residue codes of length bigger than one hundred. For this we use the Table given in Grassl (2000). Because of implementation reasons, we could only deal with quadratic residue whose length n is such that the

Code	error of weight w (**#sols**)	Number of operations	Elapsed time	Exhaustive search	Information set decoding
QR 89 [89,45,7]	8	$2^{19.9}$	$6.1\,10^{-2}$ s	2^{36}	$[2^{21}, 2^{28}]$
QR 113 [113,57,7]	7	$2^{15.2}$	$5.9\,10^{-3}$ s	$2^{35.1}$	
QR 127 [127,64,19]	9	$2^{26.7}$	0.3 s	2^{44}	$[2^{23}, 2^{30}]$
BCH [255,147,31]	15	$2^{7.2}$	$4.2\,10^{-7}$ s		
	16	$2^{8.1}$	$7.3\,10^{-7}$ s		$[2^{36.0}, 2^{44.0}]$
	17(**3**)	$2^{8.9}$	$1.4\,10^{-6}$ s		$[2^{36.0}, 2^{44.0}]$
	18(**18**)	$2^{15.6}$	$1.4\,10^{-4}$ s		$[2^{36.0}, 2^{44.0}]$
BCH [511,103,127]	62	2^{11}	$5.7\,10^{-6}$ s		
	63	$2^{11.5}$	$8.1\,10^{-6}$ s		$[2^{40.0}, 2^{49.0}]$
	66	$2^{12.1}$	$1.2\,10^{-5}$ s		$[2^{41.1}, 2^{50.1}]$
	70	$2^{14.9}$	$8.5\,10^{-5}$ s		$[2^{42.6}, 2^{51.6}]$
	74	$2^{18.4}$	$9.6\,10^{-4}$ s		
	77	$2^{20.9}$	$5.3\,10^{-3}$ s		
	78	$2^{22.3}$	$1.3\,10^{-2}$ s		
Tjhai106 [151,106, 13]	6	$2^{11.9}$	$3.2\,10^{-4}$ s	2^{33}	$[2^{25}, 2^{32}]$
Tjhai76 [151,76,23]	11	$2^{32.3}$	440 s	2^{53}	$[2^{26}, 2^{33}]$

Fig. 1. Experimental results. We give rough estimates for Information Set Decoding: an too optimistic bound with respect to Canteaut and Chabaud (1998), and a too pessimistic bound with respect to Barg (1998).

splitting field of $X^n - 1$ is $\mathbb{F}_{2^m}$, with m such that $m \leq 32$. Thus we consider the following codes:

(1) The quadratic residue code of length 89, minimum distance 15, t=7.
(2) The quadratic residue code of length 113, minimum distance 15, t=7.
(3) The quadratic residue code of length 127, minimum distance 19, t=9.

8.2 BCH codes

To show how we can decode up to half the minimum distance, and eventually above, we give computational times for some BCH codes, whose minimum distance is higher then the BCH bound. For these codes, the classical decoding algorithms (Euclidean Algorithm, or Berlekamp-Massey algorithm), can only decode up to half the BCH bound minus one. We consider two examples:

(1) the BCH code of length 255, which has designed distance 29, true minimum distance 31, thus t=15,
(2) and the BCH code of length 511, designed distance 123, and true minimum distance 127 (thus t=63) Augot et al. (1992).

8.3 Some optimal cyclic codes

From Tjhai et al. (2006), we consider two cyclic codes of length 151, which beat the BCH codes in terms of minimum distance, and which are as good as the best known codes in Brouwer's table[1].

(1) a [151,106, 13] code. We call this code Tjhai106.
(2) a [151,76,23] code. We call this code Tjhai76.

To the best of our knowledge, there is no dedicated decoding algorithms for these codes.

9 Conclusion

We have studied in details the ideal generated by the Newton's identities, which can be used for decoding any cyclic codes, up to half its minimum distance. First we have studied the variety associated to the Newton's identities, and then we have shown that there exists relevant polynomials for decoding in this ideal, when we add the "field equations" to it. However, the computation of Gröbner basis of this ideal is impractical, and even in the case when the formulas are obtained, they are too huge to be efficiently evaluated.

Thus we turned to online computation of Gröbner bases, which are more practical. First we are able to prove theoretical results about the ideal of Newton's identities, without the field equations, when specialized on the syndromes. These results justify the use of Gröbner bases: the ideal contains the relevant $\sigma - \sigma_i^*$, where the σ_i^* are the coefficients of the locator polynomial.

