HAL
archives-ouvertes.fr

Efficient Decoding of (binary) Cyclic Codes beyond the correction capacity of the code using Gröbner bases

Daniel Augot, Magali Bardet, Jean-Charles Faugère

▶ **To cite this version:**

Daniel Augot, Magali Bardet, Jean-Charles Faugère. Efficient Decoding of (binary) Cyclic Codes beyond the correction capacity of the code using Gröbner bases. [Research Report] RR-4652, INRIA. 2002. inria-00071933

HAL Id: inria-00071933
https://hal.inria.fr/inria-00071933

Submitted on 23 May 2006

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Efficient Decoding of (binary) Cyclic Codes beyond the correction capacity of the code using Gröbner bases

Daniel Augot — Magali Bardet — Jean-Charles Faugère

N° 4652

Novembre 2002

THÈME 2

ISSN 0249-6399 ISRN INRIA/RR--4652--FR+ENG

INRIA
LORRAINE

Efficient Decoding of (binary) Cyclic Codes beyond the correction capacity of the code using Gröbner bases

Daniel Augot , Magali Bardet , Jean-Charles Faugère

Thème 2 — Génie logiciel
et calcul symbolique
Projets CODES et SPACES

Rapport de recherche n° 4652 — Novembre 2002 — 25 pages

Abstract: The problem of decoding cyclic codes can be rewritten into an algebraic system of equations, whose solutions are closely related to the error that occured. Extensive work has been done previously, where it has been shown that the computation of a Gröbner basis of this algebraic system enables to decode up to the true minimum distance. The Gröbner basis computation can be done either as a preprocessing (*formal decoding*), with the parameters taken as variables, or for each word to be decoded (*online decoding*), with the parameters computed from the word and substituted into the system. For the formal decoding, it has been shown that decoding formulas for the coefficients of the locator polynomial are obtained from the formal Gröbner basis. Unfortunately, it becomes quickly impossible to compute this formal Gröbner basis even for codes of small length.

Motivated by the problem of decoding quadratic residue (QR) codes, for which no general decoding algorithm is known, we improve on several points. First we introduce modified systems, without high degree equations, for which the Gröbner basis computation is easier. This enables to compute the formal Gröbner basis for longer codes.

We show on the example of the [41,21,9] QR code that the formulas become quickly of large size, thus being useless for decoding. This indicates that the effort on the algebraic decoding of cyclic codes by formulas hits a wall. The other approach (*online* decoding) is more efficient from a computational point of view. Using general compilation methods for systems with parameters, we improve the efficiency of the computation. Many examples are given (for BCH codes of length 75, 511, for QR codes of length 41, 73, 89, 113 and for a code of length 75 which does not belong to a known class of codes).

This method for decoding cyclic codes with Gröbner basis works for *any* cyclic codes, is *automatic* and enables to decode *beyond* the true minimum distance.

Key-words: decoding; cyclic codes; ideal theory; Gröbner bases; error-locator polynomial; Newton identities

Unité de recherche INRIA Lorraine
LORIA, Technopôle de Nancy-Brabois, Campus scientifique,
615, rue du Jardin Botanique, BP 101, 54602 Villers-Lès-Nancy (France)
Téléphone : +33 3 83 59 30 00 —Télécopie : +33 3 83 27 83 19

Décodage efficace de codes cycliques binaires au delà de la capacité de correction du code en utilisant des bases de Gröbner

Résumé : Le problème du décodage des codes cycliques peut se réécrire en un système algébrique dont les solutions sont étroitement liées à l'erreur qui s'est produite. Les travaux précédents ont montré que le calcul d'une base de Gröbner de ce système algébrique permet de décoder jusqu'à la distance minimale du code. Le calcul de base de Gröbner peut se faire soit en prétraitement (*décodage formel*), les paramètres étant considérés comme des variables, soit pour chaque mot à décoder (*décodage en ligne*), en calculant pour chaque mot les paramètres et en les substituant dans le système. Dans le cas du décodage formel, il a été montré qu'il est possible d'obtenir à partir de la base de Gröbner formelle des formules de décodage pour les cœfficients du polynôme localisateur. Malheureusement, il devient rapidement impossible de calculer cette base de Gröbner formelle, même pour des code de petite longueur.

Motivés par le problème du décodage des codes à résidus quadratiques (codes RQ), pour lesquels il n'existe aucun algorithme général de décodage actuellement, nous améliorons les résultats sur plusieurs points. D'abord, nous introduisons des systèmes modifiés, sans équations de degré élevé, pour lesquels le calcul de la base de Gröbner est plus facile. Ceci permet de calculer la base de Gröbner en formel pour des codes de plus grande longueur.

Nous montrons sur l'exemple du code RQ de type [41,21,9] que les formules deviennent rapidement de grande taille, et sont donc inutilisables pour le décodage. Cela indique que les efforts développés pour le décodage algébrique des codes cycliques par formules ont peu de chance d'aboutir. L'autre approche (décodage *en ligne*) est plus efficace d'un point de vue informatique. En utilisant des méthode de compilation générales pour des systèmes avec paramètres, nous améliorons l'efficacité des calculs. Nous donnons de nombreux exemples (codes BCH de longueur 75, 511, codes RQ de longueur 41, 73, 89, 113 et un code de longueur 75 qui n'appartient a aucune classe connue de codes cycliques).

Cette technique de décodage des codes cycliques avec des bases de Gröbner s'applique à n'importe quel code, et entièrement automatique et permet de décoder au delà de la capacité de correction du code.

Mots-clés : décodage; codes cycliques; idéaux; bases de Gröbner; polynôme localisateur d'erreur; identitées de Newton

1 Introduction

The problem of decoding cyclic codes up to their true minimum distance can be solved by the use of Gröbner bases [CRHT94c, CRHT94b, LVY97]. The principle is to rewrite the decoding problem into an algebraic system of equations, which must have the following properties:

1. *Decoding property* : its solutions are closely related to the error,
2. *Computational property* : the computation of its solutions can be done in reasonable time.

The Gröbner basis computation can be done either as a preprocessing, with the parameters taken as variables, or for each word to be decoded, with the parameters computed from the word and substituted into the system. In the first case (*formal decoding*), we get formulas and to decode a word, we just have to compute the parameters and to evaluate the formulas. In the second case (*online decoding*), for each word we compute the parameters and a Gröbner basis of the specialized system (the system after substitution). In the online case, each system has less variables and the Gröbner basis is much easier to compute than in the formal case.

This idea has been considered first in [CRHT94a], using the expression of syndroms in terms of the locators of the error, and the results were demonstrated by Loustaunau and Von York [LVY97], providing a decoding algorithm with Gröbner basis precomputations. Unfortunately, it is often impossible to compute the formal Gröbner basis, even for the QR code of length 41. In parallel, Newton's identities have been extensively used, one tries to find formulas for the coefficient of the locator polynomial in terms of known syndroms. This has been applied notably to the QR codes - [RYT90, RTCY92, RRTC01, CRT94] for binary codes, and [Hum92, HH93] for ternary codes. QR codes are good codes - their dimension is about one half of their length and they have a good correction capacity - but no general decoding algorithm exists for them, such as the Berlekamp-Massey algorithm [Ber68] for the particular case of BCH codes. In those papers, the authors derive a specific construction for each particular quadratic residue code.

Motivated by the problem of decoding QR codes, we improve on several points. We introduce new systems of *positive dimension* (infinite number of solutions), whilst previous studied systems are of *dimension zero* (finite number of solutions). These new systems still have the decoding property, and do not contain any more some high degree polynomials which made the computation of the Gröbner basis intractable. In practice they behave much better for the computational point of view.

We show on the example of the [41,21,9] QR code that the size of formulas obtained in the formal Gröbner basis is too large to be useful, since for each word it will take too much time to evaluate them. Hence, even if the formal computation can be achieved, the online decoding approach seems to be the most efficient one. We get efficient and automatic decoding algorithms, which work for *any* cyclic code and enables to decode *beyond* the true minimum distance. Many examples of decoding are given (for BCH codes of length 75, 511,

for QR codes of length 41, 73, 89, 113 and for a code of length 75 which does not belong to a known class of codes). Moreover, using a general compilation method useful for systems with parameters, we improve the efficiency of our algorithms: for each cyclic code, we automatically generate a C program which, executed on any word, gives the corresponding solution without computing directly a Gröbner basis. For any of these programs, we know exactly the complexity of the decoding algorithm (i.e. the number of arithmetic operations).

The online decoding with Gröbner basis computation is an automatic method, which works for any cyclic code and is not limited by the correction capacity of the code. In fact for any weight v, we get the list of all the codewords at distance less then or equal to v from the transmitted word.

The paper is organized as follows: in Section 2 we remind basic facts on cyclic codes and syndroms, and also on Gröbner bases, elimination theory and specialization theory. The Section 3 is devoted to the case of zero-dimensional ideals, as previously studied in [LVY97, CRHT94a]. In Section 4 we introduce new systems of positive dimension, and show that they satisfy the decoding property. We study the size of the formal formulas for the [41,21,9] QR code. Finally Section 5 presents various examples of online decoding and the compilation method used for more efficiency.

2 Notations and definitions

2.1 Cyclic codes and Newton's identities

The reader is assumed to be familiar with the theory of cyclic codes (see e.g. [MS77]). Let $\mathcal{C}$ be a cyclic code over $\mathbb{F}_2$ of odd length n, of dimension k, of minimal distance d and correction capacity $t = \lfloor \frac{d-1}{2} \rfloor$. $\mathcal{C}$ is completely defined by its defining set $\mathcal{Q} = \{i_1, \ldots, i_q\} \subset \{1, \ldots, n\}$, which is an union of cyclotomic cosets modulo n. Let $\alpha \in \mathbb{F}_{2^m}$ be a primitive n-th root of unity, where $\mathbb{F}_{2^m}$ is the splitting field of $x^n - 1$, then $g(x) = \prod_{i \in \mathcal{Q}} (x - \alpha^i)$ is the generator polynomial of $\mathcal{C}$.

Let $c = a(x)g(x)$ be a code word and $\tilde{c} = c + e$ be the received word, where $e(x) = \sum_{r=0}^{n-1} e_r x^r$ is the error of weight v which occurred. If $r_1, \ldots, r_v$ locate the positions of the non-zero e_r's, let $Z_j = \alpha^{r_j}$ for $1 \leq j \leq v$ denote the locators of the error. As $c(\alpha^i) = 0$ for $i \in Q$, we can compute the syndroms $S_i^* = e(\alpha^i) = \tilde{c}(\alpha^i)$. Throughout this paper we shall distinguish an actual value from an indeterminate (variable) by appending a $*$ to it. For instance S_1^* is a value given to the indeterminate S_1.

The locators satisfy the system of equations

$$\text{POWER FUNCTIONS} \quad \left\{ S_i - \sum_{j=1}^{v} Z_j^i, \qquad \forall\, i \in Q. \right. \tag{1}$$

specialized for $S_i = S_i^*$.

