Algebraic Decoding of Negacyclic Codes over Z4

Eimear Byrne, Marcus Greferath, Jens Zumbragel, Jaume Pernas

Algebraic Decoding of Negacyclic Codes over $\mathbb{Z}_4$

Eimear Byrne[1], Marcus Greferath[1], Jaume Pernas[2], and Jens Zumbrägel[1]

[1] Claude Shannon Institute, School of Mathematical Sciences
University College Dublin, Ireland*
ebyrne@ucd.ie, marcus.greferath@ucd.ie, jens.zumbragel@ucd.ie
[2] Departament d'Enginyeria de la Informació i de les Comunicacions
Universitat Autonoma de Barcelona, España**
jaume.pernas@uab.cat

Abstract. We investigate Berlekamp's negacyclic codes and discover that these codes, when considered over the integers modulo 4, do not suffer any of the restrictions on the minimum distance observed in Berlekamp's original papers [2, 3]. We present an algebraic decoding algorithm for this class of codes that corrects any error pattern of Lee weight $\leq t$. Our treatment uses Gröbner bases, the decoding complexity is quadratic in t.

Keywords: negacyclic code, integers modulo 4, Lee metric, Galois Ring, decoding, Gröbner bases, key equation, solution by approximations, module of solutions.

1 Introduction

In his seminal papers [2, 3], Berlekamp introduced negacyclic codes over odd prime fields $\mathrm{GF}(p)$, and designed a decoding algorithm that corrects up to $t \leq \frac{p-1}{2}$ Lee errors. The main idea in Berlekamp's contribution is to represent error patterns of weight w solely by error locator polynomials of degree w, where the error values are encoded essentially in the multiplicity of the respective error locations. Berlekamp's error locator polynomial satisfies some type of key equation that is solved during the decoding procedure. Its solution ultimately depends on the multiplicative invertibility of all odd integers $i \leq 2t-1$ in (a field extension of) $\mathrm{GF}(p)$ where t is the maximum Lee weight of all correctable error patterns. This finally requires $t < \frac{p+1}{2}$, which is the reason why this idea yields only a very small class of useful codes.

The project underlying this article revisits Berlekamp's work and starts with the observation that almost all of the algebra used in the quoted papers is still

* The work of E. Byrne, M. Greferath, and J. Zumbrägel was partially supported by the Science Foundation Ireland under Grants 06/MI/006, 08/RFP/MTH1181, and 08/IN.1/I1950.

** The work of J. Pernas was partially supported by the Spanish MICINN under Grants PCI2006-A7-0616 and TIN2010-17358, and by the Catalan AGAUR under Grant 2009SGR1224.

valid in a Galois ring, i.e. a Galois extension of the integers modulo p^m where m might be greater than 1. The divisibility condition mentioned above causes problems if and only if p is odd, and this brought us to the idea to study codes over $\mathbb{Z}_{2^m}$.

The paper at hand considers the simplest (non-trivial) case, namely the case where $m = 2$, which means we consider negacyclic codes over $\mathbb{Z}_4$ under the Lee metric. We will show that a negacyclic code is indeed of minimum Lee distance at least $2t + 1$ if its generator polynomial has roots $\alpha, \alpha^3, \ldots, \alpha^{2t-1}$ for a primitive $2n$th root of unity α in a Galois extension of $\mathbb{Z}_4$. No restriction on t will be imposed. We present an algebraic decoding algorithm for this class of codes that corrects any error pattern of Lee weight $\leq t$. In fact, if the minimum Lee distance is at least $2r+1$ (where $r \geq t$), we derive a key equation which has a unique solution in all error patterns of Lee weight r. Then we find the unique solution using Gröbner bases, provided at most t errors have occured.

An extended version of this paper including all proofs is available online [5].

2 Preliminaries

Throughout this paper, let R denote the Galois ring $\mathrm{GR}(4, m)$ of characteristic 4, order 4^m, and residue field $K = \mathrm{GF}(2^m)$. We let $\mu : R \longrightarrow K$, $a \mapsto a + 2R$ be the canonical map from R onto K.

The structure of R is well understood (cf. [8]). Its multiplicative group $R^\times$ has order $2^m(2^m-1)$ and contains a unique cyclic subgroup of order 2^m-1. This group, in union with zero, forms the so-called *Teichmüller set* of R, which we denote by $\mathcal{T}$. The set $\mathcal{T}$ forms a complete set of coset representatives of $2R$ in R and so the image of $\mathcal{T}$ under μ is the residue field K. Each element $a \in R$ can be expressed in the canonical form $a := a_0 + 2a_1$ for suitable $a_0, a_1 \in \mathcal{T}$. The automorphism group of R is cyclic of order m and with respect to the above canonical form is generated by the map $\pi : R \longrightarrow R$, $a_0 + 2a_1 \mapsto a_0^2 + 2a_1^2$. Note that for an element θ of $\mathcal{T}$ we have $\pi(\theta) = \theta^2$.

