On formulas for decoding binary cyclic codes

Daniel Augot
INRIA-Rocquencourt
Domaine de Voluceau
Le Chesnay, FRANCE

Magali Bardet
Laboratoire LITIS
Université de Rouen

Jean-Charles Faugère
INRIA Rocquencourt, Salsa project
Université Pierre et Marie Curie-Paris 6
UMR 7606, LIP6

***Abstract*— We address the problem of the algebraic decoding of any cyclic code up to the true minimum distance. For this, we use the classical formulation of the problem, which is to find the error locator polynomial in terms of the syndromes of the received word. This is usually done with the Berlekamp-Massey algorithm in the case of BCH codes and related codes, but for the general case, there is no generic algorithm to decode cyclic codes. Even in the case of the quadratic residue codes, which are good codes with a very strong algebraic structure, there is no available general decoding algorithm.**

For this particular case of quadratic residue codes, several authors have worked out, by hand, formulas for the coefficients of the locator polynomial in terms of the syndromes, using the Newton identities. This work has to be done for each particular quadratic residue code, and is more and more difficult as the length is growing. Furthermore, it is error-prone.

We propose to automate these computations, using elimination theory and Gröbner bases. We prove that, by computing appropriate Gröbner bases, one automatically recovers formulas for the coefficients of the locator polynomial, in terms of the syndromes.

***Index Terms*— Algebraic decoding, general cyclic codes, Newton identities, elimination theory, Gröbner bases.**

I. Introduction

There is a longstanding problem of efficiently decoding binary quadratic residue codes. For each prime number l such that 2 is a quadratic residue modulo l, there exists essentially one such code. It is a cyclic code of length l, whose defining set if the set of the quadratic residue modulo l. It is proven that the minimum distance of these codes is at least $\lfloor\sqrt{l}\rfloor$ (the square-root bound). But compiled tables show that the minimum distance of these codes is much better than this bound, and it is an open question to find or to estimate the minimum distance of these codes, although some progress has been achieved [1].

Up to date, there is no general decoding algorithm for the whole class of quadratic residue codes. Several efforts have been put up for particular cases, that is to say for each particular length, mainly by Chen, Truong, Reed, Helleseth and others [2], [3], [4], [5], [6], [7], [8], [9], for the lengths 31, 23, 41, 73, 47, 71, 79, 97, 103 and 113. All these decoding algorithms are based on the Newton identities, which involve the so-called *error locator polynomial* and the *syndromes* of the received word. These Newton identities are to be written for each particular length, and then to be worked out for isolating the coefficients of the locator polynomial in terms of the syndromes, while eliminating the *unknown syndromes*, which appear in the Newton identities. This elimination procedure is hand crafted by the authors. So it is tedious, prone to errors, and the authors eventually fail to find formulas for the coefficients of the locator polynomial.

A separate path of research has been to use the theory of Gröbner bases for decoding *any* cyclic code. It was originated by Cooper [10], [11], [12], although the results were unproven. Cooper uses an algebraic system of equations, closely related to the decoding problem, but different from the Newton identities. These works only deal with BCH codes. Later, these algebraic systems have been studied by Loustaunau and von York [13], Caboara and Mora [14], for any cyclic code, and they give proofs of the statements by Cooper. In this vein of research, one studies the ideal generated by the system of equations, and tries to prove that the symbolic locator polynomial belongs to this ideal. Then this polynomial can be found by the computation of a Gröbner with respect to a relevant ordering on the monomials.

These systems of equations, and the correspond so-called CRHT variety, have been extensively studied by Orsini and Sala [15]. They improve by introducing a new variety, which eliminates spurious solutions. Orsini and Sala prove that every cyclic admits a *general error locator polynomial*, which is a polynomial whose coefficients are polynomials whose indeterminates are the syndromes. This polynomial is such that, when evaluated on the syndromes of an error, it turns to be the error locator polynomial of the error. In [16], the same authors extensively compute the general error locator polynomials of all binary cyclic codes of length less than or equal to 63, correcting two errors.

Another system defined by the Newton identities has been considered by Chen, Helleseth, Reed and Truong [17] (see also [18], [19]). In that case, the aim is to prove that the ideal generated by the Newton identities contains, for each coefficient σ_i of the locator polynomial, a polynomial of whose leading monomial is of degree one in σ_i, and that this polynomial does not involve the unknown syndromes. So we may say that we recover also a general error locator polynomial, but with a different system of equations.