The locator polynomial is defined from the Z_j's as $L(Z) = \prod_{j=1}^{v}(Z - Z_j) = Z^v + \sigma_1 Z^{v-1} + \cdots + \sigma_{v-1}Z + \sigma_v$ where the σ_j's are the elementary symmetric functions of the Z_j's. We use the notations: $\underline{Z_v} = (Z_j)_{j\in[1,v]}$, $\underline{\sigma_v} = (\sigma_j)_{j\in[1,v]}$, $\underline{S} = (S_i)_{i\in Q}$, $\overline{S} = (S_i)_{i\notin Q}$.

To correct the error, we have to recover $\underline{Z_v}$ from $\underline{S}$, or equivalently to recover $\underline{\sigma_v}$ from $\underline{S}$ (then using Chien search [Chi64] it is easy to compute the set $\underline{Z_v}$ from $\underline{\sigma_v}$).

Definition 1 *Let $\overline{\mathbb{F}}_2$ denote the algebraic closure of $\mathbb{F}_2$. The Fourier transform of $a = \sum_{r=0}^{n-1} a_r x^r \in \overline{\mathbb{F}}_2[x]/(x^n - 1)$ is the polynomial $S(Z) = \sum_{i=1}^{n} S_i Z^{n-i} \in \overline{\mathbb{F}}_2[Z]$, where $S_i = a(\alpha^i)$ for all $i \in [1, n]$. It is also called the Mattson-Solomon polynomial of a.*

Proposition 2 *The Fourier transform is a one-to-one application from $\overline{\mathbb{F}}_2^n$ to itself.*

With these notations, we have $S_i = \sum_{j=1}^{v} Z_j^i$ for $1 \le i \le n$, and the knowing of the Fourier transform of the error is equivalent to the knowing of the error itself. However, we do not have acces to the whole Fourier transform of the error, but only to the syndrom.

Proposition 3 ([RTCY92] pp. 981)
The map $S : \left(\begin{array}{ccc} \{\text{word of weight} \le t\} & \longrightarrow & \mathbb{F}_{2^m}^q \\ e & \longmapsto & \underline{S}^* = \{e(\alpha^i) : i \in \mathcal{Q}\} \end{array} \right)$ *is injective.*

As long as the weight of the error is less than t, the decoding is possible with the knowledge of the sole syndroms.

Proposition 4 *Let $e \in \mathbb{F}_2[x]/(x^n-1)$ be a word of Hamming's weight v, then the associated S_i^*'s and σ_j^*'s are solutions of the following systems of equations:*

- *the generalized Newton's identities* (NEWGEN_v)*:*

$$\begin{cases} S_v + \sigma_1 S_{v-1} + \cdots + \sigma_v S_1 \\ S_{v+1} + \sigma_1 S_v + \cdots + \sigma_v S_2 \\ \vdots \\ S_{v+n-1} + \sigma_1 S_{v+n-2} + \cdots + \sigma_v S_{n-1} \\ S_{i+n} + S_i \end{cases} \tag{2}$$

- *the triangular Newton's identities* (NEWTRI_v)*:*

$$\left\{ S_i + \sum_{j=1}^{i-1} \sigma_j S_{i-j} + i\sigma_i \quad \forall i \in [1, v]. \right. \tag{3}$$

Proposition 5 ([Aug96] pp. 144) *: Let $S^* \in \mathbb{F}_{2^m}^n$ be the Fourier transform of a word $e \in \mathbb{F}_2[x]/(x^n-1)$ of Hamming's weight v_e with $v_e \le v$, and let $L_e(Z)$ be the locator polynomial of e. Then, the set $\{(\sigma_1, \ldots, \sigma_v) \in \overline{\mathbb{F}}_2^n |\ (\sigma_1, \ldots, \sigma_v, S^*)$ is a solution of the system $\text{NEWGEN}_v\}$ is the affine subspace of $\overline{\mathbb{F}}_2^n$ of dimension $v - v_e$ defined by:*

$$\left\{ (\sigma_1, \ldots, \sigma_v) \in \overline{\mathbb{F}}_2^n |\ L_e(Z) \text{ divides } Z^v + \sum_{i=1}^{v} \sigma_i Z^{v-i} \right\}.$$

There are several systems derived either from (1) or from (2) and (3) which satisfy the Decoding property, but as long as Gröbner basis computation is used, the computational times for finding their solutions vary a lot.

2.2 Gröbner bases

For this section, the reader can refer to [CLO97] for more details on ideals, Gröbner bases, and polynomial system solving.

Definition 6 *Let k be a field, a* monomial ordering *on the polynomial ring $k[X_1, \ldots, X_n]$ is any total ordering $<$ on the set of monomials, satisfying:*

- *if m_1, m_2 and m_3 are monomials, then $m_1 < m_2 \Rightarrow m_1 m_3 < m_2 m_3$,*
- *for any monomial m we have $1 < m$.*

For instance, we use the following monomial orderings:

Definition 7 *Lexicographic Order (Lex Order)*

$$X^\alpha = X_1^{\alpha_1} \cdots X_n^{\alpha_n} <_{lex} X_1^{\beta_1} \cdots X_n^{\beta_n} \iff \exists j \ (\alpha_i = \beta_i \quad \forall i < j) \text{ and } \alpha_j < \beta_j,$$

Definition 8 *Graded Reverse Lex Order (Grevlex)*

$$X^\alpha <_{grevlex} X^\beta \iff$$
$$(degree(\alpha) < degree(\beta)) \text{ or } (degree(\alpha) = degree(\beta) \text{ and } \exists j \ (\alpha_i = \beta_i \quad \forall i > j) \text{ and } \alpha_j < \beta_j)$$

An *elimination order* with two blocks $[X_1, \ldots, X_k] > [X_{k+1}, \ldots, X_n]$ is a monomial ordering such that any monomial involving one of $\{X_1, \ldots, X_k\}$ is greater than any monomial in $k[X_{k+1}, \ldots, X_n]$. The Lex order is an elimination order for any blocks $[X_1, \ldots, X_k]$ and $[X_{k+1}, \ldots, X_n]$.

A *degree order* is a monomial ordering $<$ such that $\text{degree}(\alpha) < \text{degree}(\beta) \Longrightarrow X^\alpha < X^\beta$.

A monomial ordering $<$ being given, we can define the *leading term* of a polynomial p with respect to $<$ as its highest term, and we denote it by $LT(p)$. Let $F = \{f_\nu\}$ be a set of polynomials, we denote by $\langle F \rangle$ the ideal generated by F.

Definition 9 *Let I be an ideal in $k[X_1, \ldots, X_n]$ and $<$ a monomial ordering. A finite subset $G = \{g_1, \ldots, g_s\}$ of I is a* Gröbner basis *of I if*

$$\langle LT(g_1), \ldots, LT(g_s) \rangle = \langle LT(I) \rangle$$

where $LT(I)$ is the set of all the $LT(p)$, for p in I.

If I is an ideal other than $\{0\}$, then I has a Gröbner basis G, and G is a basis of I. The most important property is that there exist algorithms to compute a Gröbner basis of I, for example the Buchberger algorithm ([Buc85]) or the F4 algorithm ([Fau99]).

For the $<_{lex}$ order, if I has a finite number of solutions and is "generic", a Gröbner basis G of I has the following triangular form (in general, G is equivalent to a finite number of such systems)

$$\begin{cases} X_1 + f_1(X_n) \\ \vdots \\ X_{n-1} + f_{n-1}(X_n) \\ f_n(X_n) \end{cases}$$

Using this basis of I, the computation of the solutions is now easy: if $\{z_1, \ldots, z_d\}$ are the solutions of $f_n(X_n)$, then the solutions of I are $\{(x_1 = f_1(z_i), \ldots, x_{n-1} = f_{n-1}(z_i), \ldots x_n = z_i), i = [1, d]\}$

The following two properties will be useful:

Proposition 10 (Elimination Theorem) *([CLO97] pp. 113) Let $I \subset k[X_1, \ldots, X_n]$ be an ideal and let G be a Gröbner basis of I for an elimination order with $[X_1, \ldots, X_k] > [X_{k+1}, \ldots, X_n]$. Then, the set*

$$G_k = G \cap k[X_{k+1}, \ldots, X_n]$$

is a Gröbner basis of the kth elimination ideal $I_k = I \cap k[X_{k+1}, \ldots, X_n]$.

For a given ideal $I \subset k[X_1, \ldots, X_n]$ we denote by $V(I)$ the set of solutions of I in the algebraic closure $\overline{k}$ of k, i.e.

$$V(I) = \left\{(x_1, \ldots, x_n) \in \overline{k} \mid p(x_1, \ldots, x_n) = 0,\ \forall p \in I\right\}.$$

We say that an ideal I is zero-dimensional if $V(I)$ is finite, and that I is of positive dimension if $V(I)$ is infinite.

If Π_l denote the projection on the $n-l$ last coordinates, i.e. $\Pi_l(x_1, \ldots, x_n) = (x_{l+1}, \ldots, x_n)$ then $\Pi_l(V(I)) = V(I_l)$.

The second important property is the specialization's property. It is useful when dealing with systems containing parameters.

Let $R = k[\underline{X}, \underline{Y}]$ be the ring of polynomial in $n + m$ variables, where $\underline{X} = X_1, \ldots, X_n$ and $\underline{Y} = Y_1, \ldots, Y_m$. For y in k^m we define the specialization morphism $\varphi_y : R \to k[\underline{X}]$ such that $\varphi_y(p(\underline{X}, \underline{Y})) = p(\underline{X}, y)$.

A specialization morphism φ_y and an elimination ordering $<$ with blocks $\underline{X} > \underline{Y}$ being fixed, it is natural to ask whether the specialization $\varphi_y(G)$ of a Gröbner basis G of I is a Gröbner basis of the specialized ideal $\varphi_y(I)$ (it is not always true, see [Gia89] pp. 295). For p a polynomial in $k[\underline{X}, \underline{Y}]$, we denote by $LT_{\underline{X}}(p)$ the biggest term w.r.t. $\underline{X}$ appearing in p (i.e. the leading term of p viewed as a polynomial in the variables $\underline{X}$ and coefficients in $k(\underline{Y})$) and by $LT_{\underline{X}}(I)$ the ideal generated by the $LT_{\underline{X}}(p)$ for $p \in I$.

Proposition 11 *(Specialization Theorem I)([Gia89, Kal89]) If*

$$LT(\varphi_y(I)) = \varphi_y(LT_{\underline{X}}(I))$$

then $\varphi_y(G)$ is a Gröbner basis for $\varphi_y(I)$.

Note that it is only a sufficient condition. In particular, when no leading terms of the polynomials in G specializes to zero, then $\varphi_y(G)$ is a Gröbner basis for $\varphi_y(I)$.

Corollary 12 *(Specialization Theorem - Zero dimensional case) ([Gia89]) If I is a zero-dimensional ideal, and φ_y specializes all the variables but one, i.e. $\varphi_y : k[X, \underline{Y}] \to k[X]$ then there exists a polynomial $g \in I$ such that*

- *$\varphi_y(g)$ generates $\varphi_y(I)$,*
- *$degree_X(g) = degree_X(\varphi_y(g))$.*

and g is a polynomial of minimal degree in X whose leading coefficient does not vanish under the specialization.

