On Quasi-Cyclic Codes as a Generalization of Cyclic Codes

M. Barbier
École Polytechnique - LIX
INRIA Saclay - Île de France

C. Chabot
LJK-CASYS
University of Grenoble

G. Quintin
École Polytechnique - LIX
INRIA Saclay - Île de France

August 18, 2011

Abstract

In this article we see quasi-cyclic codes as block cyclic codes. We generalize some properties of cyclic codes to quasi-cyclic ones such as generator polynomials and ideals. Indeed we show a one-to-one correspondence between ℓ-quasi-cyclic codes of length ℓm and ideals of $M_\ell(\mathbb{F}_q)[X]/(X^m - 1)$. This permits to construct new classes of codes, namely quasi-BCH and quasi-evaluation codes. We study the parameters of such codes and propose a decoding algorithm up to half the designed minimum distance. We even found one new quasi-cyclic code with better parameters than known $[189, 11, 125]_{\mathbb{F}_4}$ and 48 derivated codes beating the known bounds as well.

1 Introduction

1.1 Context

We noticed that many of the codes with the best known minimum distance are quasi-cyclic codes or derivated from them [12, 7]. From this point of view, this family of codes is very interesting. Moreover, quasi-cyclic codes were studied for their application in McEliece cryptosystem [13, 2] – or equivalently in Niederreiter's [14, 10]. Indeed they allow an interesting key reduction compared to Goppa codes. However, since the decoding of random quasi-cyclic codes is difficult, only quasi-cyclic alternant codes are proposed for this cryptosystem. The high structure of alternant codes is actually a weakness and a cryptanalysis was proposed in [5]. For these reasons, studying the decoding methods and the general behaviour of quasi-cyclic codes remain interesting topics.

The structure of quasi-cyclic codes has been studied in different ways. In [6], they are seen as concatenation of cyclic codes while in [11] they regard them as linear codes over an auxiliary ring. In [3], their approach is more analogous to the cyclic case. Indeed they consider factorisations of $X^m - 1$ in $M_\ell(\mathbb{F}_q)[X]$ – with reversible polynomials – in order to construct ℓ-quasi-cyclic codes cancelled by those polynomials, called $\Omega(P)$-codes. This leads to the construction of self-dual codes and codes beating the known bounds. However the factorisation in this ring remains difficult. In [4] the author gives an improved method in particular cases for the factorisation of $X^m - 1$.

In this article, we prove, analogously to cyclic case, an one-to-one correspondence between ℓ-quasi-cyclic codes of length ℓm and principal ideals of the ring
$M_\ell(\mathbb{F}_q)[X]/(X^m - 1)$. Additionally, we prove that all its ideals are principal. Moreover, from the BCH and evaluation codes definitions, we propose two new classes of quasi-cyclic codes, namely *quasi-BCH* and *quasi-evaluation* codes. We propose also a new natural notion of *folded* and *unfolded* codes, which permits to decode and list decode polynomially – in the length of the code – some of these new codes. For the quasi-BCH codes which are not decodable thanks to the folding notion, we propose an unambiguous decoding algorithm based on a key equation. Finally, from the quasi-evaluation code definition, we exhibit a quasi-cyclic code whose parameters are better than the previous known and 48 other codes derivated from the first one have also better parameters than known.

The subsection 1.2 is devoted to some recalls about $\Omega(P)$-codes and definitions. Then in section 2 we prove the correspondence between principal ideals and quasi-cyclic codes. The section 3 deals with the definition, paramaters and the decoding algorithm of quasi-BCH codes. Finally, the section 4 introduces the quasi-evaluation codes and gives lower bounds on its parameters.

1.2 Quasi-cyclic codes seen as block cyclic codes

1.2.1 First definitions

Frow now on, we consider ℓ-quasi-cyclic codes as codes stable by T^ℓ with $n = m\ell$ and T is the circular shift defined by:

$$\forall c \triangleq (c_1, c_2, \ldots, c_n) \in \mathbb{F}_q^n,\ T(c) \triangleq (c_2, c_3, \ldots, c_1).$$

In [3] they consider an action of polynomials with matricial coefficients on vectors of $(\mathbb{F}_q^m)^\ell \sim \mathbb{F}_q^{m\ell}$ in the following way:

$$\begin{array}{ccc} M_\ell(\mathbb{F}_q)[X] \times (\mathbb{F}_q^m)^\ell & \longrightarrow & (\mathbb{F}_q^m)^\ell \sim \mathbb{F}_q^{m\ell} \\ \left(\displaystyle\sum_{i=0}^{\deg(P)} P_i X^i, c\right) & \longmapsto & P * c \triangleq \displaystyle\sum_{i=0}^{\deg(P)} P_i.(T^\ell)^i(c). \end{array}$$

Thanks to this action, we can define $\Omega(P)$-codes by

Definition 1.1 ($\Omega(P)$-code)**.** *Let $P \in M_\ell(\mathbb{F}_q)[X]$ be a reversible polynomial such that $P(X)$ divides $X^m - 1$ then $\Omega(P) \triangleq \{c \in (\mathbb{F}_q^m)^\ell \ : \ P * c = 0\}$ is a ℓ-quasi-cyclic code.*

Further information may be found in [3] and [4]. However all the quasi-cyclic codes cannot be obtained this way. The general case will be detailed in this paper.