3 Negacyclic Codes Over $\mathbb{Z}_4$

The following is a BCH-like description of negacyclic codes over $\mathbb{Z}_4$, and can be read as the obvious extension of Berlekamp's work in [2, 3]. We outline the theory for the convenience of the reader, see [9] for further details.

Definition 1. *Let n be a positive integer. A* negacyclic code *of length n over $\mathbb{Z}_4$ is an ideal in the ring $\mathbb{Z}_4[x]/\langle x^n+1\rangle$.*

We will henceforth assume that n is odd. Then there is a primitive $2n$th root of unity α in R such that $\alpha^n = -1$, i.e., $\alpha = -\beta$, where β is a primitive nth root of unity in R.

Any $\mathbb{Z}_4$-negacyclic code is a principal ideal in $\mathbb{Z}_4[x]/\langle x^n+1\rangle$, in fact it is generated by a polynomial of the form $a(b + 2) \in \mathbb{Z}_4[x]$ where $x^n + 1 = abc$

and a, b, c are pairwise coprime polynomials, in which case the code has size $4^{\delta c}2^{\delta b}$ where δf denotes the degree of the polynomial f (cf. [9, Th. 2.7]). There is a natural correspondence between cyclic and negacyclic codes over $\mathbb{Z}_4$. This is given by the map

$$\lambda : \mathbb{Z}_4[x]/\langle x^n - 1\rangle \longrightarrow \mathbb{Z}_4[x]/\langle x^n + 1\rangle\,, \quad a(x) \mapsto a(-x)\,.$$

Clearly, λ is ring isomorphism, from which it follows that any ideal C in $\mathbb{Z}_4[x]/\langle x^n - 1\rangle$ is mapped to an ideal $\lambda(C)$ of $\mathbb{Z}_4[x]/\langle x^n + 1\rangle$. Moreover, λ is an isometry with respect to the Lee distance, since for every $c = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} \in \mathbb{Z}_4[x]/\langle x^n - 1\rangle$, we have $\lambda(c) = c_0 - c_1 x \pm \cdots + c_{n-1}x^{n-1}$ which is obviously of the same Lee weight as c.

Theorem 1. *Let C be a negacyclic code over $\mathbb{Z}_4$ of odd length n whose generator polynomial g has the roots α, α^3, ..., α^{2t-1} for some primitive $2n$th root of unity $\alpha \in R$ such that $\alpha^n = -1$. Then C has minimum Lee distance d_{Lee} at least $2t+1$.*

Proof. Let D be the pre-image of C under λ. Then D is a cyclic code of length n, with generator polynomial f satisfying $\lambda(f) = g \in \mathbb{Z}_4[x]$. Then f has the roots $\beta, \beta^3, \ldots, \beta^{2t-1}$ where $\beta = -\alpha$ is a primitive nth root of unity in R. Now $f \in \mathbb{Z}_4[x]$ is fixed by the automorphism π, so that $0 = \pi(f(\theta)) = f(\pi(\theta))$ for any root θ of f in R. Since β is contained in the Teichmüller set of R, f also has the roots $\pi^j(\beta^i) = \beta^{2^j i}$ for $i \in \{1, 3 \ldots, 2t-1\}$. Therefore, f has the $2t$ consecutive roots $\beta, \beta^2, \ldots, \beta^{2t}$. Therefore a generalization of the well-known BCH bound (see for example [4, Th. IV.1]) shows that D has minimum Hamming distance at least $2t + 1$. This gives a trivial lower bound on the minimum Lee distance of D. The claim now follows from the above isometry observation. □

Remark 1. The lower bound on the Lee distance of negacyclic codes given in Theorem 1 is in general not sharp. Indeed there are codes C with $d_{\mathrm{Lee}} > 2t + 1$, as Table 1 shows. If the actual Lee distance is at least $2r + 1$ with $r > t$ we will see in the next section that the key equation carries sufficient information to determine all error pattern of Lee weight at most r, thus being able to correct up to r errors. We will then present a concrete decoding algorithm for error patterns up to Lee weight t.