In the case of positive-dimensional ideals, if all the variables but one are specialized, then we still have that $\varphi_y(G)$ is a Gröbner basis for $\varphi_y(I)$:

Proposition 13 *(Specialization Theorem II)([FGT01]) Let $G = \{g_1, \ldots, g_s\}$ be a Gröbner basis of an ideal $I \subset k[X, Y_1, \ldots, Y_n]$, and φ_y a specialization of all the variables but one. Let g_m be a polynomial of G of least degree in X such that $\varphi_y(g_m) \neq 0$. Then,*

- *$\varphi_y(G)$ is a Gröbner basis of $\varphi_y(I)$,*
- *$\varphi_y(g_m)$ generates $\varphi_y(I)$, and if we note $\delta(g) = degree_X(g) - degree_X(\varphi_y(g))$ and $\delta(I) = min_{g \in I}(\delta(g))$ then $\delta(I) = \delta(g_m)$.*
- *if $\exists h \in I : \varphi_y(LT_X(h)) \neq 0$ then $degree_X(g_m) = degree_X(\varphi_y(g_m))$ and $LT(\varphi_y(I)) = \varphi_y(LT_X(I))$.*

3 Ideals of zero dimension

Here we present different systems which have already been studied ([CRHT94c, CRHT94b, LVY97, CRHT94a]). We recall their properties, in particular how the computation of a Gröbner basis provides a decoding algorithm. From the ideal point of view, all these systems are closely related, and the theorem 14 shows the link between them. From the computational point of view, these systems are rather different.

3.1 Previous systems and their properties

Two systems $(\text{SYNDROM}_v) \subset \mathbb{F}_2[\underline{Z}_v, \underline{S}]$ and $(\text{NEWTON}_v) \subset \mathbb{F}_2[\underline{S}, \overline{S}, \underline{\sigma}_v]$ are introduced in ([CRHT94c, CRHT94b]):

$$(\text{SYNDROM}_v) \begin{cases} S_i - \sum_{j=1}^{v} Z_j^i & \forall\ i \in Q \\ Z_j^{n+1} - Z_j & \forall\ j \in [1, v] \end{cases}$$

$$(\text{NEWTON}_v) \begin{cases} \sigma_j^{q^m} - \sigma_j, \quad j \in [1, v] & S_j^{q^m} - S_j \quad j \notin Q \\ S_i + \sum_{j=1}^{i-1} \sigma_j S_{i-j} + i\sigma_i, \quad i \in [1, v] \\ S_{v+i} + \sum_{j=1}^{v} \sigma_j S_{v+i-j}, \quad i \in [1, n] \end{cases}$$

The online decoding approach has been treated by Chen, Reed, Helleseth and Truong for both systems.

Theorem 14 ([CRHT94b] and [CRHT94c]) *Let $e \in \mathbb{F}_2[x]/(x^n - 1)$ be a word of Hamming's weight $v_e \leq t$, $\underline{S}^*$ be its syndroms, $\underline{\sigma}^*_{v_e}$ be the elementary symmetric functions of the locators and $L_e(Z)$ be its locator polynomial. Then*

$$\begin{aligned} \langle \text{NEWTON}_t(\underline{S}^*) \rangle \cap \mathbb{F}_{2^m}[\sigma_j] &= \langle \sigma_j - \sigma_j^* \rangle \quad \forall\ 1 \leq j \leq v_e \\ \langle \text{NEWTON}_t(\underline{S}^*) \rangle \cap \mathbb{F}_{2^m}[S_k] &= \langle S_k - \overline{S}_k^* \rangle \quad \forall k \notin Q \\ \langle \text{SYNDROM}_v(\underline{S}^*) \rangle \cap \mathbb{F}_{2^m}[Z_1] &= \langle L_e(Z_1) \rangle \text{ if } v = v_e \\ &= \langle Z_1 . L_e(Z_1) \rangle \text{ if } v = v_e + 1 \\ &= \langle Z_1^{n+1} - Z_1 \rangle \text{ if } v \geq v_e + 2 \\ &= \langle 1 \rangle \text{ if } v < v_e \end{aligned}$$

One algorithm could be:

- compute the syndroms $\underline{S}^*$ and substitute the values in the system (SYNDROM_t),
- $v = t$; while the generator polynomial g_v of the ideal $\langle \text{SYNDROM}_v(\underline{S}^*) \rangle \cap \mathbb{F}_{2^m}[Z_1]$ (computed for instance from a Gröbner basis for a lex order with $Z_i > Z_1$) is divided by Z_1 do $v = v - 1$;
- the weight of the error is $v = v_e$ and the locator polynomial is g_v,
- find the locators using Chien search.

This approach has the disadvantage that we have to compute a Gröbner basis for each word to be decoded.

The second approach ("formal decoding") was introduced by Chen, Reed, Helleseth, and Truong in [CRHT94a], considering the formal system $(\text{SYNDROM}_v) \subset \mathbb{F}_2[\underline{Z}_v, \underline{S}]$. They try to find formulas from the computation of a Gröbner basis considering $\underline{S}$ as variables. The proof of the following theorem in [CRHT94a] was based on a false claim, but Loustaunau and Von York gave in [LVY97] a valid one.

Theorem 15 ([LVY97] pp. 474) *Let G be a Gröbner basis of $I = \langle \text{SYNDROM}_t \rangle$ with respect to a Lex order such that $Z_t > Z_{t-1} > \cdots > Z_1 > \underline{S}$, and let $G_k = G \cap \mathbb{F}_2[Z_k, \ldots, Z_1, \underline{S}]$ a Gröbner basis for the $(t-k)$th elimination ideal $I \cap \mathbb{F}_2[Z_k, \ldots, Z_1, \underline{S}]$. Let 0_k be the zero vector of length k.*

Then a received word $\tilde{c} = c + e$ with syndroms $\underline{S}^*$ contains $v \leq t$ errors if and only if

$$\begin{cases} \forall k \leq t - v \quad \forall g \in G_k \quad g(0_k, \underline{S}^*) = 0 \\ \exists g \in G_{t-v+1} \quad g(0_{t-v+1}, \underline{S}^*) \neq 0 \end{cases}$$

If $G_{t-v+1} = \{g_1, \ldots, g_u\}$ then the principal ideal

$$\langle G_{t-v+1}(z, 0_{t-v}, \underline{S}^*) \rangle = \langle g_i(z, 0_{t-v}, \underline{S}^*), i \in [1, u] \rangle \subset \mathbb{F}_{2^m}[z]$$

is generated by the locator polynomial, which is one of the $g_j(z, 0_{t-v}, \underline{S}^*)$'s (up to a multiplication by an element of $\mathbb{F}_{2^m}$).

The proof of the theorem requires the following properties (see sections 2.1 and 2.2): (1) unicity of the solution, (2) the Elimination Theorem, (3) radicality of the specialized ideals, and (4) the Specialization Theorem.

We show on a single example this theorem at work. Let C be the $[23, 12, 7]$ cyclic Golay code. A Gröbner basis of (SYNDROM_3) for the lex order $Z_3 > Z_2 > Z_1 > S_1$ is

$$\begin{cases} \mathbf{Z_3} + Z_2 + Z_1 + S_1 = g_3(Z_3, Z_2, Z_1, S_1), \\ Z_2^{24} + Z_2, \\ \mathbf{Z_2^2} S_1 + Z_2 S_1^2 + S_1^{256} + S_1^3 + Z_1(Z_2 + S_1)(Z_1 + Z_2 + S_1) = g_{2,1}(Z_2, Z_1, S_1), \\ (S_1^{24} + S_1)[\mathbf{Z_2^2} + Z_2 S_1 + f_1(S_1) + Z_1(Z_2 + Z_1 + S_1)] = g_{2,2}(Z_2, Z_1, S_1), \\ Z_1^{24} + Z_1, \\ (S_1^{24} + S_1)[\mathbf{Z_1^3} + Z_1^2 S_1 + Z_1 f_1(S_1) + f_2(S_1)] = g_1(Z_1, S_1), \\ S_1^{2048} + S_1 \end{cases}$$

with f_1 (resp. f_2) an univariate polynomial of degree 1313 (resp. 1314) and 13 terms (resp. 15) :

$f_1 = S_1^{25}(S_1^{1288} + S_1^{1265} + S_1^{1127} + S_1^{1012} + S_1^{759} + S_1^{506} + S_1^{391} + S_1^{368} + S_1^{299} + S_1^{138} + S_1^{46} + S_1^{23} + 1)$

$f_2 = S_1^3(S_1^{1311} + S_1^{1288} + S_1^{1150} + S_1^{1035} + S_1^{782} + S_1^{529} + S_1^{414} + S_1^{391} + S_1^{322} + S_1^{253} + S_1^{161} + S_1^{69} + S_1^{46} + S_1^{23} + 1)$

Under specialization, if there are 3 errors, then the polynomial $g_1(Z_1, S_1^*)$ is the locator polynomial (up to a constant). If there are two errors, then one of $g_{2,2}(Z_2, 0, S_1^*)$ or $g_{2,1}(Z_2, 0, S_1^*)$ is not zero and is the locator polynomial for the error. See [LVY97] for more details about this example. We shall say that the polynomial $g_1(Z_1, S_1) \in \mathbb{F}_2[Z_1, S_1]$ is a *formula* for the locator polynomial in term of the syndrom S_1, for errors of weight 3.

We remark that the Gröbner basis contains polynomials of high degree in S_1, the polynomial $S_1^{2048} + S_1$ and polynomials of degree up to 1338. More generally for the system SYNDROM, the Gröbner basis may contain the polynomials $S_i^{2^m} + S_i$ (where $\mathbb{F}_{2^m}$ is the splitting field of $x^n - 1$ and $i \in Q$), and polynomials of degree up to 2^m in S_i. This growth of degrees is a very limiting factor for the computation of the Gröbner basis.

3.2 Equality of the elimination ideals

All the equations used being symmetric in the Z_j's, it is natural to introduce the new system (SYNSYM_v) by adding to (SYNDROM_v) the elementary symmetric functions of the Z_j's:

$$(\text{SYNSYM}_v) \begin{cases} S_i - \sum_{j=1}^{v} Z_j^i & \forall\ i \in Q \\ \sigma_j - \sum_{l_1<\cdots<l_j} Z_{l_1}\cdots Z_{l_j} & \forall\ j \in [1,v] \\ Z_j^{n+1} - Z_j & \forall\ j \in [1,v] \end{cases}$$

Proposition 16 *We have the following equality of ideals:*

$$\langle \text{SYNSYM}_v \rangle \cap \mathbb{F}_2[\underline{\sigma}_v, \underline{S}] = \langle \text{NEWTON}_v \rangle \cap \mathbb{F}_2[\underline{\sigma}_v, \underline{S}] \tag{4}$$

Proof Since both ideals are radical (thanks to the field equations $Z_j^{n+1} - Z_j$), it follows from Hilbert's NullStellenSatz that it is equivalent to prove that the varieties associated with each ideal are equal.