1.3 Folded and unfolded codes

Since we see quasi-cyclic codes as a generalization of cyclic codes, we define two maps allowing a link between the two notions.

Let ℓ be an integer, then there exist an irreducible polynomial $P(X) \in \mathbb{F}_q[X]$ with degree ℓ and $\alpha \in \mathbb{F}_{q^\ell}$ a root of P such that

$$\mathbb{F}_{q^l} = \mathbb{F}_q[\alpha] \simeq \mathbb{F}_q[X]/(P(X)).$$

We define the folding of $a \in \mathbb{F}_{q^l}$ by

$$\begin{array}{rcccl} \phi : \mathbb{F}_q^\ell & \longrightarrow & \mathbb{F}_q[X]/(P(X)) & \longrightarrow & \mathbb{F}_q[\alpha] \\ (a_1, a_2, \dots, a_\ell) & \longmapsto & a_1 + a_2 X + \cdots + a_\ell X^{\ell-1} & \longmapsto & a_1 + a_2\alpha + \cdots + a_\ell \alpha^{\ell-1} = a. \end{array}$$

And the unfolding is the inverse

$$\begin{array}{rcccl} \phi^{-1} : \mathbb{F}_q[\alpha] & \longrightarrow & \mathbb{F}_q[X]/(P(X)) & \longrightarrow & \mathbb{F}_q^\ell \\ a = a_1 + a_2\alpha + \cdots + a_\ell \alpha^{\ell-1} & \longmapsto & a_1 + a_2 X + \cdots + a_\ell X^{\ell-1} & \longmapsto & (a_1, a_2, \dots, a_\ell). \end{array}$$

Note that these maps are $\mathbb{F}_q$-linear. We propose also to extend these definitions to codes.

Definition 1.2 (Folded code)**.** *Let $\mathcal{C}$ be a $\mathbb{F}_q$-code in $(\mathbb{F}_q^\ell)^m$. We defined the* folded code *of $\mathcal{C}$ by*

$$\phi(\mathcal{C}) \triangleq \{(\phi(c_1), \dots, \phi(c_m)) \ : \ c = (c_1, \dots, c_m) \in \mathcal{C}\}.$$

Definition 1.3 (Unfolded code)**.** *Let $\mathcal{C}$ be a $\mathbb{F}_q$-code in $(\mathbb{F}_{q^\ell})^m$. We defined the* unfolded code *of $\mathcal{C}$ by*

$$\phi^{-1}(\mathcal{C}) \triangleq \left\{\left(\phi^{-1}(c_1), \dots, \phi^{-1}(c_m)\right) \ : \ c = (c_1, \dots, c_m) \in \mathcal{C}\right\}.$$

Lemma 1.1. *Let $\mathcal{C}$ be a ℓ-quasi-cyclic code over $\mathbb{F}_q$ of dimension k. Then there exists an integer r such that $1 \le r \le k$ and for any generator matrix G of $\mathcal{C}$ and $0 \le i \le m-1$, the rank of the $i\ell+1, i\ell+2, \dots, (i+1)\ell$ colomns of G is r.*

Proof. Let $\mathrm{pr}_{i,j}$ the projection of the $i, i+1, \dots, j$ coordinates:

$$\begin{array}{rcl} \mathrm{pr}_{i,j} : \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^{j-i+1} \\ (x_1, \dots, x_n) & \longmapsto & (x_i, x_{i+1}, \dots, x_{j-1}, x_j). \end{array}$$

Let $r = \dim \mathrm{pr}_{1,\ell}(\mathcal{C})$ and G be a generator matrix of $\mathcal{C}$. Then G has no zero column so $r \geq 1$. The rows of G, denoted by $g_1, \ldots, g_k$ form a basis of $\mathcal{C}$ thus $r \leq \dim \mathcal{C} = k$. Moreover we have

$$\begin{aligned} r &= \dim \mathrm{pr}_{1,\ell}(\mathcal{C}) \\ &= \dim \langle \mathrm{pr}_{1,\ell}(g_1), \ldots, \mathrm{pr}_{1,\ell}(g_k) \rangle \\ &= \text{rank of the matrix formed by the first } \ell \text{ columns of } G. \end{aligned}$$