Table 1. Parameters of negacyclic codes of length n, designed error-correcting capability t, and rank k (i.e., size 4^k).

n	t	k	$2t+1$	d_{Lee}
15	1	11	3	3
	2	7	5	5
	3	5	7	10
31	1	26	3	4
	2	21	5	7
	3	16	7	12
	5	11	11	16
	7	6	15	26

4 The key equation

Let C be a negacyclic code with roots α, α^3, ..., α^{2t-1} and minimum Lee distance $d_{\text{Lee}} \geq 2r+1$. Let $v \in \mathbb{Z}_4[z]$ be a received word satisfying $d(v,C) \leq r$. We will design a decoder to retrieve the unique error polynomial e satisfying $e = v - c$ for some codeword c, where e has Lee weight at most r. Most of what follows will be reminiscent of the according steps in Berlekamp's papers [2, 3]. We will amend the methods from those sources to the situation at hand.

Let w denote the Lee weight. We define the error locator polynomial

$$\sigma = \prod_{i=0}^{n-1} (1 - X_i z)^{w(e_i)} \in R[z] \,, \tag{1}$$

where $X_i = 0$ if $e_i = 0$, $X_i = \alpha^i$ if $e_i \in \{1, 2\}$, and $X_i = -\alpha^i = \alpha^{i+n}$ if $e_i = 3$. For each positive integer k, we let s_k denote the sum of the kth powers of the reciprocals of the roots of σ, including repeated roots, i.e.

$$s_k = \sum_{j=0}^{n-1} w(e_j) X_j^k \,, \quad k \geq 1 \,.$$

We note that $w(e_j)X_j^k = e_j \alpha^{jk}$ holds for all odd k. Hence, for each $k \in \{1, 3, \ldots, 2t-1\}$, the kth syndrome $s_k = e(\alpha^k) = v(\alpha^k)$ is known to the decoder. Let s denote the power series $\sum_{k=1}^{\infty} s_k z^k \in R(z)$. We have

$$\sigma'(z) = -\sum_{j=0}^{n-1} w(e_j) X_j \prod_{i \neq j} (1 - X_i z)^{w(e_i)} (1 - X_j z)^{w(e_j)-1} \,,$$

and thus

$$\begin{aligned} z\sigma'(z) &= -z \sum_{j=0}^{n-1} \prod_{i=0}^{n-1} (1 - X_i z)^{w(e_i)} \frac{w(e_j) X_j}{1 - X_j z} = -\sigma(z) \sum_{j=0}^{n-1} w(e_j) \sum_{k=1}^{\infty} (X_j z)^k \\ &= -\sigma(z) \sum_{k=1}^{\infty} \Big(\sum_{j=0}^{n-1} w(e_j) X_j^k \Big) z^k = -\sigma(z) \sum_{k=1}^{\infty} s_k z^k = -\sigma(z) s(z) \,. \end{aligned}$$

Therefore

$$s\sigma + z\sigma' = 0 \,, \tag{2}$$

where the coefficients $s_1, s_3, \ldots, s_{2t-1}$ are known to the decoder. For any power series $P(z) = \sum_{k=0}^{\infty} P_k z^k \in R(z)$ we denote the even part and the odd part by $P_e = \sum_{j \geq 0} P_{2j} z^{2j}$ and $P_o = \sum_{j \geq 0} P_{2j+1} z^{2j+1}$, respectively. Then the even part and the odd part of equation (2) read

$$s_e \sigma_e + s_o \sigma_o + z(\sigma_e)' = 0 \,, \tag{3}$$

$$s_e \sigma_o + s_o \sigma_e + z(\sigma_o)' = 0 \,. \tag{4}$$

Subtracting σ_e times equation (4) from σ_o times equation (3) results in the equation

$$s_o(\sigma_o^2 - \sigma_e^2) + z\big((\sigma_e)'\sigma_o - (\sigma_o)'\sigma_e\big) = 0\,, \tag{5}$$

which involves only the odd part of s, the latter being known modulo z^{2t+1}. Now let $u = \frac{\sigma_o}{\sigma_e} \in R(z)$ and rewrite equation (5) to obtain

$$s_o(u^2 - 1) = zu'\,, \tag{6}$$

from which we can recursively compute the coefficients $u_1, u_3, u_5, \ldots u_{2t-1}$ via the equations $u_1 = -s_1$, $u_3 = \frac{1}{3}(-s_3 + u_1^2 s_1)$, $u_5 = \frac{1}{5}(-s_5 + u_1^2 s_3 + 2u_1 u_3 s_1)$, etc. The reader should notice that this is the point where Berlekamp's original approach can continue only by imposing a severe restriction on t. In our situation however all the above denominators are invertible in R.

