HAL open science

Skew-cyclic codes

Delphine Boucher, Willi Geiselmann, Félix Ulmer

To cite this version:

Delphine Boucher, Willi Geiselmann, Félix Ulmer. Skew-cyclic codes. Applicable Algebra in Engineering, Communication and Computing, 2007, 18 (4), pp.379-389. 10.1007/s00200-007-0043-z . hal-00023483

HAL Id: hal-00023483

https://hal.science/hal-00023483v1

Submitted on 27 Apr 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.

ccsd-00023483, version 1 - 27 Apr 2006

Skew-cyclic codes

D. Boucher*, W. Geiselmann† and F. Ulmer ‡

April 17, 2006

Abstract

We generalize the notion of cyclic codes by using generator polynomials in (non commutative) skew polynomial rings. Since skew polynomial rings are left and right euclidean, the obtained codes share most properties of cyclic codes. Since there are much more skew-cyclic codes, this new class of codes allows to systematically search for codes with good properties. We give many examples of codes which improve the previously best known linear codes.

Introduction

Let $\mathbb{F}_q$ be a finite field of q elements. A linear (n,k)-code over $\mathbb{F}_q$ is a k-dimensional vector subspace $\mathcal{C}$ of the vector space

$$V = {\mathbb{F}_q}^n = \{(a_0, \ldots, a_{n-1}) \mid a_i \in \mathbb{F}_q\}.$$

In the following we use the polynomial representation of the code. In the polynomial representation of the code $\mathcal{C}$, the code words $(a_0, a_1, \ldots, a_{n-1}) \in \mathcal{C}$ are coefficient tuples of elements $a_{n-1}X^{n-1} + \ldots + a_1X + a_0 \in \mathbb{F}_q[X]/(X^n - 1)$ which are multiples of one element $G \in A$ (the generator polynomial). A linear code $\mathcal{C}$ is a cyclic code if

$$(a_0, a_1, \ldots, a_{n-1}) \in \mathcal{C} \quad \Rightarrow \quad (a_{n-1}, a_0, a_1, \ldots, a_{n-2}) \in \mathcal{C}.$$

*IRMAR, Université de Rennes 1, Campus de Beaulieu, F-35042 Rennes Cedex

†IAKS, Universität Karlsruhe, Fakultät für Informatik, Postfach 6980, D-76128 Karlsruhe

‡IRMAR, Université de Rennes 1, Campus de Beaulieu, F-35042 Rennes Cedex

In this paper we want to generalize the notion of cyclic codes to the notion of θ-cyclic codes.

Definition 1 *Let $\mathbb{F}_q$ be a finite field and θ an automorphism of $\mathbb{F}_q$. A θ-cyclic code is a linear code $\mathcal{C}_\theta$ with the property that*

$$(a_0, a_1, \ldots, a_{n-1}) \in \mathcal{C}_\theta \quad \Rightarrow \quad (\theta(a_{n-1}), \theta(a_0), \theta(a_1), \ldots, \theta(a_{n-2})) \in \mathcal{C}_\theta.$$

In order to generalize the notion of cyclic codes (corresponding to the case where θ is the identity) we consider skew polynomial rings of automorphism type which we now define. Starting from the finite field $\mathbb{F}_q$ and an automorphism θ of $\mathbb{F}_q$ one defines a ring structure on the set

$$\mathbb{F}_q[X, \theta] \;=\; \left\{ a_n X^{n-1} + \ldots + a_1 X + a_0 \,|\, a_i \in \mathbb{F}_q \text{ and } n \in \mathbb{N} \right\}.$$

This is the set of formal polynomials where the coefficients are written on the left of the variable X. The addition in $\mathbb{F}_q[X, \theta]$ is defined to be the usual addition of polynomials and the multiplication is defined by the basic rule $Xa = \theta(a)X$ ($a \in \mathbb{F}_q$) and extended to all elements of $\mathbb{F}_q[X, \theta]$ by associativity and distributivity. Those rings are well known (cf. [4, 1]) and, since over a finite field all derivations are inner, they are the most general "polynomial rings" with a commutative field of coefficients where the degree of a product of two elements is the sum of the degrees of the elements.