Let $(\underline{\sigma}_v^*, \underline{S}^*) \in V(\langle \text{SYNSYM}_v \rangle \cap \mathbb{F}_2[\underline{\sigma}_v, \underline{S}])$, then there exists $\underline{Z}_v^* \in \mathbb{F}_{2^m}^v$ such that $(\underline{Z}_v^*, \underline{\sigma}_v^*, \underline{S}^*) \in V(\text{SYNDROM}_v)$ (projection property). If we note $S_i^* = \sum_{j=1}^{v} Z_j^{*i}$ for $i \notin Q$, then $\underline{S}^*$ and the $\overline{S}^*$ are solutions together with $\underline{\sigma}_v^*$ of the (NEWTON_v) system and $(\underline{\sigma}_v^*, \underline{S}^*) \in V(\langle \text{NEWTON}_v \rangle \cap \mathbb{F}_2[\underline{\sigma}_v, \underline{S}])$.

Conversely, if $(\underline{\sigma}_v^*, \underline{S}^*) \in V(\langle \text{NEWTON}_v \rangle \cap \mathbb{F}_2[\underline{\sigma}_v, \underline{S}])$, let $Z_1^*, \ldots, Z_v^*$ be the solutions of the equation $L_v(Z) = 0$, where $L_v(Z) = Z^v + \sigma_1^* Z^{v-1} + \cdots + \sigma_v^*$, then we have $\sigma_j^* = \sum_{l_1<l_2<\cdots<l_j} Z_{l_1}^* \cdots Z_{l_j}^* \quad \forall\ j \in [1,v]$. Moreover, from the Newton's identities we can derive the relations $S_i^* + f_i(\underline{\sigma}_v^*) = 0$ where the f_i's are the Waring's functions (see [LN97] pp. 30):

$$f_i(\sigma_1, \ldots, \sigma_v) \quad = \sum_{i_1+2i_2+\cdots+vi_v=i} \frac{(i_1+i_2+\cdots+i_v-1)!}{i_1!\cdots i_v!} \cdot i \cdot \sigma_1^{i_1} \ldots \sigma_v^{i_v}$$

As

$$f_i(\sigma_1(\underline{Z}_v), \ldots, \sigma_v(\underline{Z}_v)) = f_i(Z_1 + \cdots + Z_v, \ldots, Z_1 \cdots Z_v) = Z_1^i + \cdots + Z_v^i$$

we deduce that $S_i^* = \sum_{j=1}^{v} Z_j^{*i} \quad \forall\ i \in Q$ and that $(\underline{Z}_v^*, \underline{\sigma}_v^*, \underline{S}^*) \in V(\text{SYNSYM}_v)$. Hence, $(\underline{\sigma}_v^*, \underline{S}^*) \in V(\langle \text{SYNSYM}_v \rangle \cap \mathbb{F}_{2^m}[\underline{\sigma}_v, \underline{S}])$ and as before,

$$\langle \text{SYNSYM}_v \rangle \cap \mathbb{F}_2[\underline{\sigma}_v, \underline{S}] \subset \langle \text{NEWTON}_v \rangle \cap \mathbb{F}_2[\underline{\sigma}_v, \underline{S}]$$

which concludes the proof. □

A similar result as the theorem 15 can be proved for the system (SYNSYM_v), using almost the same proof as in [LVY97]. One can also get *formulas* from the system (SYNSYM_v). The difference is that the system (SYNSYM_v) gives directly one formula for each σ_i in term of known syndroms. From the equality of ideals (4), the system (NEWTON_v) also leads to the same formulas for the σ_i's. Thus, theoretically, these systems are equivalent and lead almost to the same results, but for computational purposes, they will present very different

behaviors for Gröbner bases computations. For practical purposes, the most convenient system is (SYNSYM). Still, it is hard to compute the Gröbner basis of (SYNSYM_v) for codes of greater length. The cause of this difficulty is that (SYNSYM_t) (as the other ideals) is a zero-dimensional ideal with many solutions, more than $\frac{n^t}{t!}$ and that is contains equations of very high degree.

3.3 Example: the [31,16,7] quadratic residue code

In this paragraph we compare the behavior of the preceding systems w.r.t Gröbner bases computation on the binary quadratic residue code of length 31, which was treated by Reed et al. in [RYT90]. The binary $[31, 16, 7]$ QR code is defined by its cyclotomic set

$$Q_{31} = \{1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 25, 28\}$$

which is the set of all the squares modulo 31. This code can correct up to 3 errors. We will show that our method enables us to recover automatically the formulas found "by hand" in [RYT90].

Note that it is useless to consider the entire set Q_{31}: as soon as the set Q contains i and $2i \bmod n$, we have the relation $S_{2i \bmod n} = \sum_{j=1}^{v} Z_j^{2i} = (S_i)^2$. It is then enough to take one element for each cyclotomic coset of Q. Q_{31} contains 3 cyclotomic cosets: $Cl(1)$, $Cl(5)$ and $Cl(7)$. The systems become (simplified):

$$(\text{SYNDROM}_3) \begin{cases} S_1 + Z_1 + Z_2 + Z_3, & Z_1^{32} + Z_1, \\ S_5 + Z_1^5 + Z_2^5 + Z_3^5, & Z_2^{32} + Z_2, \\ S_7 + Z_1^7 + Z_2^7 + Z_3^7, & Z_3^{32} + Z_3, \end{cases}$$

$$(\text{SYNSYM}_3) \begin{cases} S_1 + Z_1 + Z_2 + Z_3, & Z_1^{32} + Z_1, & \sigma_1 + Z_1 + Z_2 + Z_3, \\ S_5 + Z_1^5 + Z_2^5 + Z_3^5, & Z_2^{32} + Z_2, & \sigma_2 + Z_1Z_2 + Z_1Z_3 + Z_2Z_3, \\ S_7 + Z_1^7 + Z_2^7 + Z_3^7, & Z_3^{32} + Z_3, & \sigma_3 + Z_1Z_2Z_3, \end{cases}$$

A Gröbner basis for $(\text{SYNSYM}_3) \cap \mathbb{F}_2[\sigma_1, \sigma_2, \sigma_3, S_7, S_5, S_1]$ for the lex order $\sigma_1 > \sigma_2 > \sigma_3 > S_7 > S_5 > S_1$ can be computed using the efficient C software FGb in 17 sec (using a selection strategie such that S_i has weight i and s_j has weight j):

$$\begin{cases}
\sigma_1 + S_1, \quad \sigma_3^{32} + \sigma_3, \quad \sigma_2^{32} + \sigma_2, \quad S_5^{32} + S_5, \quad S_1^{32} + S_1, \\
\sigma_2\sigma_3 + \text{ polynom}(\sigma_3, S_1, S_5, S_7), \text{ degree 9 in } \sigma_3, \text{ 55 terms}, \\
\sigma_2 S_1 + \text{ polynom}(\sigma_3, S_1, S_5, S_7), \text{ degree 9 in } \sigma_3, \text{ 61 terms}, \\
\sigma_2 S_7 + \text{ polynom}(\sigma_3, S_1, S_5, S_7), \text{ degree 8 in } \sigma_3, \text{ 61 terms}, \\
\sigma_2 S_5 + \text{ polynom}(\sigma_3, S_1, S_5, S_7), \text{ degree 7 in } \sigma_3, \text{ 59 terms}, \\
\sigma_3(S_7 + S_1^7) + \text{ polynom}(S_1, S_5, S_7), \text{ 78 terms}, \\
\sigma_3(S_5 + S_1^5) + \text{ polynom}(S_1, S_5, S_7), \text{ 76 terms}, \\
\sigma_3(S_1^{31} + 1) + \text{ polynom}(S_1, S_5, S_7), \text{ 84 terms}, \\
S_7^5 + S_7^4 S_5 S_1^2 + S_7^3(S_5^9 + S_5^2 S_1^4 + S_5 S_1^9 + S_1^{14}) + S_7^2(S_5^{16} S_1^3 + S_5^4 S_1 + S_5^2 S_1^{11} + S_1^{21}) + S_7(S_5^{17} S_1^5 + \\
S_5^{16} S_1^{10} + S_5^{10} S_1^9 + S_5^9 S_1^{14} + S_5^8 S_1^{19} + S_5^5 S_1^3 + S_5^3 S_1^{13} + S_5^2 S_1^{18} + S_1^{28}) + S_5^{25} S_1^3 + S_5^{24} S_1^8 + S_5^{19} S_1^2 + \\
S_5^{18} S_1^7 + S_5^{16} S_1^{17} + S_5^{13} S_1 + S_5^{12} S_1^6 + S_5^7 + S_5^6 S_1^5 + S_5^4 S_1^{15} + S_5^2 S_1^{25} + S_5 S_1^{30} + S_1^4, \\
(S_7 + S_1^7)((S_5 + S_1^5)^{31} + 1)
\end{cases}$$

The ideal is of dimension 0 and has 5984 solutions.

The computation of a Gröbner basis for the system of Loustaunau and Von York, (SYNDROM$_3$) with respect to the lex ordering $Z_1 > Z_2 > Z_3 > S_7 > S_5 > S_1$ takes about 1 minute, again using a selection strategie such that S_i is of weight i. The resulting system has about 3! times more solutions, exactly 32768 solutions.

The Newton's identities for the syndroms of even rank are useless too, because they also lead to the equation $S_{2i} = S_i^2$ (see equality 4), so the system (NEWTON$_3$) simplifies to:

$$(\text{NEWTON}_3)\begin{cases}
S_1 + \sigma_1, & \sigma_1^{2^5} + \sigma_1, \\
S_3 + \sigma_1 {S_1}^2 + \sigma_2 S_1 + \sigma_3, & \sigma_2^{2^5} + \sigma_2, \\
S_5 + \sigma_1 {S_1}^4 + \sigma_2 S_3 + \sigma_3 {S_1}^2, & \sigma_3^{2^5} + \sigma_3, \\
S_7 + S_3^2\sigma_1 + S_5\sigma_2 + {S_1}^4\sigma_3, & S_3^{2^5} + S_3, \\
S_{11} + S_5^2\sigma_1 + S_5^8\sigma_2 + S_1^8\sigma_3, & S_{11}^{2^5} + S_{11}, \\
S_{15} + S_7^2\sigma_1 + S_{11}^4\sigma_2 + S_3^4\sigma_3, & S_{15}^{2^5} + S_{15}
\end{cases}$$

We want to compute the Gröbner basis for this system for the lex order with $S_{15} > S_{11} > S_3 > \sigma_1 > \sigma_2 > \sigma_3 > S_7 > S_5 > S_1$. Then S_{11} and S_{15} are already eliminated in the system, hence we do not need the last two equations. We still have more variables than in the previous systems, and it takes much more time to compute the Gröbner basis (about 11 minutes).

Thus for practical purposes, the most convenient system is (SYNSYM). Still, it is not possible to compute the Gröbner basis of (SYNSYM$_v$) for codes of greater length. For instance we did not succeed in finding the Gröbner basis of (SYNSYM$_4$) for the quadratic residue code $[41, 21, 9]$. The cause of this difficulty is that (SYNSYM$_t$) is a zero-dimensional ideal with many solutions, more than $\frac{n^t}{t!}$ and that is contains equations of very high degree.

4 Ideals of positive dimension

In order to remove this equations of high degree, $S_i^{2^m} - S_i$ or $\sigma_j^{2^m} - \sigma_j$, we introduce new systems. We first study their properties, and then demonstrate on examples their practical efficiency for the computation of a Gröbner basis.