Clearly, u is an odd function and so we may define the power series T by

$$T(z^2) = (1 + zu(z))^{-1} - 1\,. \tag{7}$$

Moreover, the coefficients $T_1, \ldots, T_t$ are all known to the decoder. Next, we define the polynomials $\varphi, \omega \in R[z]$ by the equations

$$\omega(z^2) = \sigma_e(z)\,, \quad \text{and} \quad \varphi(z^2) = \sigma_e(z) + z\sigma_o(z)\,. \tag{8}$$

Noting that $1 + T(z^2) = \frac{\sigma_e}{\sigma_e + z\sigma_o}$ we finally arrive at a key equation:

$$(1 + T)\,\varphi \equiv \omega \mod z^{t+1}\,, \tag{9}$$

which is the main task of the decoder to solve.

Knowledge of φ and ω is sufficient to recover the error locations along with their multiplicities. Using equation (8) we may obtain σ. The decoder could then run through the $2n$ roots of unity $1, \alpha, \ldots, \alpha^{2n-1}$ and determine the error polynomial e by evaluating $\sigma(\alpha^{-j})$ and $\sigma(\alpha^{-j+n})$ for all $j \in \{0, \ldots, n-1\}$.

Now we will show that the key equation carries sufficient information to determine any error pattern of Lee weight at most r. Let $B(0, r)$ denote the ball in $\mathbb{Z}_4^n$ centered in 0 with radius r, and let $\alpha : B(0, r) \to R[z]$ be the function $e \mapsto \sigma$, mapping an error pattern to its error locator polynomial (see equation (1)), which is injective. Then we consider the function

$$f : \alpha(B(0, r)) \to R^t\,, \quad \sigma \mapsto (T_1, \ldots, T_t)\,,$$

where the coefficients $T_1, \ldots, T_t$ of the power series T are obtained as outlined above (see equations (6) and (7)).

Lemma 1. *The map $f : \sigma \mapsto (T_1, \ldots, T_t)$ is injective on $\alpha(B(0, r))$.*

Proof. Consider the syndrome map $\mathbb{Z}_4[z]/\langle z^n{+}1\rangle \to R^t$, $v \mapsto (s_1, \ldots, s_{2t-1})$, with $s_k = v(\alpha^k)$. Its kernel equals the code C of Lee distance at least $2r{+}1$, hence the map is injective on $B(0, r)$. Now we observe that the mappings $(s_1, \ldots, s_{2t-1}) \mapsto (u_1, \ldots, u_{2t-1}) \mapsto (T_1, \ldots, T_t)$ of equations (6) and (7) are bijective. □

Proposition 1. *Let* $S := R[z]/\langle z^{t+1}\rangle$. *For any* $T = \sum_{i=1}^{t} T_i z_i \in S$ *there is at most one error locator polynomial* $\sigma \in \alpha(B(0,r))$ *such that the corresponding key equation* $(1+T)\,\varphi = \omega$ *in* S *is satisfied, where* $\omega(z^2) = \sigma_e(z)$ *and* $\varphi(z^2) = \sigma_e(z) + z\sigma_o(z)$.

Proof. Suppose that $\sigma \in \alpha(B(0,r))$ satisfies $(1+T)\,\varphi = \omega$. Now S is a local ring with maximal ideal $\langle z\rangle$, and as $\sigma(0) = 1$ we have $\varphi(0) = \omega(0) = 1$, so that φ and ω are units in S. This implies $1 + T = \omega\varphi^{-1}$, in particular, T is uniquely determined by the key equation. As also $f(\sigma)$ satisfies the key equation by construction we have thus $T = f(\sigma)$. Since f is injective, it must hold $\sigma = f^{-1}(T)$, and σ is hence uniquely determined. □

In the view of Proposition 1 it remains an open problem to find the unique solution of the key equation efficiently. In the following we assume that e has Lee weight at most t, and we present an efficient decoding method for this case.

For the classical finite field case, there is a unique pair of coprime polynomials $[a,b] \in \mathrm{GF}(p^m)[z]^2$ satisfying the key equation (9) along with the constraints:

$$a(0) = b(0) = 1\,, \quad \delta a \le \tfrac{t+1}{2}\,, \quad \delta b \le \tfrac{t}{2}\,. \tag{10}$$

For the Galois ring case, it is apparent that the required solution pair $[\varphi,\omega]$ satisfies the constraints (10). Although φ and ω are not necessarily coprime in $R[z]$, we will show in the next section that $2 \in R[z]\varphi + R[z]\omega$. Now over the ring R, a solution $[a,b]$ of the key equation (9) satisfying $2 \in R[z]a + R[z]b$ and the constraints (10) will still not be unique in general, but the modulo 2 solution $[\mu a, \mu b] \in K[z]$ is unique, which will be sufficient for the decoding problem.