Our goal is to give a skew polynomial representation of θ-cyclic codes. We will show that the code words $(a_0, a_1, \ldots, a_{n-1})$ of a θ-cyclic code $\mathcal{C}_\theta$ are coefficient tuples of elements of $a_{n-1}X^{n-1} + \ldots + a_1 X + a_0 \in \mathbb{F}_q[X, \theta]/(X^n - 1)$ which are left multiples of one element $G \in \mathbb{F}_q[X, \theta]/(X^n - 1)$ (the generator polynomial). This property also guaranties that the encoding procedure of a θ-cyclic code is as easy as for cyclic codes.

We will also show by concrete examples that the class of θ-cyclic codes is a very large class of linear codes (containing the cyclic codes) and that this class contains codes with good properties. Therefore the class θ-cyclic codes is an interesting class of linear codes which are easy to construct in a systematic way. In a final section we will show how to decode some θ-cyclic codes.

1 Generalities on θ-cyclic codes

Properties of θ-cyclic codes are closely related to properties of $\mathbb{F}_q[X, \theta]$. The ring $\mathbb{F}_q[X, \theta]$ is a left and right euclidean ring whose left and right ideals are

principal [4]. Here right division means that for $P_1(X), P_2(X) \in \mathbb{F}_q[X,\theta]$ which are non zero, there exist unique polynomials $Q_r(X), R_r(X) \in \mathbb{F}_q[X,\theta]$ such that

$$P_1(X) = Q_r(X) \cdot P_2(X) \; + \; P_r(X).$$

If $P_r(X) = 0$ then $P_2(X)$ is a right divisor of $P_1(X)$ in $\mathbb{F}_q[X,\theta]$. The definition of left divisor in $\mathbb{F}_q[X,\theta]$ is similar using the left euclidean division. In the ring $\mathbb{F}_q[X,\theta]$ left and right gcd and lcm exist and can be computed using the left and right euclidean algorithm. We denote $\mathcal{F} \subset \mathbb{F}_q$ the subfield of elements of $\mathbb{F}_q$ that are left fixed by θ. An element $P \in \mathbb{F}_q[X,\theta]$ is central (i.e. commutes with all elements of $\mathbb{F}_q[X,\theta]$) if and only if $P = \sum_{i=0}^{m} c_i X^{i\cdot\alpha} \in \mathcal{F}[X]$ where $\alpha = | < \theta > |$ is the order of θ ([1], Theorem II.12). In particular central elements of $\mathbb{F}_q[X,\theta]$ are the generators of two-sided ideals in $\mathbb{F}_q[X,\theta]$. Therefore, if $| < \theta > |$ divides n, then $(X^n - 1) \subset \mathbb{F}_q[X,\theta]$ is a two-sided ideal. In the non-commutative ring $\mathbb{F}_q[X,\theta]/(X^n-1)$ we identify the image of $P \in \mathbb{F}_q[X,\theta]$ under the canonical morphism $\psi\colon \mathbb{F}_q[X,\theta] \to \mathbb{F}_q[X,\theta]/(X^n-1)$ with the remainder P_r of P by the right division with $X^n - 1$ in $\mathbb{F}_q[X,\theta]$ and we denote $\psi(X)$ still by X. This representation gives a canonical form for the elements of $\mathbb{F}_q[X,\theta]/(X^n-1)$.

Lemma 1 *Let $\mathbb{F}_q$ be a finite field, θ an automorphism of $\mathbb{F}_q$ and n an integer divisible by the order $| < \theta > |$ of θ. The ring $\mathbb{F}_q[X,\theta]/(X^n-1)$ is a principal left ideal domain in which left ideals are generated by $\psi(G)$ where G is a right divisor of $X^n - 1$ in $\mathbb{F}_q[X,\theta]$.*

Proof. The proof is an exact copy of the commutative case only taking care of left and right. Let I be a left ideal of $\mathbb{F}_q[X,\theta]/(X^n-1)$. If $I = \{0\}$ then $I = (0)$. Otherwise denote $G_r \in I$ a monic non zero polynomial of minimal degree in I. By abuse of notation we identify the element $G_r \in I$ with itself in $\mathbb{F}_q[X,\theta]$ and denote this element G (i.e. $G \in \mathbb{F}_q[X,\theta]$ is of degree $< n$ and $\psi(G) = G_r$). Let $P_r \in I$ be an arbitrary element of I which we again identify with $P \in \mathbb{F}_q[X,\theta]$. Performing a right division of P by G in $\mathbb{F}_q[X,\theta]$ we get

$$P \; = \; Q \cdot G \; + R, \qquad \text{where } \deg(R) < \deg(G)$$

from which we get $\psi(R) = P_r - \psi(Q) \cdot G_r \in I$. By minimality of the degree of G_r we must have $\psi(R) = 0$, showing that $P_r = \psi(Q) \cdot G_r$ and thus $I = (G_r)$. ∎