II. Our contribution

We have already discussed the use of Gröbner bases for decoding cyclic codes [20] with a system different from the Newton identities. At that time, we discussed the computation of Gröbner bases online: for each received word, one computes

the syndromes, and substitutes them into an algebraic system of equations. Then the computation of the Gröbner basis gives the coefficients of the locator polynomials, which are sought for.

In this work, we discuss the idea of precomputing the Gröbner basis of a system in which the syndromes are left as indeterminates. Then we show that this Gröbner basis leads to formulas for the coefficients of the locator polynomial. This is called *one-step decoding*.

Still, there is the problem that these formulas for the coefficients σ_i's of the locator polynomial are of the form $p_i\sigma_i + q_i = 0$, where p_i, q_i involve only the syndromes. Thus finding σ_i can be done as follows

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

which may lead to a division by zero, when the actual values of the syndromes are substituted into p_i.

Our second contribution is to introduce a new ideal, which contains formulas of the form $\sigma_i + q_i = 0$. Thus finding the σ_i's do not involve any division after substitution.

III. Definitions

We consider only binary cyclic codes. Let n be the length, which is odd, and α be a primitive n-th root of unity in some extension $\mathbb{F}_{2^m}$ of $\mathbb{F}_2$. To each binary word $c = (c_0, \ldots, c_{n-1})$ of length n, is associated the polynomial $c_0 + c_1X + \cdots + c_{n-1}X^{n-1}$. The Fourier Transform of c is the vector $S = (S_0, \ldots, S_{n-1})$, with $S_i = c(\alpha^i)$. A cyclic code is built by considering a *defining set* $Q = \{i_1, \ldots, i_l\} \subset \{0, 1, \ldots, n-1\}$. The cyclic code C of defining set Q is then the set of words whose Fourier Transform satisfies

$$S_{i_1} = \cdots = S_{i_l} = 0.$$

Let $y \in \mathbb{F}_2^n$ the received word, to be decoded. As usual, we write $y = c + e$, where c is the codeword, and e is the error. We compute the Fourier Transform S of y, and for $i \in Q$, we have:

$$S_i = y(\alpha^i) = c(\alpha^i + e(\alpha^i) = e(\alpha^i), \quad i \in Q,$$

since $c \in C$. The S_i's, $i \in Q$ are called the *syndromes* of e, and the S_j's, $j \notin Q$ are the *unknown syndromes*. The decoding problem is to find e given the syndromes S_i's, $i \in Q$, under the constraint that the weight of e is bounded by $t = \lfloor \frac{d-1}{2} \rfloor$, where d is the minimum distance of C, and the *decoding radius* of C.

IV. The Newton's identities

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 $\alpha^{u_1}, \ldots, \alpha^{u_l}$, which are called the *locators* of e. We note by $Z_1, \ldots, Z_w$ 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 [21].

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 [22]):

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

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, $i \in Q$, and the S_i's, $i \notin Q$, that we try to eliminate. Our objective is to find an expression of the σ_i's in terms of the S_i's, $i \in Q$.

V. Elimination theory

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

$$I_{N,w} : \left\langle \begin{array}{ll} S_i + \sum_{j=1}^{i-1}\sigma_j S_{i-j} + i\sigma_i, & i \leq w \\ S_i + \sum_{j=1}^{w}\sigma_j S_{i-j}, & n + w \geq i > w \end{array} \right\rangle. \quad (2)$$

Let us note by σ the set of the variables $\sigma_1, \ldots, \sigma_w$, by S_Q the set $\{S_i; i \in Q\}$, and S_N the set $\{S_i, i \notin Q\}$. Then we have that $I_{N,w}$ is an ideal in the polynomial algebra $\mathbb{F}_2[\sigma, S_Q, S_N]$.

A *Gröbner basis* of an ideal I is a particular set of generators of I, which is well behaved with respect to various operations: it enables to test equalities of ideals, to test ideal membership and so on. Due to lack of space, we will not recall to formal definition here, which can be found in [23]. We recall that this notion depends on a monomial ordering: for each particular monomial ordering there exists a corresponding Gröbner basis. Of utmost importance for us are the following considerations [23].

Definition 1: Let $I \subset \mathbb{F}_2[x_1, \ldots, x_m]$. Then the ideal

$$I_k = I \cap \mathbb{F}_2[x_{k+1}, \ldots, x_m]$$

is the k-th *elimination ideal*. It is the set of all the relations that can be obtained on $x_{k+1}, \ldots, x_m$, by elimination of the k first variables $x_1, \ldots, x_k$.