5 The Ideal Generated by φ and ω

We will show that 2 can be expressed as a $R[z]$-linear combination of φ and ω. First we note some useful observations. The proofs will be largely omitted, due to space considerations.

Let S be a commutative ring with identity 1. For $f, g \in S$ we use the notation $(f,g) := Sf + Sg$ to denote the ideal generated by f and g in S.

Lemma 2. *Let* $f, g, h \in S$. *Then*

(a) $(f,g) = (f, hf+g)$,
(b) $(h,g) = S$ *implies* $(f,g) = (hf,g)$.

Lemma 3. *Let* $a, b, u, v \in S$ *and let* $f = a + b$, $g = u + v$. *Suppose that*

$$2b = 0, \quad (f,g) = S, \text{ and } (g,u) = S\,.$$

Then $(fg, au+bv) = (f,a)$.

We now specialize to the case that $S = R[z]$ where R is a Galois ring with residual field K. Consider the polynomial

$$\Sigma(z) := \prod_{i=1}^{r}(1 - Y_i z)^{a_i} \in R[z] \,,$$

for some $a_i \in \{1, 2\}$ and $Y_i \in R$ such that the $\mu Y_i \in K^\times$ are pairwise distinct. We further let $\tau = \prod_{i=1}^{s}(1 - Y_i z)^2$ and $\varepsilon = \prod_{i=s+1}^{r}(1 - Y_i z)$ be the square and non-square part of Σ (under a suitable re-ordering of the Y_i if necessary). As before, we denote the even and the odd part of a polynomial $f \in R[z]$ by f_e and f_o, respectively.

Lemma 4. *Given the above notation, there holds* $2\tau_o = 0$, $(\tau, \varepsilon) = R[z]$, *and* $(\varepsilon, \varepsilon_e) = R[z]$.

Corollary 1. $(\Sigma, \Sigma_e) = (\tau, \tau_e)$.

Proof. We observe that $\Sigma_e = \tau_e\varepsilon_e + \tau_o\varepsilon_o$. Combining Lemma 3 and Lemma 4 we obtain $(\Sigma, \Sigma_e) = (\tau\varepsilon, \tau_e\varepsilon_e + \tau_o\varepsilon_o) = (\tau, \tau_e)$. □

With these preparations one can prove:

Proposition 2. $2 \in (\Sigma_e, \Sigma_o)$.

Corollary 2. $2 \in (\varphi, \omega)$.

Proof. It is clear that σ has the same form as Σ, defined before, and thus $2 \in (\sigma_o, \sigma_e)$. Moreover

$$(\varphi(z^2), \omega(z^2)) = (\sigma_e(z) + z\sigma_o(z), \sigma_e(z)) = (z\sigma_o(z), \sigma_e(z)) = (\sigma_o, \sigma_e) \,,$$

since $(z, \sigma_e) = R[z]$. As $2 \in (\sigma_o, \sigma_e)$ there exist $a, b \in R[z]$ such that $a\,\varphi(z^2) + b\,\omega(z^2) = 2$. It follows $a_e\,\varphi(z^2) + b_e\,\omega(z^2) = 2$. Thus we have $u\varphi + v\omega = 2$ with $u, v \in R[z]$ such that $u(z^2) = a_e$ and $v(z^2) = b_e$. □

Remark 2. Suppose that no 'double-errors' occurred, i.e., there is no position j with $e_j = 2$. Then we have $\tau = 1$, and by Corollary 1, we have $(\sigma, \sigma_e) = (\tau, \tau_e) = R[z]$. From this it follows $(\varphi, \omega) = R[z]$, as before.

6 The Solution Module of the Key Equation

In this section we investigate the module of solutions to the key equation (9), $M = \{[a, b] \in R[z]^2 \mid a(1 + T) \equiv b \mod z^{t+1}\}$. First we recall some basic facts on Gröbner basis in $R[z]^2$, further details can be found in [1, 4, 6].

Definition 2. *Let ℓ be an integer. We define a term order $<_\ell$ on $R[z]^2$ by*

(a) $[z^i, 0] <_\ell [z^j, 0]$ *and* $[0, z^i] <_\ell [0, z^j]$ *for* $i < j$,
(b) $[0, z^j] <_\ell [z^i, 0]$ *if and only if* $j \le i + \ell$.