4.1 New systems and their relationships

As in Section 3, we have the two systems coming from the definitions of the locators and from the Newton's identities:

$$(\textsc{SynSymPos}_v) \begin{cases} S_i - \sum_{j=1}^{v} Z_j^i & \forall\ i \in Q \\ \sigma_j - \sum_{l_1<\cdots<l_j} Z_{l_1}\cdots Z_{l_j} & \forall\ j \in [1,v] \end{cases}$$

$$(\textsc{NewtonPos}_v) \begin{cases} S_i + \sum_{j=1}^{i-1} \sigma_j S_{i-j} + i\sigma_i, & i \in [1,v] \\ S_{v+i} + \sum_{j=1}^{v} \sigma_j S_{v+i-j}, & i \in [1,n] \end{cases}$$

with $\textsc{SynSymPos}_v \subset \mathbb{F}_2[\underline{Z}_v, \underline{S}]$ and $\textsc{NewtonPos}_v \subset \mathbb{F}_2[\underline{\sigma}_v, \underline{S}, \overline{S}]$. Those systems are now of positive dimension, but we have the following new property:

Proposition 17 ([CLO97] chapter 7 §4) *The elimination ideal* $\langle \textsc{SynSymPos}_v \rangle \cap \mathbb{F}_2[\underline{\sigma}_v, \underline{S}]$ *is a prime ideal.*

Starting with the system $(\textsc{NewtonPos}_v)$ we can eliminate the unknowns syndroms by successive substitutions, to obtain the binary system

$$(\textsc{Bin}_v)\ \{S_i - f_i(\sigma_1, \ldots, \sigma_v) = 0 \quad \forall\ i \in Q$$

where the f_i's are the Waring's functions (see equation 5).

Proposition 18 *Those systems are related by*

$$\begin{aligned} \langle \textsc{Bin}_v \rangle &= \langle \textsc{SynSymPos}_v \rangle \cap \mathbb{F}_2[\sigma, S] \\ &= \langle \textsc{NewtonPos}_v \rangle \cap \mathbb{F}_2[\sigma, S] \end{aligned} \tag{5}$$

Proof We have

$$\begin{aligned} & \langle \textsc{Bin}_v, \sigma_j + \textstyle\sum_{l_1<l_2<\cdots<l_j} Z_{l_1}\cdots Z_{l_j},\ j \in [1,v] \ \rangle \\ = \ & \langle S_i + f_i(\sigma_1, \ldots, \sigma_v), \sigma_j + \textstyle\sum_{l_1<l_2<\cdots<l_j} Z_{l_1}\cdots Z_{l_j} \rangle \\ = \ & \langle S_i + f_i(Z_1 + \cdots + Z_v, \ldots, Z_1\cdots Z_v), \sigma_j + \textstyle\sum_{i_1<\cdots<i_j} Z_{i_1}\cdots Z_{i_j} \rangle \\ = \ & \langle S_i + Z_1^i + \cdots + Z_v^i, \sigma_j + \textstyle\sum_{l_1<l_2<\cdots<l_j} Z_{l_1}\cdots Z_{l_j} \rangle \\ = \ & \langle \textsc{SynSymPos}_v \rangle \end{aligned}$$

Moreover, $(\textsc{Bin}_v)$ is a Gröbner basis for $\langle \textsc{Bin}_v \rangle$ with respect to any lex order with $\underline{S} > \underline{\sigma}_v$. Let G be a Gröbner basis for $\langle \sigma_j + \sum_{l_1<l_2<\cdots<l_j} Z_{l_1}\cdots Z_{l_j},\ j \in [1,v] \ \rangle$ with respect to

any lex order with $\underline{Z}_v > \underline{\sigma}_v$, then (BIN_v, G) is a Gröbner basis for $\langle \text{SYNSYMPOS}_v \rangle$ with respect to any lex order with $\underline{Z}_v > \underline{S} > \underline{\sigma}_v$ (it follows from the first Buchberger criterion, see e.g. [CLO97]). Then by the Elimination Theorem (10), (BIN_v) is a Gröbner basis for $\langle \text{SYNSYMPOS}_v \rangle \cap \mathbb{F}_2[\underline{\sigma}_v, \underline{S}]$ with respect to any lex order with $\underline{S} > \underline{\sigma}_v$.

As $(\text{BIN}_v) \subset \langle \text{NEWTONPOS}_v \rangle \subset \langle \text{SYNSYMPOS}_v \rangle$, it concludes the proof. □

4.2 Unicity theorem

As in the case of zero-dimensional systems, we need to prove that the solutions are "closely related" with the errors that occurred. The main difference is that, because we removed the field's equations, the set of solutions associated with the ideal contains now solutions in the algebraic closure of $\mathbb{F}_{2^m}$. The following proposition show that the parasitic solutions (solutions in the algebraic closure not corresponding to a codeword) are well known, and that the computations of the real solutions is still easy.

Proposition 19 (Unicity) *Let $\underline{S}^* \subset \mathbb{F}_{2^m}$ be the syndrom of an error $e \in \mathbb{F}_2[x]/(x^n - 1)$ of Hamming's weight $\leq t$.*

- *the specialized system $(\text{BIN}_v(\underline{S}^*))$ has a unique solution $(\sigma_1^*, \ldots, \sigma_v^*)$ and $L_e(Z) = \sum_{j=0}^{v} \sigma_j^* Z^{v-j}$ is the locator polynomial of e.*
- *$\exists!(\sigma_1^*, \ldots, \sigma_v^*)$ such that $(\sigma_1^*, \ldots, \sigma_v^*, 0_{t-v}, \underline{S}^*) \in V(\text{BIN}_t)$ and $(0_{t-v+1}, \underline{S}^*) \notin \Pi_{t-v+1}(V(\text{BIN}_t))$. The weight of e is therefore exactly v and $\sum_{j=0}^{v} \sigma_j^* Z^{v-j}$ is the locator polynomial $L_e(Z)$ of e.*
- *if $\tilde{\sigma}^* = (\tilde{\sigma}_1^*, \ldots, \tilde{\sigma}_t^*)$ is such that $(\tilde{\sigma}^*, \underline{S}^*) \in V(\text{BIN}_t)$, then $L_e(Z)$ divides $L(Z) = \sum_{j=0}^{t} \tilde{\sigma}_j^* Z^{t-j}$ and $L_e(Z)$ can be obtained considering the factors of $L(Z)$ with odd multiplicity and distinct from Z. More precisely, $L(Z) = p_1^{e_1} \cdots p_k^{e_k} Z^a \Rightarrow L_e(Z) = p_1^{(e_1 \bmod 2)} \cdots p_k^{(e_k \bmod 2)}$.*

This means that if we compute a Gröbner basis of (BIN) for a degree ordering with $\underline{\sigma} > \underline{S}$, we will get formulas for the σ_j's in terms of the S_i's of *minimal degree*. We expect these equations to be of degree one, but even if they are of high degree, they have a unique root when specialized on a syndrom.

4.3 Proof of the Unicity theorem

Lemma 20 *Let $e \in \overline{\mathbb{F}}_2[x]/(x^n - 1)$ be a word such that the associated σ_j^*'s and S_i^*'s are solutions of the system (NEWTONPOS_v). Then the weight of e is less than v and $e(x) = \sum_{r=0}^{n-1} e_r x^r$ with $e_r = 0$ or 1.*

Proof For the weight of e see [Aug96] theorem 2.2. Let us write $e(x) = \sum_{j=1}^{v'} Y_j^* x^{i_j}$ with $v' \leq v$, the Y_j^*'s being non zero elements of $\overline{\mathbb{F}}_2$. As before, we denote by $Z_j^* = \alpha^{i_j}$ the

locators of e. We have the relations $S_i^* = \sum_{j=1}^{v'} Y_j^* Z_j^{*i}, \quad \forall i \in Q$. From the proposition 18, $(\sigma^*, \underline{S}^*)$ being a solution of (NewtonPos$_v$), we deduce that $S_i^* = f_i(\sigma_1^*, \ldots, \sigma_{v'}^*) \quad \forall i \in Q$ and then that $S_i^* = Z_1^{*i} + \cdots + Z_{v'}^{*i} \quad \forall i \in Q$. Hence the Y_j^*'s and the Z_j^*'s are solutions of the following system of equations:

$$\begin{cases} Y_1 Z_1 + \cdots + Y_{v'} Z_{v'} = Z_1 + \cdots + Z_{v'} \\ Y_1 Z_1^2 + \cdots + Y_{v'} Z_{v'}^2 = Z_1^2 + \cdots + Z_{v'}^2 \\ \vdots \\ Y_1 Z_1^{v'} + \cdots + Y_{v'} Z_{v'}^{v'} = Z_1^{v'} + \cdots + Z_{v'}^{v'} \end{cases}$$

This system, viewed as a system with indeterminates the Y_j's, has a Vandermonde determinant:

$$(\prod_{j=1}^{v'} Z_j) \prod_{j_1 < j_2} (Z_{j_2} - Z_{j_1}) \neq 0$$

Then it has a unique solution, $(Y_1^*, \ldots, Y_{v'}^*) = (1, \ldots, 1)$. □

Lemma 21 *Let $\underline{S}^* = (S_1^*, \ldots, S_n^*) \in \mathbb{F}_{2^m}^n$ be the Fourier transform of a word $c \in \mathbb{F}_2[x]/(x^n - 1)$, and let $\sigma^* = (\sigma_1^*, \ldots, \sigma_v^*) \in \overline{\mathbb{F}}_2^v$ be such that $(\underline{S}^*, \sigma^*)$ is a solution of the system (NewtonPos$_v$), with $v \leq n$. Let $(Z_1^*, \ldots, Z_v^*) \in \overline{\mathbb{F}}_2$ be the roots of $L(Z) = Z^v + \sum_{i=1}^{v} \sigma_i^* Z^{v-i}$.*

Then the weight v_c of c is such that $v_c \leq v$ and $L(Z) = L_c(Z) \cdot P(Z)^2 \cdot Z^a$ where $L_c(Z)$ is the locator polynomial of c, $P(0) \neq 0$ and $a \in \mathbb{N}$.

Proof From the proposition 5 we can write $L(Z) = L_c(Z)P(Z)Z^a$ with $P(0) \neq 0$. We list the roots $Z_1^*, \ldots, Z_{v'}^*, \ldots, Z_w^*, \ldots, Z_v^*$ of L such that $Z_1^*, \ldots, Z_{v'}^*$ are $L_c(Z)$'s roots, $Z_{v'+1}^* = \ldots = Z_w^* = 0$ ($a = w - v' \geq 0$) and $Z_{w+1}^*, \ldots, Z_v^*$ are not zero. As $S_i^* = f_i(\sigma_1^*, \ldots, \sigma_v^*)$ (see proposition 18) and the σ_j^*'s are the elementary symmetric functions of the Z_j^*'s, we have $S_i^* = \sum_{j=1}^{v} Z_j^{*i}$ for $1 \leq i \leq n$. But $S_i^* = \sum_{j=1}^{v'} X_j^{\,i}$ for $1 \leq i \leq n$, where the X_j's are the roots of $L_c(Z)$. Then, $\sum_{j=w+1}^{v} Z_j^{*i} = 0$ for $1 \leq i \leq n$, all the Z_j's being non zero. From the proposition 2 we deduce that the Z_j^*'s, $w + 1 \leq j \leq v$ are equal by pairs and then that $P(Z)$ is a square. □

Proof [of the Unicity theorem] Let $\sigma^* = (\sigma_1^*, \ldots, \sigma_v^*)$ be such that $(\sigma^*, \underline{S}^*) \in V(\text{Bin}_v)$. If we denote by $Z^* = (Z_1^*, \ldots, Z_v^*)$ the roots of $\sum_{j=0}^{v} \sigma_j^* Z^{v-j}$, then we have $(Z^*, \sigma^*, \underline{S}^*) \in V(\text{SynSymPos}_v)$.