Finally using recent algorithms and software tools for computing Gröbner bases, we obtain reasonable times for relevant codes of length of more then one hundred.

[1] `http://www.codetables.de/`

References

Augot, D., Bardet, M., Faugère, J.-C., 2003. Efficient decoding of (binary) cyclic codes above the correction capacity of the code using Gröbner bases. In: Proceedings of the 2003 IEEE International Symposium on Information Theory. pp. 362–362.

Augot, D., Charpin, P., Sendrier, N., 1992. Studying the locator polynomial of minimum weight codewords of BCH codes. IEEE Transactions on Information Theory 38 (3), 960–973.

Bardet, M., 2004. Étude des systèmes algébriques surdeterminés. Applications aux codes correcteurs et à la cryptographie. Ph.D. thesis, Université Paris 6.

Bardet, M., Faugère, J., B., S., Nov. 2004. On the complexity of gröbner basis computation of semi-regular overdetermined algebraic equations. In: Valibouze, A. (Ed.), ICPSS Paris. pp. 71–75.

Bardet, Magali and Faugère, Jean-Charles and Salvy, Bruno, 2005. Asymptotic expansion of the degree of regularity for semi-regular systems of equations. In: Gianni, P. (Ed.), Mega 2005 Sardinia (Italy). 15 pages.

Barg, A., 1998. Complexity issues in coding theory. In: Pless, V. S., Huffman, W. C. (Eds.), Handbook of Coding Theory. Vol. I. North-Holland.

Buchberger B., 1965. Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. Ph.D. thesis, Innsbruck.

Buchberger B., 1970. An Algorithmical Criterion for the Solvability of Algebraic Systems. Aequationes Mathematicae 4 (3), 374–383, (German).

Buchberger B., 1976. A theoretical basis for the reduction of polynomials to canonical forms. ACM SIGSAM Bull. 39, 19–29.

Buchberger B., 1979. A Criterion for Detecting Unnecessary Reductions in the Construction of Gröbner Basis. In: Proc. EUROSAM 79. Vol. 72 of Lect. Notes in Comp. Sci. Springer Verlag, pp. 3–21.

Buchberger B., 1985. Gröbner Bases : an Algorithmic Method in Polynomial Ideal Theory. In: Reidel Publishing Company (Ed.), Recent trends in multidimensional system theory. Bose, Ch. 6, pp. 184–232.

Caboara, M., Mora, T., 2002. The Chen-Reed-Helleseth-Truong decoding algorithm and the Gianni-Kalkbrenner Gröbner shape theorem. Applicable Algebra in Engineering, Communication and Computing 13 (3), 209–232.

Canteaut, A., Chabaud, F., 1998. A new algorithm for finding minimum-weight words in a linear code: application to mceliece's cryptosystem and to narrow-sense bch codes of length 511. Information Theory, IEEE Transactions on 44 (1), 367–378.

Chang, Y., Truong, T.-K., Reed, I. S., Cheng, H. Y., Lee, C. D., 2003. Algebraic decoding of (71, 36, 11), (79, 40, 15), and (97, 49, 15) quadratic residue codes. IEEE Transactions on Communications 51 (9), 1463–1473.

Chen, X., Reed, I. S., Helleseth, T., Truong, T. K., September 1994a. General principles for the algebraic decoding of cyclic codes. IEEE Transactions on