Proposition 1: Let $I \subset \mathbb{F}_2[x_1, \ldots, x_m]$ be an ideal and let G be a Gröbner basis for the lexicographical ordering, with $x_1 > \cdots > x_n$. Then, the set

$$G_k = G \cap \mathbb{F}_2[x_{k+1}, \ldots, x_m]$$

is a Gröbner basis of the k-th elimination ideal $I_k = I\mathbb{F}_2[x_{k+1}, \ldots, x_m]$.

Thus it is sufficient to compute a single Gröbner G, and to retain the relevant polynomials, to eliminate the unwanted variables. For the problem of decoding, we get:

Proposition 2: Let be given a monomial ordering such that the S_i's, $i \notin Q$ are greater than the S_i's, $i \in Q$, and the σ_i's. Let G be a Gröbner basis of $I_{N,w}$ for this ordering. Then

$$G \cap \mathbb{F}_2[\sigma, S_Q]$$

is a Gröbner basis of the elimination ideal $I_{N,w} \cap \mathbb{F}_2[\sigma, S_Q]$.

This means that, if we compute a Gröbner basis of $I_{N,w}$ for a relevant ordering, we find a (finite) basis of all the relations between the σ_i's and the S_i's, $i \in Q$. The problem is that these relations may not be of degree one in the σ_i's. Our aim is to prove that there exists relations of the form $p_i\sigma_i + q_i$ in this ideal, where $p_i, q_i \in \mathbb{F}_2[S_Q]$.

VI. The variety associated to the Newton identities

First we have to study $V(I_{N,w})$ the *variety associated* to the ideal $I_{N,w}$. It is the set of all σ_i's, S_i's, which satisfy the Newton identities. Note that we consider this variety in $\overline{\mathbb{F}}_2$, the algebraic closure of $\mathbb{F}_2$. We have the following Theorem, which is an extension of the main result of [24].

Theorem 1: Let (σ, S) be in $V(I_{N,w})$, with $\sigma = (\sigma_1, \ldots, \sigma_w) \in \overline{\mathbb{F}}_2^w$ and $S = (S_0, \ldots, S_{n-1}) \in \overline{\mathbb{F}}_2^n$. Let e be the inverse Fourier Transform of S. Note that *a priori* e has coordinates in $\overline{\mathbb{F}}_2$. Then

1. the weight of e is less than w;
2. e has indeed coordinates in $\mathbb{F}_2$;
3. if $\sigma(Z)$ is the polynomial

$$1 + \sum_{i=1}^{w} \sigma_i Z^i,$$

and if $\sigma_e(Z)$ is the locator polynomial of e, then there exists an integer l and a polynomial $G(Z)$ such that

$$\sigma(Z) = \sigma_e(Z) G(Z)^2 Z^l.$$

Proof: Omitted due to lack of space. ∎

From the NullStellenSatz [23], we have:

Corollary 1: Let $I_{N,w} \cap \mathbb{F}_2[S_Q, S_N]$ be the elimination ideal of the σ_i's. If $I_{N,w}$ is radical, then $I_{N,w} \cap \mathbb{F}_2[S_Q, S_N]$ is the set of all the relations between the coefficients of the Fourier Transform of the binary words of weight less than w. Furthermore, if we eliminate the S_i's, $i \notin Q$, then $I_{N,w} \cap \mathbb{F}_2[S_Q]$ is the set of all the relations between the syndromes of the words of weight less than $w \leq t$.

Corollary 2: Let $S_{Q,e}$ be the set of syndromes of some word e. Let T_w be a basis of $I_{N,w} \cap \mathbb{F}_2[S_Q]$, then e has weight $w \leq t$ if and only if

$$t(S_{Q,e}) = 0, \text{for all } t \in T_v, \text{ for all } v \leq w. \tag{3}$$

VII. Radical ideals

In the above, we have stumbled on the difficulty on proving that $I_{N,w}$ is a radical ideal. We believe it is, but we have not been able to prove it. To overcome this difficulty, we consider the ideal $I^0_{N,w}$, where we add the "field equations" to ensure that the σ_i's and the S_i's belong to the field $\mathbb{F}_{2^m}$. It is the ideal

$$I^0_{N,w} = I_{N,w} + \left\langle \begin{array}{l} S_i^{2^m} + S_i, i \in \{0, \ldots, n-1\}, \\ \sigma_i^{2^m} + \sigma_i, i \in \{1, \ldots, w\} \end{array} \right\rangle. \tag{4}$$

Thanks to these field equations, the ideal $I^0_{N,w}$ is radical, and has dimension zero (it has a finite number of solutions). It is a consequence of [25, Chap. 2, Prop. 2.7], which implies that, if an ideal contains, for each variable, a square-free univariate polynomial in this variable, then it is radical.