Let $\overline{S}_i^* = \sum_{j=1}^{v} Z_j^{*i}$ for all $i \notin Q$, then $(\sigma^*, \underline{S}^*, \overline{S}^*)$ is a solution of the system (NewtonPos$_v$). Applying the lemma 20 we get that the word $c(x) \in \overline{\mathbb{F}}_2[x]/(x^n - 1)$ with Fourier Transform $(\underline{S}^*, \overline{S}^*)$ has a weight $\leq v$, is in $\mathbb{F}_2[x]/(x^n - 1)$ and so is equal to e. Then from the lemma 21 we get that $L(Z) = L_e(Z) \cdot P(Z)^2 \cdot Z^a$.

- If v is the weight of e, then the degree of $L(Z)$ is exactly the degree of $L_e(Z)$ and $L(Z) = L_e(Z)$

- if $\sigma^* = (\sigma_1^*, \ldots, \sigma_v^*)$ is such that $(\sigma^*, 0_{t-v}, \underline{S^*}) \in V(\text{BIN}_t)$, then $L(Z) = Z^{t-v}L_1(Z)$ with $L_1(Z) = \sum_{j=0}^{v} \sigma_j^* Z^{v-j}$. It follows from $P(0) \neq 0$ that $t - v \leq a$ and from $(0_{t-v+1}, \underline{S^*}) \notin \Pi_{t-v+1}(V(\text{BIN}_t))$ that $L_1(0) \neq 0$ and so that $a \leq t - v$. We have then $a = t - v$ and $L_1(Z) = L_e(Z)P(Z)^2$ with degree(L_1)=v and degree(L_e)$\geq v$ (because $(0_{t-v+1}, \underline{S^*}) \notin \Pi_{t-v+1}(V(\text{BIN}_t))$). Then $L_1(Z) = L_e(Z)$ is of degree v.

The third point is a direct consequence of lemma 21. □

4.4 Example: the [31,16,7] quadratic residue code

The most efficient system for the formal precomputation of a Gröbner basis seems to be the system (BIN), because we do not have to eliminate the indeterminates corresponding to the unknown syndroms.

If $i \in Q$ and $2i \in Q$ we have the relation $S_{2i} = S_i^2$ – but now we do not have the "fields equations" so we do not have the relations $S_j = S_i^2$ for $j = 2i \bmod n$, $j \neq 2i$. The significant syndroms are the odd ones. For the QR Code [31,16,7], the system (BIN_3) simplifies to

$$\begin{cases} \mathbf{S_{25}} + \sigma_1^{25} + \sigma_1^{23}\sigma_2 + \sigma_1^{22}\sigma_3 + \sigma_1^{21}\sigma_2^2 + \sigma_1^{20}\sigma_2\sigma_3 + \sigma_1^{17}\sigma_2^4 + \sigma_1^{17}\sigma_2\sigma_3^2 + \sigma_1^{16}\sigma_2^3\sigma_3 + \sigma_1^{16}\sigma_3^3 + \sigma_1^{11}\sigma_2\sigma_3^4 + \\ \sigma_1^{10}\sigma_3^5 + \sigma_1^9\sigma_2^5\sigma_3^2 + \sigma_1^9\sigma_2^2\sigma_3^4 + \sigma_1^8\sigma_2^7\sigma_3 + \sigma_1^8\sigma_2^4\sigma_3^3 + \sigma_1^8\sigma_2\sigma_3^5 + \sigma_1^7\sigma_2^9 + \sigma_1^6\sigma_2^8\sigma_3 + \sigma_1^5\sigma_2^{10} + \sigma_1^4\sigma_2^9\sigma_3 + \sigma_1\sigma_2^{12} + \\ \sigma_1\sigma_2^9\sigma_3^2 + \sigma_1\sigma_3^8 + \sigma_2^{11}\sigma_3 + \sigma_2^8\sigma_3^3, \\ \mathbf{S_{19}} + \sigma_1^{19} + \sigma_1^{17}\sigma_2 + \sigma_1^{16}\sigma_3 + \sigma_1^{14}\sigma_2\sigma_3 + \sigma_1^{13}\sigma_2^3 + \sigma_1^{13}\sigma_3^2 + \sigma_1^{12}\sigma_2^2\sigma_3 + \sigma_1^{11}\sigma_2^4 + \sigma_1^9\sigma_2^5 + \sigma_1^8\sigma_2^4\sigma_3 + \\ \sigma_1^8\sigma_2\sigma_3^3 + \sigma_1^3\sigma_2^8 + \sigma_1^2\sigma_2\sigma_3^5 + \sigma_1\sigma_2^9 + \sigma_1\sigma_2^3\sigma_3^4 + \sigma_1\sigma_3^6 + \sigma_2^8\sigma_3 + \sigma_2^5\sigma_3^3 + \sigma_2^2\sigma_3^5, \\ \mathbf{S_9} + \sigma_1^9 + \sigma_1^7\sigma_2 + \sigma_1^6\sigma_3 + \sigma_1^5\sigma_2^2 + \sigma_1^4\sigma_2\sigma_3 + \sigma_1\sigma_2^4 + \sigma_1\sigma_2\sigma_3^2 + \sigma_2^3\sigma_3 + \sigma_3^3, \\ \mathbf{S_7} + \sigma_1^7 + \sigma_1^5\sigma_2 + \sigma_1^4\sigma_3 + \sigma_1^2\sigma_2\sigma_3 + \sigma_1\sigma_2^3 + \sigma_1\sigma_3^2 + \sigma_2^2\sigma_3, \\ \mathbf{S_5} + \sigma_1^5 + \sigma_1^3\sigma_2 + \sigma_1^2\sigma_3 + \sigma_1\sigma_2^2 + \sigma_2\sigma_3, \\ \mathbf{S_1} + \sigma_1 \end{cases}$$

Our goal is to obtain linear formulas for the σ_j's. Theoretically we just have to compute a Gröbner basis of the previous system and we will get the formulas of minimal degree. But any syndrom S_i gives an equation of degree i, and if we take all the syndroms we get equation of high degree (degree 19 or 25 in the preceding example), and with these high degree equations the Gröbner basis is harder to compute (in the example we were not able to compute the Gröbner basis for the ideal with the equations coming from S_{19} or S_{25}). In practice, it is very often possible to obtain a similar result (equations of degree 1) using fewer equations. In our example we consider only the syndroms S_1, S_5, S_7, S_9 and we get linear formulas for the σ_j's, as:

$$\sigma_{\mathbf{3}}(\sigma_2 + S_1^2) + \sigma_2^2 S_1 + \sigma_2 S_1^3 + S_5 + S_1^5 \quad \text{or} \quad \sigma_{\mathbf{3}} S_7 + \sigma_2 S_1^8 + S_9 S_1 + S_5^2$$

Actually the Gröbner basis is quite large, and can not be printed here. For the Lex order $\sigma_1 > \sigma_3 > \sigma_2 > S_9 > S_7 > S_5 > S_1$, it contains 32 polynomials, with degrees up to 88 and containing up to 234 terms. We remark that the ideal contains the relations obtained by hand in [RYT90], and precisely, these relations are obtained automatically as elements of the Gröbner basis, using the above ordering. We also remark that the linear formula (15) given in [RYT90] for σ_2 is false, the true one being

$\sigma_2(S_9S_7S_1^3 + S_9S_1^{10} + S_7^2S_5 + S_7^2S_1^5 + S_7S_5^2S_1^2 + S_7S_1^{12} + S_5^2S_1^9 + S_1^{19}) + S_9^2S_1^3 + S_9S_1^{12} + S_7^3 + S_7^2S_5S_1^2 + S_7S_5S_1^9 + S_7S_1^{14} + S_5^4S_1 + S_5^2S_1^{11}$

However, the Gröbner basis contains many formulas of degree one in the σ_j's. For decoding, the aim is to have only one formula for each σ_j. The idea is to extract from the Gröbner basis a triangular system with the same solutions.

The ideal considered here is a prime ideal, and so we have the following property:

Theorem 22 ([Aub99] pp. 65) *Let G be a Gröbner basis of an ideal $J \subset k[\underline{X}]$ with respect to a monomial ordering $<$. The* main variable *of a polynomial p, $main(p)$, is the greatest variable appearing in p. The* initial *of p is the greatest coefficient of p viewed as an univariate polynomial in $main(p)$. A subset T of G is a* triangular set *extracted from G if*

- $main(T) = \{main(t), t \in T\} = main(G)$,
- *For all $v \in main(G)$, the polynomial $T_v \in T$ with $main(T_v) = v$ has the smallest degree (in v) inside $G_v = \{p \in G, main(p) = v\}$.*

Let T be a triangular set extracted from G, then

$$J = \langle T : h^\infty \rangle = \{p \in k[\underline{X}] \ : \ \exists n \in N, \quad h^n.p \in \langle T \rangle\}$$

where h is the product of the initials of the polynomials in T, and

$$V(J) = \overline{\{x \in k^n \ : \ \forall p \in T \ p(x) = 0 \text{ and } h(x) \neq 0\}}$$

for the Zariski topology.

Thus the theorem indicates that all the triangular sets behave in the same way with respect to the zeros of the original ideal. In practice, we do not know how to pick a triangular set which describes all the solutions of the decoding problem: it may happen that an equation of degree one may be chosen, and that its initial vanishes on some syndrom (but in this case the number of syndroms for which the initial vanish is negligible).

One solution is to prove by exhaustive search on all the possible syndroms that the initials do not vanish on all syndroms corresponding to errors of weight 3. This is also the solution adopted by the authors in [RYT90] to verify that the initials of their formulas are not zero when specialized on syndroms. This may seem to be a limiting factor when the length and the error capacity grow, but in next section we will see that the true limiting factor is the Gröbner basis computation by itself.

Indeed, after an exhaustive search, we are able to give the following system of three polynomials, which solve the decoding problem for the QR code of length 31, for words of weight 2 or 3:

$$\begin{cases} \sigma_1 + S_1, \\ \sigma_3(\sigma_2 + S_1^2) + \sigma_2^2 S_1 + \sigma_2 S_1^3 + S_5 + S_1^5, \\ \sigma_2(S_9S_7S_1^3 + S_9S_1^{10} + S_7^2S_5 + S_7^2S_1^5 + S_7S_5^2S_1^2 + S_7S_1^{12} + S_5^2S_1^9 + S_1^{19}) + S_9^2S_1^3 + S_9S_1^{12} + \\ S_7^3 + S_7^2S_5S_1^2 + S_7S_5S_1^9 + S_7S_1^{14} + S_5^4S_1 + S_5^2S_1^{11} \end{cases}$$

If the last equation is zero, then the error has a weight 0 or 1, we have $\sigma_2 = \sigma_3 = 0$ and the first equation gives the value of σ_1.