Information Theory 40 (5), 1661–1663.
Chen, X., Reed, I. S., Helleseth, T., Truong, T. K., 1994b. Use of Gröbner bases to decode binary cyclic codes up to the true minimum distance. IEEE Transactions on Information Theory 40 (5), 1654–1661.
Chen, X., Reed, I. S., Truong, T.-K., 1994c. Decoding the (73, 37, 13) quadratic residue code. IEE Proceedings on Computers and Digital Techniques 141 (5), 253–258.
Chien, R. T., 1964. Cyclic decoding procedures for Bose-Chaudhuri-Hocquenghem codes. IEEE Transactions on Information Theory 10 (4), 357–363.
Cooper III, A. B., 1990. Direct solution of BCH syndrome equations. In: Arkian, E. (Ed.), Communications, Control, and Signal Processing. Elsevier, pp. 281–286.
Cooper III, A. B., 1991a. Finding BCH error locator polynomials in one step. Electronics Letters 27 (22), 2090–2091.
Cooper III, A. B., 1991b. A one-step algorithm for finding BCH error locator polynomials. In: International Symposium ion Information Theory, ISIT 1991. pp. 93–93.
Cox, D., Littel, J., O'Shea, D., 1992. Ideals, Varieties and Algorithms. Springer.
Cox, D. A., Little, J., O'Shea, D., March 2005. Using Algebraic Geometry. Graduate Texts in Mathematics. Springer.
de Boer, M., Pellikaan, R., 1999a. Gröbner bases for codes. In: Cohen, A. M., Cuypers, H., Sterk, H. (Eds.), Some tapas in computer algebra. No. 4 in Algorithms and Computation in Mathematics. Springer, pp. 237–259.
de Boer, M., Pellikaan, R., 1999b. Gröbner bases for decoding. In: Cohen, A. M., Cuypers, H., Sterk, H. (Eds.), Some tapas in computer algebra. No. 4 in Algorithms and Computation in Mathematics. Springer, pp. 260–275.
Eisenbud, D., 1995. Commutative Algebra with a View Toward Algebraic Geometry. Vol. 150 of Graduate Texts in Mathematics. Springer-Verlag.
Faugère J.C., June 1999. A new efficient algorithm for computing Gröbner bases (F4). Journal of Pure and Applied Algebra 139 (1–3), 61–88.
Faugère J.C., July 2002. A new efficient algorithm for computing Gröbner bases without reduction to zero F5. In: T. Mora (Ed.), Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation. ACM Press, pp. 75–83, isbn: 1-58113-484-3.
Gianni, P., 1989. Properties of Gröbner bases under specializations. In: Davenport, J. (Ed.), Eurocal '87: European Conference on Computer Algebra, Leipzig GDR. Vol. 378 of Lecture Notes in Computer Science. Springer, pp. 293–297.
Grassl, M., 2000. On the minimum distance of some quadratic-residue codes. In: 2000 IEEE International Symposium on Information Theory (ISIT). Sorento, pp. 253–253.
He, R., Reed, I. S., Truong, T.-K., Chen, X., 2001. Decoding the (47,24,11) quadratic residue code. IEEE Transactions on Information Theory 47 (3),

1181–1186.
Kalkbrener, M., 1989. Solving systems of algebraic equations by using gröbner bases. In: EUROCAL '87 (Leipzig, 1987). Vol. 378 of Lecture Notes in Computer Science. Springer, pp. 282–292.
Lidl, R., Niederreiter, H., October 1996. Finite Fields. Encyclopedia of Mathematics and its Applications. Cambridge University Press.
Loustaunau, P., York, E. V., 1997. On the decoding of cyclic codes using Gröbner bases. Applicable Algebra in Engineering, Communication and Computation 8 (6), 469–483.
Lu, E. H., Wuu, H. P., Cheng, Y. C., Lu, P. C., 1995. Fast algorithms for decoding the (23,12) binary Golay code with four-error-correcting capability. International Journal of Systems Science 26 (4), 937–945.
Macwilliams, F. J., Sloane, N. J. A., January 1983. The Theory of Error-Correcting Codes. North-Holland Mathematical Library. North Holland.
Orsini, E., Sala, M., August 2005. Correcting errors and erasures via the syndrome variety. Journal of Pure and Applied Algebra 200 (1-2), 191–226.
Orsini, E., Sala, M., 2007. General error locator polynomials for binary cyclic codes with $tle2$ and $n < 63$. IEEE Transactions on Information Theory 53 (3), 1095–1107.
Reed, I. S., Truong, T.-K., Chen, X., Yin, X., 1992. The algebraic decoding of the (41, 21, 9) quadratic residue code. IEEE Transactions on Information Theory 38 (3), 974–986.
Reed, I. S., Yin, X., Truong, T.-K., 1990a. Algebraic decoding of the (32, 16, 8) quadratic residue code. IEEE Transactions on Information Theory 36 (4), 876–880.
Reed, I. S., Yin, X., Truong, T.-K., Holmes, J. K., 1990b. Decoding the (24,12,8) golay code. Computers and Digital Techniques, IEE Proceedings-137 (3), 202–206.
Tjhai, C., Tomlinson, M., Grassl, M., Horan, R., Ahmed, M., Ambroze, M., 2006. New linear codes derived from binary cyclic codes of length 151. IEE Proceedings on Communications 153 (5), 581–585.
Truong, T.-K., Chang, Y., Chen, Y.-H., Lee, C. D., 2005. Algebraic decoding of (103, 52, 19) and (113, 57, 15) quadratic residue codes. IEEE Transactions on Communications 53 (5), 749–754.
Valibouze, A., 1995. Modules de cauchy, polynômes caractéristiques et résolvantes. Tech. Rep. 1995-131, LIAFA.