One can prove the following.

Theorem 2: For each binary word e of weight w less than t, for each $i \in \{1, \ldots, w\}$, the ideal $I^0_{N,w}$ 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 the syndromes of e.

Proof: Omitted due to lack of space. ∎

Thus the decoding algorithm could be:

1) (precomputation) For each $w \in \{1, \ldots, t\}$, compute a Gröbner basis G_w of $I^0_{N,w}$, 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, for each i, collect all the relations $p_i\sigma_i + q_i$, call $\Sigma_{w,i}$ this set;
3) (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;
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 (3).
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 $p_i\sigma_+ q_i$, $i \in \{1, \ldots, w\}$, 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 $I^0_{N,w}$ 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 $I_{N,w}$ without the field equations.

VIII. An augmented ideal

The difficulty, as mentioned above, is that we have not proven that $I_{N,w}$ is a radical ideal, which is a necessary ingredient, among others, to prove Theorem 2. We will build an ideal which contains $I_{N,w}$, which is radical, and which

will contain "nice" formulas. First we introduce the ideal I_σ corresponding to the definitions of the elementary symmetric functions, and I_S corresponding to the definition of the coefficients of the Fourier Transform:

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

and

$$I_S = \left\langle \begin{array}{ll} S_i - \sum_{j=1}^{w} Z_j^i, & i \in \{1, \dots, n+w\}; \\ S_{i+n} - S_i, & i \in \{1, \dots, w\} \end{array} \right\rangle.$$

Note this ideal belongs to the polynomial ring $\mathbb{F}_2[\sigma, S, Z_1, \dots, Z_w]$. When we eliminate the $Z_i's$, we have the following

Proposition 3:

$$(I_S + I_\sigma) \cap \mathbb{F}_q[S, \sigma] = I_N$$

Proof: Omitted due to lack of space. ∎

Let us introduce the following polynomial:

$$\Delta(Z_1, \dots, Z_w) = Z_1 \cdots Z_w \prod_{1 \le i < j \le w} (Z_i - Z_j).$$

This polynomial has the property that, if the weight w_e of e of the error is less than w, then one can extend the locators $Z_1, \dots, Z_{w_e}$ into $Z_1, \dots, Z_w$, in a way such that $Z_1, \dots, Z_w$ are zeros of Δ. In other words, it captures, in some sense, the property of being of weight strictly less than w.

We need the definition of a saturated ideal, with respect to a polynomial.

Definition 2: Let $I \subset \mathbb{F}[x_1, \dots, x_n]$ be an ideal, and $f \in \mathbb{F}[x_1, \dots, x_n]$ be given. The saturated ideal of I with respect to f, denoted $I : f^\infty$, is the ideal

$$I : f^\infty = \{g \in \mathbb{F}[x_1, \dots, x_n] : f^m g \in I \text{ for some } m > 0\} \tag{5}$$

One has that, under some restrictions, the variety associated to the saturated ideal $I : f^\infty$, does not contain the zeros of f.

Proposition 4: Let $I = \langle f_1, \dots, f_s \rangle \subset \mathbb{F}[x_1, \dots, x_n]$ be an ideal and $f \in \mathbb{F}[x_1, \dots, x_n]$ be given. Let y be a new indeterminate. Consider

$$\tilde{I} = \langle f_1, \dots, f_s, 1 - fy \rangle \subset \mathbb{F}[x_1, \dots, x_n, y],$$

then $I : f^\infty = \tilde{I} \cap \mathbb{F}[x_1, \dots, x_n]$.