Let $<$ denote an arbitrary fixed term order and let $[a,b] \in R[z]^2 \setminus \{0\}$. We denote the leading term of $[a,b]$ by $\mathrm{lt}[a,b]$, its leading coefficient by $\mathrm{lc}[a,b]$, and its leading monomial by $\mathrm{lm}[a,b] = \mathrm{lc}[a,b]\mathrm{lt}[a,b]$. For any $[a,b],[c,d] \in R[z]^2$ we say that $[a,b] \preceq [c,d]$ if and only if $\mathrm{lt}[a,b] \leq \mathrm{lt}[c,d]$. Given a set of non-zero elements of $R[z]^2$ there exists in the set a (not necessarily unique) minimal element with respect to the quasi-order $\preceq$ associated with $<$. We will refer to this element as being minimal with respect to $<$.

We say that $\mathrm{lt}[a,b]$ is on the *left* (resp. *right*) if $\mathrm{lt}[a,b] = [z^i,0]$ (resp. $\mathrm{lt}[a,b] = [0,z^i]$) for some non-negative integer i. A subset $\mathcal{B}$ of a submodule A of $R[z]^2$ is called *Gröbner basis*, if for all $\alpha \in A$ there exists $\beta \in \mathcal{B}$ such that $\mathrm{lm}(\beta)$ divides $\mathrm{lm}(\alpha)$. The structure of a Gröbner basis in $R[z]^2$ is given by the following lemma (cf. [4, Th. V.3]).

Lemma 5. *Let A be a submodule of $R[z]^2$. Suppose that A has elements with leading terms on the left and elements with leading terms on the right. Then A has a (not necessarily minimal) Gröbner basis of the form*

$$\big\{[a,b],[c,d],[g,h],[u,v]\big\}$$

with $\mathrm{lm}[a,b] = [z^i,0]$, $\mathrm{lm}[c,d] = [2z^j,0]$, $\mathrm{lm}[g,h] = [0,z^r]$, $\mathrm{lm}[u,v] = [0,2z^s]$ satisfying $i \geq j$ and $r \geq s$. Moreover, the integers i,j,r,s are uniquely determined.

In [4, Sec. VI] an efficient algorithm to compute a Gröbner basis for a submodule M of the form $M = \{[a,b] \in R[z]^2 \mid a\,U \equiv b \mod z^r\}$, for some $U \in R[z]$ is given, the so-called method of Solution by Approximations. This algorithm generalizes one for the finite field case, derived in [7], which can be viewed as the Gröbner basis equivalent of the Berlekamp-Massey algorithm [3, Alg. 7.4]. The Solution by Approximations method works by computing iteratively a Gröbner basis of each successive solution module $M^{(k)} = \{[a,b] \in R[z]^2 \mid a\,U \equiv b \mod z^k\}$, finally arriving at a basis of $M = M^{(r)}$. The algorithm requires no searching at any stage of its implementation and has complexity quadratic in r.

In the next result we establish the minimality of $[\varphi,\omega]$ among the regular elements of the solution module of the key equation (9) with respect to the term order $<_{-1}$. The proof is omitted due to space constraints.

Theorem 2. *Let $M = \{[a,b] \in R[z]^2 \mid a(1+T) \equiv b \mod z^{t+1}\}$. Let $[a,b] \in M$ such that $\delta a \leq \frac{t+1}{2}$, $\delta b \leq \frac{t}{2}$, and $2 \in (a,b)$. Suppose further that $\mathrm{lc}(a) \in R^\times$ if $\delta a > \delta b$ and $\mathrm{lc}(b) \in R^\times$ if $\delta a \leq \delta b$.*

(a) Then $[a,b]$ is minimal in $M \setminus M \cap 2R[z]^2$ with respect to the term order $<_{-1}$. Moreover, if $[a',b']$ is minimal in $M \setminus M \cap 2R[z]^2$ then $[\mu a, \mu b] = \nu[\mu a', \mu b']$ for some $\nu \in K^\times$.

(b) If in addition $(a,b) = R[z]$ holds, then $[a,b]$ is minimal in $M \setminus \{0\}$ with respect to the term order $<_{-1}$, and if $[a',b']$ is minimal in $M \setminus M \cap 2R[z]^2$ then $[a,b] = \theta[a',b']$ for some $\theta \in R^\times$.