For a linear code $\mathcal{C}$ of length n we denote $\mathcal{C}(X)$ the skew polynomial representation of $\mathcal{C}$. In this representation we associate to a code word $a =$

$(a_0, a_1, \ldots, a_{n-1}) \in \mathcal{C}$ the element $a(X) = a_{n-1}X^{n-1} + \ldots + a_1 X + a_0$ in $\mathbb{F}_q[X, \theta]/(X^n - 1)$. If $a \in \mathcal{C}$, then we denote $a(X) \in \mathbb{F}_q[X, \theta]/(X^n - 1)$ the skew polynomial representation of a.

Theorem 1 *Let $\mathbb{F}_q$ be a finite field, θ an automorphism of $\mathbb{F}_q$ and $\mathcal{C}$ be a linear code over $\mathbb{F}_q$ of length n. If $| < \theta > |$, the order of θ, divides n, then the code $\mathcal{C}$ is a θ-cyclic code if and only if the skew polynomial representation $\mathcal{C}(X)$ of $\mathcal{C}$ is a left ideal $(G) \subset \mathbb{F}_q[X, \theta]/(X^n - 1)$.*

Proof. By the above Lemma we have to show that $\mathcal{C}(X)$ is a left ideal of $\mathbb{F}_q[X, \theta]/(X^n - 1)$. Since $\mathcal{C}$ is a linear code, $\mathcal{C}(X)$ is an additive group. Let $a = (a_0, \ldots, a_{n-1}) \in \mathcal{C}$, then

$$\begin{aligned} X\, a(X) &= X\, a_0 + X\,(a_1\, X) + \cdots + X\,(a_{n-1}\, X^{n-1}) \\ &= \theta(a_0)\, X + (\theta(a_1)\, X)\, X + \cdots + (\theta(a_{n-1})\, X)\, X^{n-1} \\ &= \theta(a_{n-1}) + \theta(a_0)\, X + \cdots \theta(a_{n-2})\, X^{n-1} + \theta(a_{n-1})\,(X^n - 1). \end{aligned}$$

Therefore in $\mathbb{F}_q[X, \theta]/(X^n - 1)$ (i.e. working modulo $X^n - 1$) we have $X\, a(X) = \theta(a_{n-1}) + \theta(a_0)\, X + \cdots \theta(a_{n-2})\, X^{n-1}$. Since $\mathcal{C}$ is θ-cyclic we have $X\, a(X) \in \mathcal{C}(X)$ and by iteration and linearity we get for all $P_r \in \mathbb{F}_q[X, \theta]/(X^n - 1)$ that $P_r \cdot a(X) \in \mathcal{C}(X)$. This shows that $\mathcal{C}(X)$ is a left ideal of $\mathbb{F}_q[X, \theta]/(X^n - 1)$. In the opposite direction the properties of a left ideal show that the coefficient vectors of the elements of a left ideal $(G) \subset \mathbb{F}_q[X, \theta]/(X^n - 1)$ form a linear subspace and from $a(X) \in (G) \Rightarrow X\, a(X) \in (G)$ we get from the above computation that the corresponding linear code is θ-cyclic. ∎

2 Finding good codes

An obvious technique for finding good linear codes (codes with a large minimum distance d) is a random search. With this technique, the probability to find a code with better parameters than the best known codes, e.g. according to Brouwer's table [3] (http://www.win.tue.nl/ aeb/), is very small. Many of the best known codes have some additional structure (e.g. are cyclic codes or are constructed using cyclic codes). Therefore a search within the θ-cyclic codes seems more promising than a random search — especially as, since $\mathbb{F}_q[X, \theta]$ is not a unique factorization ring, there are many θ-cyclic codes for a given set of parameters (n, k).