Thus the saturated ideal can be computed by a Gröbner basis computation and elimination. Now we introduce the saturated ideal

$$(I_\sigma + I_S) : \Delta^\infty \tag{6}$$

Then

Proposition 5: The ideal

$$(I_\sigma + I_S) : \Delta^\infty$$

contains the polynomials

$$\begin{array}{l} Z_i^n + Z_i, i \in \{1, \dots, w\}, \\ \sigma_i^{2^m} + \sigma_i, i \in \{1, \dots, w\}, \\ S_i^{2^m} + S_i, i \in \{0, \dots, n-1\}. \end{array}$$

Proof: Omitted due to lack of space. ∎

In particular, it is a radical ideal. Then, by elimination of the Z_i's, we have the ideal $I_{N,w}^\infty$:

$$I_{N,w}^\infty = ((I_\sigma + I_S) : \Delta^\infty) \cap \mathbb{F}_2[\sigma, S] \supset I_{N,w}$$

Note that a basis of $I_{N,w}^\infty$ can be computed by computing a Gröbner basis of $I_S + I_\sigma + (1 - y\Delta)$ for an ordering eliminating y and Z_i's, and by retaining the polynomials in terms of the σ_i's and the S_i's. Note also that $I_{N,w}^\infty$ is a radical ideal.

The variety associated to $I_{N,w}^\infty$ can be described as follows:

Theorem 3: The variety $V(I_{N,w}^\infty)$ is exactly the set of the elementary symmetric functions and the elementary power-sum functions of the words of weight exactly w.

Proof: Omitted due to lack of space. ∎

In particular, we have:

Corollary 3: Let $S_{Q,e}$ be the set of syndromes of some word e. Let T_w be a basis of $I_{N,w}^\infty \cap \mathbb{F}_2[S_Q]$, then e has weight w if and only if

$$t(S_{Q,e}) = 0, \text{for all } t \in T_w. \tag{7}$$

Armed with this Theorem, and with the radicality of $I_{N,w}^\infty$, we can prove:

Theorem 4: For each $i \in \{1, \dots, w\}$, $I_{N,w}^\infty$ contains a polynomial of the form $\sigma_i + q_i$, with $q_i \in \mathbb{F}_2[S_Q]$.

Note that this polynomial will appear in a Gröbner basis of $I_{N,w}^\infty$, computed as above.

The algorithm for decoding is

1) (precomputation) For each $w \in \{1, \dots, t\}$, compute a Gröbner basis G_w of $I_{N,w}^\infty$, written for the weight w;
2) (precomputation) From each G_w, for each i, pick the polynomial $q_{i,w}$ which appears in the polynomial $\sigma_i + q_{i,w}$ in Theorem 4.
3) (precomputation) From each G_w, pick all the polynomials in $G_w \cap \mathbb{F}_2[S_Q]$, call T_w 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) for each possible weight w of the error, find the weight w_e of the error using the criterion (7).
6) (online) compute $\sigma_i = q_{i,w_e}(S_{Q,e})$.

Thus we have removed the problem of the field equations, and the problem of the division by zero.

IX. Conclusion

For the decoding of any cyclic code, up to the true minimum distance, we have shown how to find relations of degree one for the coefficients of the locator polynomials, in terms of the syndromes. These relations can be computed from the Newton identities. Then we have introduced an ideal containing the ideal generated by the Newton identities, which give formulas for the coefficient of the locator polynomial, with no leading terms (and thus avoiding the problem of dividing by zero).

We thus obtain a general error locator polynomial as Orsini and Sala [15], but we do not if it the same polynomial. That should be investigated in the future.

REFERENCES

[1] F. Voloch, "Asymptotics of the minimal distance of quadratic residue codes," 2004. [Online]. Available: http://www.ma.utexas.edu/users/voloch/preprint.html

[2] I. S. Reed, X. Yin, and T.-K. Truong, "Algebraic decoding of the (32, 16, 8) quadratic residue code," *IEEE Transactions on Information Theory*, vol. 36, no. 4, pp. 876–880, 1990. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=53750

[3] I. S. Reed, X. Yin, T.-K. Truong, and J. K. Holmes, "Decoding the (24,12,8) golay code," *Computers and Digital Techniques, IEE Proceedings-*, vol. 137, no. 3, pp. 202–206, 1990. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=50613

[4] I. S. Reed, T.-K. Truong, X. Chen, and X. Yin, "The algebraic decoding of the (41, 21, 9) quadratic residue code," *IEEE Transactions on Information Theory*, vol. 38, no. 3, pp. 974–986, 1992. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=135639

[5] X. Chen, I. S. Reed, and T.-K. Truong, "Decoding the (73, 37, 13) quadratic residue code," *IEE Proceedings on Computers and Digital Techniques*, vol. 141, no. 5, pp. 253–258, 1994. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=326788

[6] E. H. Lu, H. P. Wuu, Y. C. Cheng, and P. C. Lu, "Fast algorithms for decoding the (23,12) binary Golay code with four-error-correcting capability," *International Journal of Systems Science*, vol. 26, no. 4, pp. 937–945, 1995.