4.5 Size of formulas

The next binary quadratic residue code is the $[41, 21, 9]$ QR code, which can correct up to four errors. The odd syndroms are $\{1, 5, 9, 21, 23, 25, 31, 33, 37, 39\}$. When trying to compute a Gröbner basis of the system (BIN_4), we were not able to get the result. So we tried to remove equations of high degree. The experience has shown that either the Gröbner basis could not be computed, either σ_4 appeared as a free variable (when too much equations were removed).

So we generalize the method from [RTCY92]: -1 is a quadratic residue modulo 41, so we get the relation $\sigma_3 = S_{40}\sigma_4$. More generally, 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 with the $\tilde{Z}_j$. Then the following relations hold: $\tilde{S}_i = S_{n-i}$, and $\sigma_j = \sigma_v \tilde{\sigma}_{v-j}$ (in this example $v = 4$). Then

$$S_i = f_i(\sigma_1, \ldots, \sigma_v) = \tilde{S}_{n-i} = f_{n-i}(\tilde{\sigma}_1, \ldots, \tilde{\sigma}_v) = f_{n-i}(\frac{\sigma_{v-1}}{\sigma_v}, \ldots, \frac{1}{\sigma_v})$$

the f_i's being the Waring polynomials. Clearing out denominators in (4.5) gives a formula

$$\sigma_v^{n-i} S_i = \tilde{f}_{n-i}(\sigma_1, \ldots, \sigma_v) \tag{6}$$

which has degree $n - i + 1$ instead of i. In our case, we deduce the relation $S_{36}\sigma_4^5 + \sigma_3^5 + \sigma_4^2\sigma_2^2\sigma_3 + \sigma_4^3\sigma_2\sigma_1 + \sigma_4^3\sigma_3 + \sigma_4\sigma_3^3\sigma_2 + \sigma_4^2\sigma_3^2\sigma_1$. In what follow, we use the notation $\text{BIN}_v(E_1, E_2) = \{S_{i_1} - f_{i_1}(\underline{\sigma}_v), i_1 \in E_1\} \cup \{\sigma_v^{n-i_2} S_{i_2} - \tilde{f}_{n-i_2}(\underline{\sigma}_v), i_2 \in E_2\}$. The syndroms $\{1, 5, 9, 36, 40\}$ gives the system $\text{BIN}_4(\{1, 5, 9\}, \{36, 40\})$:

$$\begin{cases} \mathbf{S_1} + \sigma_1, \\ \mathbf{S_5} + \sigma_1^5 + \sigma_1^3\sigma_2 + \sigma_1^2\sigma_3 + \sigma_1\sigma_2^2 + \sigma_1\sigma_4 + \sigma_2\sigma_3, \\ \mathbf{S_9} + \sigma_1^9 + \sigma_1^7\sigma_2 + \sigma_1^6\sigma_3 + \sigma_1^5\sigma_2^2 + \sigma_1^5\sigma_4 + \sigma_1^4\sigma_2\sigma_3 + \sigma_1^2\sigma_3\sigma_4 + \sigma_1\sigma_2^4 + \sigma_1\sigma_2^2\sigma_4 + \sigma_1\sigma_2\sigma_3^2 + \\ \sigma_1\sigma_4^2 + \sigma_2^3\sigma_3 + \sigma_3^3, \\ \mathbf{S_{36}}\sigma_4^5 + \sigma_1\sigma_2\sigma_4^3 + \sigma_1\sigma_3^2\sigma_4^2 + \sigma_2^2\sigma_3\sigma_4^2 + \sigma_2\sigma_3^3\sigma_4 + \sigma_3^5 + \sigma_3\sigma_4^3, \\ \mathbf{S_{40}}\sigma_4 + \sigma_3 \end{cases}$$

We can eliminate the variables σ_1 and σ_3 with the first and the last equations. Unfortunately, the Gröbner basis of the remaining system could not be computed. In another way, considering both systems $\{g_5, g_9\}$ and $\{g_5, g_{36}\}$ (where g_i is the equation for the syndrom S_i) we could computed the Gröbner bases of each of these systems for the lex order $\sigma_2 > \sigma_4 > S_{40} > S_{36} > S_9 > S_5 > S_1$. We obtained the two following polynomials for σ_4:

$P_{5,9} = (S_{40}^5 S_5 + S_{40}^5 S_1^5 + S_{40}^4 S_1^4 + S_{40}^3 S_1^3)\sigma_4^5 + (S_{40}^4 S_5 S_1^3 + S_{40}^4 S_1^8 + S_{40}^3 S_1^7 + S_{40}^2 S_5 S_1 + S_{40} S_1^5 + S_1^4)\sigma_4^4 + (S_{40}^3 S_9 S_1^2 + S_{40}^3 S_5^2 S_1 + S_{40}^2 S_1^{10})\sigma_4^3 + (S_{40}^2 S_9 S_5 + S_{40}^2 S_5^2 S_1^4 + S_{40}^2 S_5 S_1^9 + S_{40}^2 S_1^{14} + S_{40} S_9 S_1^4 + S_{40} S_5 S_1^8 + S_{40} S_1^{13} + S_5^2 S_1^2)\sigma_4^2 + (S_{40} S_9 S_5 S_1^3 + S_{40} S_5^3 S_1^2 + S_{40} S_5 S_1^{12} + S_{40} S_1^{17} + S_9 S_1^7 + S_5^2 S_1^6 + S_5 S_1^{11} + S_1^{16})\sigma_4 + S_9^2 S_1^2 + S_9 S_1^{11} + S_5^4 + S_5^2 S_1^{10} + S_5 S_1^{15} + S_1^{20}$

$P_{5,36} = (S_{40}^{10} S_1^2 + S_{40}^9 S_1 + S_{40}^8 + S_{40}^4 S_{36} S_1 + S_{40}^3 S_{36} + S_{36}^2 S_1^2)\sigma_4^4 + (S_{40}^8 S_1^4 + S_{40}^7 S_1^3 + S_{40}^5 S_1 + S_{40}^4 + S_{40}^3 S_{36} S_1^4 + S_{40} S_{36} S_1^2)\sigma_4^3 + (S_{40}^6 S_5 S_1 + S_{40}^5 S_5 + S_{40} S_{36} S_1^6 + S_{36} S_1^5)\sigma_4^2 + (S_{40}^4 S_5 S_1^3 + S_{40}^4 S_1^8 + S_{40}^3 S_1^7 + S_{40}^2 S_5 S_1 + S_{40} S_1^5 + S_1^4)\sigma_4 + S_{40}^2 S_5^2 + S_{40}^2 S_1^{10} + S_{40} S_5 S_1^4 + S_{40} S_1^9 + S_5 S_1^3 + S_1^8$

A linear formula for σ_4 is simply obtained by computing a formal greatest common divisor of those two polynomials considered as polynomials in σ_4. This formal gcd could be

computed using Magma and the result is a linear polynomial in σ_4, which coefficients are polynomials in $S_1, S_5, S_9, S_{36}, S_{40}$ of total degree 170, and with 29828 terms.

This indicates that, in general, the size of the linear formula with formal parameters is very big, and even if it could be obtained, it would be useless for decoding, since its evaluation on syndroms would have a cost corresponding to its size. Thus the idea of doing precomputation of formal Gröbner basis is not relevant for effective decoding of cyclic codes.

5 Practical decoding

5.1 Effective online decoding

We turn back to the original approach of [CRHT94c, CRHT94b], and consider in this Section online decoding. For each word e we construct the system $\textsc{Bin}(\underline{S}^*)$ or $\textsc{NewtonPos}(\underline{S}^*)$ and compute its Gröbner basis over $\mathbb{F}_{2^m}$. The system has a unique solution (cf. Unicity Theorem 19), and it turns out that formulas of degree one are obtained (but we did not proved that there is no multiplicity). This means that the Gröbner basis has in practice the shape

$$\textsc{Bin}(\underline{S}^*) \begin{cases} \sigma_1 + \sigma_1^* \\ \sigma_2 + \sigma_2^* \\ \quad \vdots \\ \sigma_v + \sigma_v^* \end{cases} \tag{7}$$

where the σ_i^* are the actual coefficients of the locator polynomial.

We use a general method for solving systems with parameters. The Specialization Theorem tells us that the result of an online Gröbner basis computation over $\mathbb{F}_{2^m}$ is the specialization of the formal Gröbner basis over $\mathbb{F}_2$. It seems that when the size 2^m of the finite field is large enought, this property extends to the fact that all steps of the computation of the specialized basis are the specialization of all steps of the computation of the formal basis. In other words, it seems that the behavior of the Gröbner basis computation is the same for all the possible values of the syndroms, provided that it corresponds to an error of a given weight. We use this remark to drastically reduce the complexity of the online computation (we gain a factor 1000) when the underlying field 2^m is large enought.

We describe the method in the particular case of the F4 algorithm ([Fau99]), because this is the one we use in practice, but it also applies to any other algorithm. The F4 algorithm uses the correspondence between polynomial algebra and linear algebra. It constructs several matrices from polynomials, and uses linear algebra to compute the Row Echelon form for each of these matrices (see [Fau99] for more details).

Considering the computation of a Gröbner basis of $\textsc{Bin}(S^*_{e_0})$ for a given error e_0 of weight v_0, we can record the trace of the computation (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 of e. It successively constructs matrices, in the same way as for e_0, and perform linear algebra on it, as for e_0. The fact that

experimentally we always obtain exactly the Gröbner basis of $\text{BIN}(S_e^*)$ comfort the idea that the Specialization Theorem extends to all steps of the computation. These considerations justify the following algorithm:

- PREPROCESSING: compute a Gröbner basis for $\text{BIN}_v(S_{e_0}^*)$ 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 $\text{BIN}_v(S_e^*)$ and get the values of the σ_j's.

Remark 23 If $I_e = \text{BIN}(S_e^*)$, the linear algebraic operations performed during the execution of the C program correspond in terms of polynomials to operations in the ideal I_e, i.e. all the polynomials obtained are in I_e. If we get a result $G = \{g_0, \ldots, g_s\}$ 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 $V(\langle g_0, \ldots, g_s \rangle) \supset V(I_e)$. If the system G has only one solution, then it is the solution of I_e. If $V(\langle g_0, \ldots, g_s \rangle)$ contains more than one solution, we know at least that the solution of I_e is one of the solutions of $V(\langle g_0, \ldots, g_s \rangle)$.

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 $\mathcal{C}$ correcting t errors, a decoding algorithm consists in t programs $P_1, \ldots, P_t$, 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.