Corollary 3. *Let $M = \{[a,b] \in R[z]^2 \mid a(1+T) \equiv b \mod z^{t+1}\}$, and let $[a',b']$ be the minimal regular element of a Gröbner basis of M.*

(a) Then $[\mu\varphi, \mu\omega] = \nu[\mu a', \mu b']$ *for some* $\nu \in K^\times$.
(b) If e *contains no 'double-errors', then* $[\varphi, \omega] = \theta[a', b']$ *for some* $\theta \in R^\times$.

Proof. Let $w := w(e) = \delta\sigma \leq t$ be the number of errors occurred. If w is odd, then $\delta\varphi = \frac{w+1}{2}$ and $\delta\omega \leq \frac{w-1}{2}$, hence $\delta\varphi > \delta\omega$; and $\mathrm{lc}(\varphi) \in R^\times$. If w is even, then $\delta\omega = \frac{w}{2}$ and $\delta\varphi \leq \frac{w}{2}$, hence $\delta\varphi \leq \delta\omega$; and $\mathrm{lc}(\omega) \in R^\times$. By Corollary 2, we have $2 \in (\varphi, \omega)$. So we can apply Theorem 2 with Remark 2. □

We note that since $\omega(0) = \varphi(0) = 1$ we may choose $[a', b']$ such that $a'(0) = b'(0) = 1$, and then we have $[\mu\varphi, \mu\omega] = [\mu a', \mu b']$ and $[\varphi, \omega] = [a', b']$, respectively.

7 Decoding $\mathbb{Z}_4$-linear Negacyclic Codes

Let the $\mathbb{Z}_4$-linear negacyclic code C be given as in the previous sections, and let $v, c, e \in \mathbb{Z}_4[z]$, $\sigma, \sigma_o, \sigma_e, \varphi, \omega \in R[z]$ and $T \in R(z)$ be given as before. In particular, $v = c + e$ with $c \in C$ and the error vector e is of Lee weight at most t. Let $M = \{[a, b] \in R[z] \mid a\,(1 + T) \equiv b \mod z^{t+1}\}$ be the module of solutions to the key equation (9). We first compute a Gröbner basis of M relative to the term order $<_{-1}$, which contains an element $[a, b]$ such that $\mu a = \mu\varphi$ and $\mu b = \mu\omega$. Then $\mu\varphi, \mu\omega$ can be used to determine $\mu\sigma = \prod_{i=0}^{n-1}(1 - \mu X_i z)^{w(e_i)} \in K[z]$ via the equations

$$\mu\sigma = \mu\sigma_e + \mu\sigma_o\,,\ \mu\sigma_e(z) = \mu\omega(z^2)\,,\ \text{and}\ \ \mu\varphi(z^2) = \mu\sigma_e(z) + z\mu\sigma_o(z)\,.$$

Knowledge of $\mu\sigma$ is not sufficient to recover the error pattern e, as errors of the form $e_j = \pm 1$ cannot be distinguished. However, by examining the roots of $\mu\sigma$ we find all error positions, and by examining the double roots we get all locations j where $e_j = 2$ (i.e., the 'double-errors').

Let $e^2 \in \mathbb{Z}_4^n$ be defined by $e_j^2 = 2$ if $e_j = 2$ and $e_j^2 = 0$ otherwise. Note that e^2 is completely determined by the roots of $\mu\sigma$. Now consider the word $v' := v - e^2 = c + e'$ with $e' := e - e^2$. Then e' does not contain double-errors and has Lee weight at most t. Then, using Corollary 3, the error pattern e' can be found by computing the minimal regular element of a Gröbner basis.

We outline the steps of the algorithm below.

Algorithm 1 (Algebraic Decoding of $\mathbb{Z}_4$ Negacyclic Codes). *Let C be a negacyclic code over $\mathbb{Z}_4$ of length n, whose generator polynomial has roots α, α^3, …, α^{2t-1} for a primitive $2n$th root of unity $\alpha \in R$ such that $\alpha^n = -1$.*

Input: $v \in \mathbb{Z}_4[z]$ such that $d(v, C) \leq t$
Output: $c \in C$ such that $w(v - c) \leq t$

1. *Compute the syndromes $s_k := v(\alpha^k)$ for $k = 1, 3, \ldots, 2t-1$.*
2. *Compute the coefficients u_k using equation (6) for $k = 1, 3, \ldots, 2t-1$. Let $u := \sum_{k=1}^{2t-1} u_k z^k$.*
3. *Compute $T(z) \mod z^{t+1}$ from u using equation (7).*