We implemented a factorization procedure in the CA-System MAGMA[2]. This procedure outputs all right skew-factors of $X^n - 1$, producing the possible generator skew polynomials for θ-cyclic codes. A right factor of degree $n - k$ of $X^n - 1$ generates a linear code with parameters (n, k). If θ is not the identity (corresponding to the cyclic codes), then $\mathbb{F}_q[X, \theta]$ is in general not a unique factorization ring. In this case there are typically much more right factors than in the commutative case, producing many θ-cyclic codes. Once the code is given, its minimum distance can be calculated using the existing MAGMA procedures. This latter operation is very time consuming for larger codes, hence we restricted our search to smaller codes with ground fields $\mathbb{F}_4$) and $\mathbb{F}_9$ and to 5000 codes in the cases, where more skew factors for a given parameter set (n, k) have been found. With this technique we obtained a minimum distance one larger than the previously known best code (according to Brouwer's table) for 8 parameter sets over $\mathbb{F}_4$. Those codes have been added to the MAGMA list of known codes. In most cases we found many different codes with the same minimum distance; in Table 1 the code parameters, the number of codes found with these parameters (No), and a generating polynomial for one code in this class of parameters are given.

For codes over $\mathbb{F}_9$ we managed to improve the lower bound for the best known codes in one case (cf. Table 2). Due to the larger ground field and the larger codes, the calculation of d_{min} is even more time consuming than in the previous case. Therefore we stopped our search for good codes at $n = 44$.

(n,k,d_{min})	No	g
$(56,30,14)$	1	$x^{26}+x^{23}+\alpha\,x^{22}+\alpha^2\,x^{21}+\alpha\,x^{20}+\alpha^2\,x^{19}+\alpha^2\,x^{18}+\alpha\,x^{17}+x^{16}+x^{14}+x^{13}+\alpha\,x^{11}+\alpha^2\,x^{10}+\alpha^2\,x^9+\alpha^2\,x^8+\alpha\,x^7+\alpha^2\,x^6+\alpha\,x^5+\alpha^2\,x^4+x^2+\alpha^2\,x+\alpha^2$
$(48,19,17)$	2	$x^{29}+\alpha^2\,x^{28}+x^{26}+\alpha\,x^{25}+\alpha^2\,x^{24}+\alpha\,x^{23}+\alpha\,x^{21}+\alpha\,x^{20}+\alpha^2\,x^{19}+\alpha\,x^{18}+\alpha\,x^{17}+\alpha\,x^{16}+x^{15}+x^{14}+\alpha\,x^{13}+\alpha\,x^{10}+\alpha\,x^8+\alpha^2\,x^7+x^6+x^5+x^4+\alpha^2\,x^3+x^2+\alpha^2$
$(48,25,13)$	2	$x^{23}+\alpha^2\,x^{22}+x^{21}+\alpha\,x^{20}+\alpha\,x^{19}+\alpha^2\,x^{18}+\alpha\,x^{17}+\alpha\,x^{14}+\alpha^2\,x^{13}+\alpha^2\,x^{11}+x^9+\alpha\,x^7+x^6+x^3+\alpha^2\,x^2+1$
$(42,17,16)$	3	$x^{25}+x^{23}+\alpha\,x^{22}+x^{21}+x^{20}+x^{19}+x^{18}+\alpha^2\,x^{17}+\alpha^2\,x^{16}+\alpha\,x^{15}+\alpha\,x^{14}+x^{13}+x^{11}+x^{10}+x^8+\alpha^2\,x^4+\alpha^2\,x^3+x^2+\alpha\,x+1$
$(42,23,11)$	92	$x^{19}+x^{17}+\alpha^2\,x^{16}+\alpha\,x^{15}+\alpha^2\,x^{14}+\alpha\,x^{13}+\alpha\,x^{11}+\alpha^2\,x^{10}+\alpha\,x^9+x^7+\alpha\,x^6+\alpha^2\,x^5+\alpha\,x^4+\alpha\,x+\alpha^2$
$(40,16,15)$	6	$x^{24}+\alpha\,x^{23}+x^{22}+x^{21}+\alpha^2\,x^{20}+\alpha\,x^{19}+\alpha\,x^{18}+\alpha\,x^{17}+x^{15}+x^{14}+x^{13}+\alpha\,x^{11}+\alpha^2\,x^{10}+x^9+x^8+x^7+\alpha^2\,x^6+\alpha\,x^5+\alpha^2\,x^4+\alpha\,x^2+\alpha^2$
$(36,20,10)$	13	$x^{16}+\alpha^2\,x^{15}+x^{13}+\alpha^2\,x^{12}+x^{11}+\alpha\,x^{10}+x^9+\alpha^2\,x^8+\alpha\,x^7+\alpha\,x^6+\alpha\,x^4+\alpha^2\,x^3+\alpha^2\,x^2+1$
$(30,16,9)$	422	$x^{14}+x^{13}+\alpha\,x^{11}+x^{10}+x^9+x^8+\alpha\,x^7+x^6+\alpha\,x^5+\alpha^2\,x^4+\alpha^2\,x^2+\alpha\,x+\alpha^2$