Indeed, the set of solutions of the system $\text{BIN}_v(\underline{S}^*)$ is the set of all the errors of weight less then or equal to v which have $\underline{S}^*$ as syndroms. As long as there exists only one error of weight less than v with syndroms $\underline{S}^*$, this error can be decoded, even if v is greater than t the correction capacity of $\mathcal{C}$. In the other cases, this enable to do list decoding up to the weight v. The size of the list is not known, and may be large. Note also that the complexity of the Gröbner basis computation increases with the size of the list. We illustrate this result with the [31,16,7] QR code: we made an exhaustive search for all errors of weight 4 (there are 31465 of them). As we can see in Figure 1, 31% of these errors of weight 4 can be decoded (i.e. there is a single codeword at distance less then or equal to 4), and for 4.9% of the errors of weight 4 the set of solutions of $\text{BIN}_4(\underline{S}^*)$ contains one solution of weight 4 and one solution of weight 3. It is always a list of size at most 5.

	% of errors having n_3 (resp. n_4) solutions of weight 3 (resp. 4)								
(n_3, n_4)	(0,1)	(0,2)	(1,1)	(0,3)	(1,2)	(0,4)	(1,3)	(0,5)	(1,4)
	31%	29,6%	4,9%	14,8%	5,9%	5,9%	4,4%	1,5%	2%

Figure 1: Decoding the errors of weight 4 for the QR code of length 31.

δ	k	d	t	weight of errors	number of $*$	number of tests giving i solutions	
						$i=1$	$i=2$
93	175	95	47	48	$2^{16.2}$	10000	
				49	$2^{16.7}$	10000	
				50	$2^{17.6}$	10000	
				51	$2^{24.0}$	10000	
91	184	91	45	46	$2^{15.9}$	100	
				47	$2^{16.1}$	100	
				48	$2^{16.4}$	100	
				49	$2^{21.4}$	100	
				50	$2^{26.7}$	100	

Figure 2: Decoding BCH Codes $[511, k, \delta]$, correcting $t = \lfloor \frac{d-1}{2} \rfloor$ errors, above t

5.2 Results

We present here results for some selected codes. For each code, we give the number of multiplications $(*)$ in the field $\mathbb{F}_{2^m}$ that occurred during the execution of the C programs. Note that the number of multiplications gives a better complexity's measure than the time: it neither depend on the computer used, nor on the finite field implementation. To give an ordre of magnitude, for the field $\mathbb{F}_{512}$, 1 second corresponds approximatively to $2^{19.5}$ multiplications.

Figure 2 presents the decoding of two BCH codes of length 511, with designed distance 93 and 91, above their correction capacity. We are able to decode far beyond the correction capacity of the code: for instance, for the BCH code [511,175,93] the true minimum distance is 95, hence it corrects 47 errors, but we are able to correct up to 51 errors. Figure 3 shows decoding algorithms for some QR codes (for which no decoding algorithm was known before).

We compare finally in Figure 4 two codes of length 75 : the BCH code [75,31,7] and a code of type [75,33,7] and defining set $\{1, 3, 25\}$ which does not belong to a known class of codes. Our decoding method is independent of taking the code in a specific class. Any cyclic code can be decoded in the same way. We chose a code which is better than the corresponding BCH code (it has the same length, the same minimum distance, but its dimension is smaller, and it behaves a little better above 4 errors).

n	d	Field	weight of errors	number of $*$	number of tests giving i solutions					
					$i=1$	$i=2$	$i=3$	$i=4$	$i=5$	∞
41	9	2^{20}	2-3	$2^{7.4}$	1000					
			4	$2^{8.8}$	1000					
73	13	2^9	2-3	$2^{6.3} - 2^{6.7}$	10000					
			4	$2^{9.3}$	10000					
			5	$2^{10.4}$	10000					
			6	$2^{15.3}$	10000					
			7	$2^{21.5}$	9837	163				
			8	$2^{24.3}$	8530	1346	108	2	1	13
89	17	2^{11}	1-3	$2^{6.9}$	10000					
			4	$2^{9.3}$	10000					
			5	$2^{13.3}$	10000					
			6	$2^{17.3}$	10000					
			7	$2^{21.2}$	10000					
			8	$2^{26.2}$	9996	4				
113	15	2^{11}	1-3	2^7	10000					
			4	$2^{9.4}$	10000					
			5	$2^{12.7}$	10000					
			6	$2^{14.9}$	10000					
			7	$2^{20.0}$	10000					
			8	$2^{23.4}$	9996	4				

Figure 3: Decoding QR Codes $[n, \frac{n+1}{2}, d]$.

Code	weight of errors	time (seconds)	number of tests giving i solutions								
			$i=1$	2	3	4	5	6	8	12	∞
BCH	1-3	0	10000								
$[75, 31, 7]$	4	2^6 to $2^{10.8}$	9940	53		7					
	5	$2^{11.3}$	9375	533		45		23			23
Random code	1-3	0	10000								
$\mathcal{Q} = \{1, 3, 25\}$	4	2^6 to 2^{10}	9940	53		7					
$[75, 33, 7]$	5	$2^{10.7}$	9618	344		35		2			
	6	$2^{15.9}$	8823	882	70	91	30	54	16	3	31

Figure 4: Decoding the BCH Code $[75, 31, 7]$ and a code with $\mathcal{Q} = \{1, 3, 25\}$ and type $[75, 33, 7]$.

6 Conclusion

We have studied the decoding of cyclic codes using Gröbner bases. After reviewing existing methods in the literature, we have introduced new systems, which behave better with respect to the complexity of Gröbner bases computation. Those new systems and progress in the field of computer algebra enables to consider longer codes. We have indicated that there are little hope to get formulas for the algebraic decoding of quadratic codes: for example computations become intractable for the [41,21,9] quadratic residue code.

Still, we have shown that it is reasonable to perform online Gröbner bases computation, one for each word to be decoded. We get practical results for many cyclic codes. This uses a technique where, after a reasonable amount of preprocessing, a small and efficient program can be constructed for decoding. Examples have been given, including a BCH code of length 511 and a random code of length 75.

We have noted that this techniques holds for any cyclic code, and show how to use these techniques to decode above the error correction capacity, enabling list-decoding of cyclic codes. This topic may be perhaps further studied.

References

[Aub99] Philippe Aubry. *Ensembles triangulaires de polynômes et résolution de systèmes algébriques. Implantation en Axiom.* PhD thesis, Université Paris VI, 1999.

[Aug96] Daniel Augot. Description of minimum weight codewords of cyclic codes by algebraic systems. *Finite Fields Appl.*, 2:138–152, 1996.

[Ber68] Elwyn R. Berlekamp. *Algebraic coding theory.* McGraw-Hill Book Co., New York, 1968.

[Buc85] B. Buchberger. Gröbner bases: An algorithmic method in polynomial ideal theory. In *Multidimensional systems theory, Progress, directions and open problems, Math. Appl.*, pages 184–232. D. Reidel Publishing Company, 1985.

[Chi64] R. T. Chien. Cyclic decoding procedure for bose-chauduri-hocquenghem codes. *IEEE Trans. Inf. Theory*, 10:357–363, October 1964.

[CLO97] David Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms.* Undergraduate Texts in Mathematics. Springer-Verlag, New York, second edition, 1997. An introduction to computational algebraic geometry and commutative algebra.

[CRHT94a] Xuemin Chen, I. S. Reed, T. Helleseth, and T. K. Truong. Algebraic decoding of cyclic codes: a polynomial ideal point of view. In *Finite fields: theory, applications, and algorithms (Las Vegas, NV, 1993)*, volume 168 of *Contemp. Math.*, pages 15–22. Amer. Math. Soc., Providence, RI, 1994.

[CRHT94b] Xuemin Chen, I. S. Reed, T. Helleseth, and T. K. Truong. General principles for the algebraic decoding of cyclic codes. *IEEE Trans. Inform. Theory*, 40(5):1661–1663, 1994.

[CRHT94c] Xuemin Chen, I. S. Reed, T. Helleseth, and T. K. Truong. Use of Gröbner bases to decode binary cyclic codes up to the true minimum distance. *IEEE Trans. Inform. Theory*, 40(5):1654–1661, 1994.

[CRT94] Xuemin Chen, I.S. Reed, and T.K. Truong. Decoding the (73,37,13) quadratic residue code. *IEE Proc., Comput. Digit. Tech.*, 141(5):253–258, 1994.

[Fau99] Jean-Charles Faugère. A new efficient algorithm for computing Gröbner bases (F_4). *J. Pure Appl. Algebra*, 139(1-3):61–88, 1999.

[FGT01] Elisabetta Fortuna, Patrizia Gianni, and Barry Trager. Degree reduction under specialization. *J. Pure Appl. Algebra*, 164(1-2):153–163, 2001. Effective methods in algebraic geometry (Bath, 2000).

[Gia89] Patrizia Gianni. Properties of Gröbner bases under specializations. In *EUROCAL '87 (Leipzig, 1987)*, pages 293–297. Springer, Berlin, 1989.

[HH93] Russell J. Higgs and J. F. Humphreys. Decoding the ternary Golay code. *IEEE Trans. Inf. Theory*, 39(3):1043–1046, 1993.

[Hum92] J. F. Humphreys. Algebraic decoding of the ternary (13, 7, 5) quadratic residue code. *IEEE Trans. Inf. Theory*, 38(3):1122–1125, 1992.

[Kal89] Michael Kalkbrener. Solving systems of algebraic equations by using Gröbner bases. In *EUROCAL '87 (Leipzig, 1987)*, pages 282–292. Springer, Berlin, 1989.

[LN97] Rudolf Lidl and Harald Niederreiter. *Finite fields*. Cambridge University Press, Cambridge, second edition, 1997. With a foreword by P. M. Cohn.

[LVY97] Philippe Loustaunau and Eric Von York. On the decoding of cyclic codes using Gröbner bases. *Appl. Algebra Eng. Commun. Comput.*, 8(6):469–483, 1997.

[MS77] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes*. Amsterdam : North Holland, 1977.

[RRTC01] H. Ruhua, I.S. Reed, T.K. Truong, and X. Chen. Decoding the (47,24,11) quadratic residue code. *IEEE Trans. Inf. Theory*, 47(3):1181–1186, 2001.

[RTCY92] I.S. Reed, T.K. Truong, Xuemin Chen, and X. Yin. The algebraic decoding of the (41, 21, 9) quadratic residue code. *IEEE Trans. Inf. Theory*, 38(3):974–986, 1992.

[RYT90] I.S. Reed, X. Yin, and T.K. Truong. Algebraic decoding of the (32,16,8) quadratic residue code. *IEEE Trans. Inf. Theory*, 36(4):876–880, 1990.

Unité de recherche INRIA Lorraine
LORIA, Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - BP 101 - 54602 Villers-lès-Nancy Cedex (France)

Unité de recherche INRIA Futurs : Domaine de Voluceau - Rocquencourt - BP 105 - 78153 Le Chesnay Cedex (France)
Unité de recherche INRIA Rennes : IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex (France)
Unité de recherche INRIA Rhône-Alpes : 655, avenue de l'Europe - 38330 Montbonnot-St-Martin (France)
Unité de recherche INRIA Rocquencourt : Domaine de Voluceau - Rocquencourt - BP 105 - 78153 Le Chesnay Cedex (France)
Unité de recherche INRIA Sophia Antipolis : 2004, route des Lucioles - BP 93 - 06902 Sophia Antipolis Cedex (France)

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, BP 105 - 78153 Le Chesnay Cedex (France)
http://www.inria.fr
ISSN 0249-6399