4. *Obtain a solution* $[g, h] \in R[z]^2$ *of the key equation* $a(1+T) = b \mod z^{t+1}$ *satisfying the hypothesis of Theorem 2. One way to do this is to identify the minimal regular element of a Gröbner basis of the solution module* M*, relative to the term order* $<_{-1}$*.*
5. *Compute* $\mu\sigma(z) = \mu\sigma_e(z) + \mu\sigma_o(z) := \mu h(z^2) + z^{-1}(\mu g(z^2) - \mu h(z^2))$*.*
6. *Evaluate* $\mu\sigma(\mu\alpha^{-j})$ *for* $j = 0, \ldots, n-1$*.*
   - *If* $\mu\alpha^{-j}$ *is a double root of* $\mu\sigma$ *then* $e_j = 2$*.*
   - *If* $\mu\alpha^{-j}$ *is a single root of* $\mu\sigma$ *then* $e_j \in \{\pm 1\}$*.*
7. *Let* $e^2 := \sum_{j, e_j = 2} 2z^j$*, and let* $v' := v - e^2$*.*
8. *Repeat Steps 1.–4. with* v' *in place of* v*, and compute* $\sigma'(z) = \sigma'_e(z) + \sigma'_o(z) := h(z^2) + z^{-1}(g(z^2) - h(z^2))$*.*
9. *Compute* e' *by evaluating* $\sigma(\alpha^{-j})$ *and* $\sigma(\alpha^{-j+n})$ *for* $j = 0, \ldots, n-1$*.*
   - *If* α^{-j} *is a root of* σ *then* $e'_j = 1$*.*
   - *If* α^{-j+n} *is a root of* σ *then* $e'_j = 3$*.*
10. *Output* $c := v' - e'$*.*

We will conclude our work by a concrete example.

Example 1. Let $R = \mathrm{GR}(4, 4) = \mathbb{Z}_4[x]/\langle x^4 + 2x^2 + 3x + 1\rangle$ and let $\alpha = [x] \in R$. We use a code of length $n = 15$ with $t = 2$. Let the received word be $v = 2 + z + 3z^2 + 2z^4 + z^5 + 2z^6 + 3z^7 + z^8 + 3z^9 + z^{10} + 3z^{13}$.

1. The list of syndromes is $[3\alpha^3 + \alpha^2 + 3\alpha + 2,\ 2\alpha^3 + \alpha^2 + 2\alpha + 1]$.
3. The T polynomial of the key equation is $T(z) = (2\alpha^3 + \alpha^2 + \alpha)z^2 + (3\alpha^3 + \alpha^2 + 3\alpha + 2)z + 1$.
4. The solution of the key equation is $[(\alpha^3 + 2\alpha^2 + 3\alpha + 3)z + 3\alpha^3 + 3\alpha^2 + 2\alpha + 3,\ z + 3\alpha^3 + 3\alpha^2 + 2\alpha + 3)] \in R[z]^2$.
7. We find $e^2 = 0$.
9. Repeating the process with $v' = v$ we find $e' = z^4 - z^{13}$ and $c = v' - e'$.

References

1. Adams, W. W., Loustaunau, P.: An Introduction to Gröbner Bases. American Mathematical Society, Providence, RI (1994)
2. Berlekamp, E. R.: Negacyclic Codes for the Lee Metric. In: Combinatorial Mathematics and its Applications (Proc. Conf., Univ. North Carolina, Chapel Hill, NC, 1967), 298–316. Univ. North Carolina, Chapel Hill, NC (1969)
3. Berlekamp, E. R.: Algebraic Coding Theory. McGraw-Hill, New York (1968)
4. Byrne, E., Fitzpatrick, P.: Hamming Metric Decoding of Alternant Codes Over Galois Rings. IEEE Trans. Inform. Theory 48-3, 683–694 (2002)
5. Byrne, E., Greferath, M., Pernas, J., Zumbrägel, J.: Algebraic Decoding of Negacyclic Codes over $\mathbb{Z}_4$. Available online: http://arxiv.org/abs/1102.3604 (2011)
6. Byrne, E., Mora, T.: Gröbner Bases over Commutative Rings with Applications to Coding Theory. In: Sala, M. et al (eds.) Gröbner Bases, Coding, and Cryptography. RISC Series, Springer-Verlag, Berlin, 239–262 (2009)
7. Fitzpatrick, P.: On the Key Equation. IEEE Trans. Inform. Theory 41-5, 1290–1302 (1995)
8. Raghavendran, R.: Finite associative rings. Compositio Math. 21, 195–229 (1969)
9. Wolfmann, J.: Negacyclic and Cyclic Codes over $\mathbb{Z}_4^n$. IEEE Trans. Inform. Theory 45-7, 2527–2532 (1999)