Table 1: Parameters and generating polynomial of skew-cyclic codes over $\mathbb{F}_4$. Here α a zero of y^2+y+1 and θ the Frobenius automorphism. For each code the minimum distance has been improved by 1 according to Brouwer's table

(n,k,d_{min})	No	g
$(44,20,17)$	5	$x^{24}+x^{21}+x^{20}+\alpha^7\,x^{19}+\alpha^3\,x^{18}+2\,x^{17}+\alpha^3\,x^{16}+\alpha^5\,x^{14}+\alpha^5\,x^{13}+2\,x^{12}+\alpha^2\,x^{10}+\alpha^7\,x^9+2\,x^6+\alpha^5\,x^5+\alpha^7\,x^4+\alpha^3\,x^3+\alpha^7\,x^2+\alpha^2\,x+2$

Table 2: Parameters and generating polynomial of skew-cyclic codes over $\mathbb{F}_9$. Here α a zero of y^2-y-1 and θ the Frobenius automorphism. The minimum distance has been improved by 1 according to the best known codes.

3 Decoding

In the following, instead of a general decoding procedure, we will adapt (to *skew BCH codes*) the algorithm for decoding BCH codes with designed distance (see [5] pages $27-33$ or [6]) to θ-cyclic codes. We denote $\alpha \in \mathbb{F}_q$ a primitive $(q-1)$-th root of unity. We suppose that n is even, $q = 2^m$ where $m = n$ and that $\theta(\alpha) = \alpha^2$. Consider a θ-cyclic code $\mathcal{C}$ whose generating polynomial is $G \in \mathbb{F}_q[X, \theta]$ which is a right divisor of $X^n - 1$ in $\mathbb{F}_q[X, \theta]$. We suppose that $\mathcal{C}$ is a skew BCH codes of designed distance $d \in \mathbb{N}$, which in this context just means that $X - \alpha^k$ is a right factor of G for $k \in \{1, \ldots, d-1\}$. In the following section we give an example of a skew BCH codes which is not even cyclic in the classical sense, showing that this class extends the class of BCH codes. The following result allows us to switch to commutative rings for some considerations :

Property 1 *For* $P = \sum_{k=0}^{n-1} a_k\, X^k \in \mathbb{F}_q[X, \theta]$, $\beta \in \mathbb{F}_q$ *and* $r \in \mathbb{F}_q$ *the remainder of the right division of* P *by* $X - \beta$, *then* $r = \tilde{P}(\beta)$ *where* $\tilde{P}$ *is a (classical) polynomial given by* $\tilde{P} = \sum_{k=0}^{n-1} a_k\, z^{2^k-1} \in \mathbb{F}_q[z]$

Proof. The remainder of the right division of $P(X)$ by $X - \beta$ is

$$r = a_0 + a_1\,\beta + a_2\,\beta\,\theta(\beta) + a_3\,\beta\,\theta(\beta)\,\theta^2(\beta) + \cdots + a_{n-1}\,\beta\,\cdots\theta^{n-2}(\beta)$$

Replacing $\theta^k(\beta)$ with β^{2^k}, we get $r = \sum_{k=0}^{n-1} a_k\,\beta^{2^k-1} = \tilde{P}(\beta)$ ∎

Therefore the remainder of the right division of $P \in \mathbb{F}_q[X, \theta]$ by $X - \beta$ (and the image of the remainder in $\mathbb{F}_q[X, \theta]/(X^n - 1)$) can be interpreted as the evaluation of the polynomial $\tilde{P}$ in the *commutative ring* $\mathbb{F}_q[z]$ at $\beta \in \mathbb{F}_q$. Using this property, we can prove like in the classical case ([6], Theorem 6.2) that the distance of the code is at least equal to the designed distance d.