[7] R. He, I. S. Reed, T.-K. Truong, and X. Chen, "Decoding the (47,24,11) quadratic residue code," *IEEE Transactions on Information Theory*, vol. 47, no. 3, pp. 1181–1186, 2001. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=915677

[8] Y. Chang, T.-K. Truong, I. S. Reed, H. Y. Cheng, and C. D. Lee, "Algebraic decoding of (71, 36, 11), (79, 40, 15), and (97, 49, 15) quadratic residue codes," *IEEE Transactions on Communications*, vol. 51, no. 9, pp. 1463–1473, 2003. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1231644

[9] T.-K. Truong, Y. Chang, Y.-H. Chen, and C. D. Lee, "Algebraic decoding of (103, 52, 19) and (113, 57, 15) quadratic residue codes," *IEEE Transactions on Communications*, vol. 53, no. 5, pp. 749–754, 2005. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1431115

[10] A. B. Cooper III, "Direct solution of BCH syndrome equations," in *Communications, Control, and Signal Processing*, E. Arkian, Ed. Elsevier, 1990, pp. 281–286.

[11] ——, "A one-step algorithm for finding BCH error locator polynomials," in *International Symposium ion Information Theory, ISIT 1991*, 1991, pp. 93–93. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=695149

[12] ——, "Finding BCH error locator polynomials in one step," *Electronics Letters*, vol. 27, no. 22, pp. 2090–2091, 1991. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=133007

[13] P. Loustaunau and E. V. York, "On the decoding of cyclic codes using Gröbner bases," *Applicable Algebra in Engineering, Communication and Computation*, vol. 8, no. 6, pp. 469–483, 1997. [Online]. Available: http://dx.doi.org/10.1007/s002000050084

[14] M. Caboara and T. Mora, "The Chen-Reed-Helleseth-Truong decoding algorithm and the Gianni-Kalkbrenner Gröbner shape theorem," *Applicable Algebra in Engineering, Communication and Computing*, vol. 13, no. 3, pp. 209–232, 2002. [Online]. Available: http://dx.doi.org/10.1007/s002000200097

[15] E. Orsini and M. Sala, "Correcting errors and erasures via the syndrome variety," *Journal of Pure and Applied Algebra*, vol. 200, no. 1-2, pp. 191–226, August 2005. [Online]. Available: http://www.sciencedirect.com/science/article/B6V0K-4FDJ795-3/2/32048d373e220e817988980735edcbfd

[16] ——, "General error locator polynomials for binary cyclic codes with $tle2$ and $n < 63$," *IEEE Transactions on Information Theory*, vol. 53, no. 3, pp. 1095–1107, 2007. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4106137

[17] X. Chen, I. S. Reed, T. Helleseth, and T. K. Truong, "General principles for the algebraic decoding of cyclic codes," *IEEE Transactions on Information Theory*, vol. 40, no. 5, pp. 1661–1663, September 1994. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=333886

[18] M. de Boer and R. Pellikaan, *Gröbner bases for codes*, ser. Algorithms and Computation in Mathematics. Springer, 1999, no. 4, ch. 10, pp. 237–259. [Online]. Available: http://www.win.tue.nl/ ruudp/paper/34.pdf

[19] ——, *Gröbner bases for decoding*, ser. Algorithms and Computation in Mathematics. Springer, 1999, no. 4, ch. 11, pp. 260–275. [Online]. Available: http://www.win.tue.nl/ ruudp/paper/35.pdf

[20] D. Augot, M. Bardet, and J.-C. Faugère, "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*, 2003, pp. 362–362. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1228378

[21] R. T. Chien, "Cyclic decoding procedures for Bose-Chaudhuri-Hocquenghem codes," *IEEE Transactions on Information Theory*, vol. 10, no. 4, pp. 357–363, 1964. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1053699

[22] F. J. Macwilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, ser. North-Holland Mathematical Library. North Holland, January 1983.

[23] D. Cox, J. Littel, and D. O'Shea, *Ideals, Varieties and Algorithms*. Springer, 1992.

[24] D. Augot, "Description of minimum weight codewords of cyclic codes by algebraic systems," *Finite Fields Appl.*, vol. 2, no. 2, pp. 138–152, 1996.

[25] D. A. Cox, J. Little, and D. O'Shea, *Using Algebraic Geometry*, ser. Graduate Texts in Mathematics. Springer, March 2005.