Property 2 *Let* n *even,* $q = 2^n$, α *a primitive* $(q-1)$*-th root of unity. Let* $\mathcal{C}$ *be a* θ*-cyclic code with* $\theta(\alpha) = \alpha^2$. *Let* $G \in \mathbb{F}_q[X, \theta]$ *be its generating polynomial such that* G *is a right divisor of* $X^n - 1$ *in* $\mathbb{F}_q[X, \theta]$ *and* $X - \alpha^k$ *is a right factor of* G *for* $k \in \{1, \ldots, d-1\}$.
The distance of the code $\mathcal{C}$ *is equal to its designed distance* d.

Proof. According to property (1), a test matrix for the code is

$$H = \begin{pmatrix} H_1 \\ H_2 \end{pmatrix}$$

where

$$H_1 = \begin{pmatrix} \alpha_0 & \alpha_1 & \cdots & \alpha_{d-1} & \cdots & \alpha_{n-1} \\ \alpha_0^2 & \alpha_1^2 & \cdots & \alpha_{d-1}^2 & \cdots & \alpha_{n-1}^2 \\ \vdots & & & & & \vdots \\ \alpha_0^{d-1} & & \cdots & & & \alpha_{n-1}^{d-1} \end{pmatrix}$$

and $\alpha_i = \alpha^{2^i-1}$. If we consider all the possible sets of $d-1$ columns extracted from the n columns of H_1, we get square matrices of order $d-1$. Their determinants are non zero if and only if $\alpha_i - \alpha_j$ is non zero for $j < i < n$. But $\alpha_i - \alpha_j = 0 \Leftrightarrow \alpha^{2^i-2^j} = 1$ and $0 < 2^i - 2^j < 2^n - 1$, so as $2^n - 1$ is the order of α, we get non zero determinants. So each set of $d-1$ columns of H_1 are linearly independant, one cannot find any word of weight less than d and the minimum distance of the code is at least d. ∎

We can now adapt *almost* entirely the classical decoding algorithm for BCH codes which in described in [5] pages $27-33$.
Let $a \in \mathbb{F}_q[X,\theta]/(X^n-1)$ be a code word and let $b = a+e \in \mathbb{F}_q[X,\theta]/(X^n-1)$ be the received word where $e = e_{i_1} X^{i_1} + \cdots + e_{i_r} X^{i_r}$ is the error polynomial with $i_1 < i_2 < \cdots < i_r$ and where $r \leq t := \frac{d-1}{2}$.
One defines the *syndrome polynomial* of e as the polynomial

$$S_d(z) = \sum_{k=1}^{d-1} \mathrm{Rem}(e, X - \alpha^k) z^{k-1} \in \mathbb{F}_q[z].$$

Here the remainder $\mathrm{Rem}(e, X - \alpha^k)$ is to be computed in $\mathbb{F}_q[X,\theta]$. As $\mathrm{Rem}(e, X - \alpha^k) = \mathrm{Rem}(b, X - \alpha^k)$, one can compute $S_d(z)$ using the received polynomial b. The syndrome polynomial can also be written

$$S_d(z) = \sum_{k=1}^{d-1} \tilde{e}(\alpha^k)\, z^{k-1}$$

where $\tilde{e}(z) = \displaystyle\sum_{k=1}^{r} e_{i_k}\, z^{j_k} \in \mathbb{F}_q[z]$ and $j_k = 2^{i_k} - 1$.
One also defines the *pseudo-locator polynomial*

$$\sigma(z) = \prod_{k=1}^{r} (1 - \alpha^{j_k}\, z)$$

and the *evaluator polynomial*

$$w(z) = \sum_{l=1}^{r} e_{i_l}\, \alpha^{j_l} \prod_{k \neq l} (1 - \alpha^{j_k}\, z).$$

Knowing $\sigma(z)$ enables us to find the j_k, so that we have *almost* located the positions i_k of the errors in e. This point is in fact the only difference with the classical algorithm.

Once we know the j_k and the evaluator polynomial $w(z)$, we can recover all the e_{i_k} using the following equality

$$e_{i_k} = \alpha^{-j_k}\, w(\alpha^{-j_k}) \prod_{l \neq k} (1 - \alpha^{j_l - j_k}),\ k \in \{1, \ldots, r\}.$$

Let us now define

$$S(z) = \sum_{k=1}^{\infty} \tilde{e}(\alpha^k)\, z^{k-1} = S_d(z) + z^{d-1} \sum_{k=0}^{\infty} \tilde{e}(\alpha^{k+1+d})\, z^k$$

Like in [5] (theorem $I.8$ page 28), one gets the classical 'key equation':

$$\sigma(z)\, S(z) = w(z)$$

which one can write

$$\sigma(z)\, S_d(z) + v(z)\, z^{d-1} = w(z)$$

where $v(z) = \sigma(z) \sum_{k=0}^{\infty} \tilde{e}(\alpha^{k+1+d})\, z^k$.

Following [5] (theorem $I.11$ page 32) we apply Euclid's algorithm to the polynomials $S_d(z)$ and z^{d-1} in $\mathbb{F}_q[z]$. We construct the sequences $(r_i(z))$, $(U_i(z))$ and $(V_i(z))$ defined by

$$r_{-1}(z) = z^{d-1},\ r_0(z) = S_d(z)$$

$$U_{-1}(z) = 0, U_0(z) = 1, V_{-1}(z) = 1, V_0(z) = 0$$

and at each step i,

$$r_i(z) = r_{i-2}(z) - q_i(z)\, r_{i-1}(z) \text{ with } \deg(r_i(z)) < \deg(r_{i-1}(z))$$

$$U_i(z) = U_{i-2}(z) - q_i(z)\, U_{i-1}(z), V_i(z) = V_{i-2}(z) - q_i(z)\, V_{i-1}(z).$$

and we stop as soon as we find k such that $\deg(r_{k-1}) \geq t$ and $\deg(r_k) < t$. We get

$$U_k(z)\, S_d(z) + V_k(z)\, z^{d-1} = r_k(z),$$

$$\sigma(z) = \frac{U_k(z)}{U_k(0)}$$

and

$$w(z) = \frac{r_k(z)}{r_k(0)}$$

Now from the roots of the pseudo-locator polynomial $\sigma(z)$ we get j_l, $l \in \{1, \ldots, r\}$ and from the evaluator polynomial $w(z)$ we get

$$e_{i_l} = \alpha^{-j_l}\, w(\alpha^{-j_l}) \prod_{k \neq l} (1 - \alpha^{j_k - j_l}),\ l \in \{1, \ldots, r\}.$$

So we have found the coefficients of e and we have almost found the positions i_l of the errors. For each j_l, we get a finite number of possibilities i_l solutions to the equation

$$j_l \equiv 2^{i_l} - 1 \pmod{n}$$

So we get a finite number of possible errors, which we test until we find e such that $b + e$ is a code word. As the distance of the code is d we are sure that such a e is unique and so we have decoded.

4 Worked example

Let $n = m = 10$ and let α such that $\alpha^{2^{10}-1} = 1$. The polynomial

$$G = X^6 + \alpha^{345}\, X^5 + \alpha^{643}\, X^4 + \alpha^{878}\, X^3 + \alpha^{670}\, X^2 + \alpha^{1020}\, X + \alpha^{777}$$

divides $X^{10} + 1$ to the right in $\mathbb{F}_{2^{10}}[X, \theta]$. Therefore it is the generator polynomial of a θ-cyclic code $\mathcal{C}$ of length 10 over $\mathbb{F}_{2^{10}}$. Since $X - \alpha^k$ is a right factor of G for $k \in \{1, \ldots, 6\}$, the code $\mathcal{C}$ is of designed distance $d = 7$. One can check that this skew BCH code is not cyclic in the classical sense.

We consider the code word a given by

$$a(X) = \alpha^{654}\, X^9 + \alpha^{547}\, X^8 + \alpha^{650}\, X^7 + \alpha^{16}\, X^6 + \alpha^{567}\, X^5 + \alpha^{29}\, X^4 + \alpha^{87}\, X^3 + \alpha^{696}\, X^2 + \alpha^{252}\, X + \alpha^{555},$$

an error

$$e = \alpha^{341}\, X^9 + \alpha^{682}\, X^8 + \alpha^{682}.$$

The received perturbed code word $b = a + e$ is

$$b = \alpha^{818} X^9 + \alpha^{775} X^8 + \alpha^{650} X^7 + \alpha^{16} X^6 + \alpha^{567} X^5 + \alpha^{29} X^4 + \alpha^{87} X^3 + \alpha^{696} X^2 + \alpha^{252} X + \alpha^{557}.$$

Knowing the received polynomial b and $d = 7$, we can compute the syndrome polynomial

$$S_7(z) = \alpha^{404}\, z^5 + \alpha^{403}\, z^4 + \alpha^{601}\, z^3 + \alpha^{645}\, z^2 + \alpha^{614}\, z + \alpha^{406}$$

Applying Euclid algorithm to $S_7(z)$ and z^6 in $\mathbb{F}_{2^{10}}[z]$ with $t = 3$, we get the *pseudo-locator polynomial* $\sigma(z)$

$$\sigma(z) = \alpha^{766}\, z^3 + \alpha^{642}\, z^2 + \alpha^{241}\, z + 1$$

and the *evaluator polynomial* $w(z)$

$$w(z) = \alpha^{84}\, z^2 + \alpha^{185}\, z + \alpha^{406}.$$

From the roots $1, \alpha^{512}$ and α^{768} of the polynomial $\sigma(z)$ we get the value of r ($r = 3$) and the values of j_1, j_2, j_3 :

$$j_1 = 0, j_2 = 511, j_3 = 255.$$

We can now find the values of the coefficients of e via the polynomial w :

$$e_{i_1} = \alpha^{682}, e_{i_2} = \alpha^{341}, e_{i_3} = \alpha^{682}.$$

We have now to locate exactly the positions of the errors. For each k in $\{1, 2, 3\}$, we solve the equations

$$2^{i_k} - 1 \equiv j_k \pmod{10}.$$

$$\begin{array}{lll} 2^{i_1} - 1 \equiv 0 \pmod{10} & \Leftrightarrow & i_1 \pmod{10} = 0 \\ 2^{i_2} - 1 \equiv 511 \pmod{10} & \Leftrightarrow & i_2 \pmod{10} \in \{1, 5, 9\} \\ 2^{i_3} - 1 \equiv 255 \pmod{10} & \Leftrightarrow & i_3 \pmod{10} \in \{4, 8\} \end{array}$$

So the list of the possible errors is

$$\begin{array}{ll}[\alpha^{682}\,X^4+\alpha^{341}\,X+\alpha^{682}, & \alpha^{682}\,X^8+\alpha^{341}\,X+\alpha^{682},\\ \alpha^{341}\,X^5+\alpha^{682}\,X^4+\alpha^{682}, & \alpha^{682}\,X^8+\alpha^{341}\,X^5+\alpha^{682},\\ \alpha^{341}\,X^9+\alpha^{682}\,X^4+\alpha^{682}, & \alpha^{341}\,X^9+\alpha^{682}\,X^8+\alpha^{682}]\end{array}$$

The only one such that g divides $b+e$ to the right is

$$e=\alpha^{341}\,X^9+\alpha^{682}\,X^8+\alpha^{682}.$$

For this code, 5000 random tests have been made (each random test takes a random code word, a random error of weight at most three and checks whether the corrected word is equal to the code word).

References

[1] Bernard R. McDonald, *Finite Rings with Identity.*, Marcel Dekker Inc. (1974).

[2] Wieb Bosma, John Cannon and Catherine Playoust (1997). The Magma Algebra System I: The User Language. *Journal of Symbolic Computation,* **24**, pp. 235–265.

[3] Andries E. Brouwer (2005). Server for bounds on the minimum distance of q-ary linear codes, $q=2,3,4,5,7,8,9$. `http://www.win.tue.nl/~aeb/`

[4] Ore, O. (1933). Theory of non-commutative polynomials. *Ann. of Math.* **34**.

[5] Nicolas Sendrier, *Codes Correcteurs d'Erreurs à Haut Pouvoir de Correction.* Thèse de doctorat, spécialité informatique. Université Paris 6, décembre 1991.

[6] S.A. Vanstone and P.C. van Oorschot, *An Introduction to error correcting codes with applications*, Kluwer Academic Publishers (1989).