Now let $0 \leq i \leq m-1$. As $T^\ell \in \mathrm{Aut}(\mathcal{C})$ we have

$$\begin{aligned} r &= \dim \mathrm{pr}_{1,\ell}(\mathcal{C}) \\ &= \dim \langle \mathrm{pr}_{1,\ell}\, T^{-i\ell}(g_1), \ldots, \mathrm{pr}_{1,\ell}\, T^{-i\ell}(g_k) \rangle \\ &= \dim \langle \mathrm{pr}_{i\ell+1,(i+1)\ell}(g_1), \ldots, \mathrm{pr}_{i\ell+1,(i+1)\ell}(g_k) \rangle \\ &= \text{rank of the } i\ell+1, i\ell+2, \ldots, (i+1)\ell \text{ columns of } G. \end{aligned}$$

□

Remark 1. *Using the notations from the proof of Lemma 1.3, it is easy to see that* $\langle \mathrm{pr}_{i\ell+1,(i+1)\ell}(G) \rangle = \langle \mathrm{pr}_{j\ell+1,(j+1)\ell}(G) \rangle$ *for all* $0 \leq i, j \leq m-1$.

Definition 1.4 (block rank)**.** *We call the integer r from Lemma 1.3 the* block rank *of $\mathcal{C}$. Note that r depends only on $\mathcal{C}$ and not on a generator matrix of $\mathcal{C}$.*

Remark 2. *Observe that*

- *The folded code of a ℓ-quasi-cyclic code of length $m\ell$ over $\mathbb{F}_q$ is a $\mathbb{F}_q$-cyclic code of length m over $\mathbb{F}_{q^\ell}$.*
- *The unfolded code of a cyclic code of length m over $\mathbb{F}_{q^\ell}$ is a ℓ-quasi-cyclic code of length $m\ell$ over $\mathbb{F}_q$.*

2 Classification of quasi-cyclic codes

It is well-known that there is an one-to-one correspondence between cyclic codes of length n over $\mathbb{F}_q$ and monic factors of $X^n - 1$ in $\mathbb{F}_q[X]$ – that is to say ideals of $\mathbb{F}_q[X]/(X^n - 1)$. In [3, 4] the authors start to exhibit such a correspondence for quasi-cyclic codes. Indeed they show that there is a correspondence between a sub-family of ℓ-quasi-cyclic codes of length $m\ell$ over $\mathbb{F}_q$ and reversible factors of $X^m - 1$ in $M_\ell(\mathbb{F}_q)[X]$ – the polynomials cancel those quasi-cyclic codes.

In this paper we prove that every single ℓ-quasi-cyclic code of length $m\ell$ over $\mathbb{F}_q$ corresponds to a principal ideal of $M_\ell(\mathbb{F}_q)[X]/(X^m - 1)$. Furthermore every ideals of this ring are principal.

2.1 Building a quasi-cyclic code from a principal ideal

Let I be an ideal of $M_\ell(\mathbb{F}_q)[X]/(X^m-1)$. Let us consider the following $\mathbb{F}_q$-linear map:

$$\begin{array}{ccc} M_\ell(\mathbb{F}_q)[X]/(X^m-1) & \overset{\mathrm{row}_i}{\longrightarrow} & (\mathbb{F}_q^\ell)^m \sim \mathbb{F}_q^{m\ell} \\ Q(X) = \displaystyle\sum_{j=0}^{m-1} Q_j X^j & \longmapsto & \mathrm{row}_i(Q(X)) = (\mathrm{row}_i(Q_0), \dots, \mathrm{row}_i(Q_{m-1})). \end{array}$$

Definition 2.1 (Code associated to an ideal)**.** *Let I be an ideal of $M_\ell(\mathbb{F}_q)[X]/(X^m-1)$. We define the* code $\mathcal{C}_I$ associated to I *by*

$$\mathcal{C}_I = \sum_{i=1}^{\ell} \mathrm{row}_i(I),$$

the $\mathbb{F}_q$-vector subspace of $\mathbb{F}_q^{m\ell}$ generated by the vectors of $\mathrm{row}_1(I), \dots, \mathrm{row}_\ell(I)$.

Proposition 2.1. *Let I be an ideal of $M_\ell(\mathbb{F}_q)[X]/(X^m-1)$. Then*

$$\mathcal{C}_I = \mathrm{row}_1(I).$$

Proof. Let $Q(X) \in I$ and $i \in \{1, \dots, \ell\}$. Let $P_{1,i}$ be the permutation matrix that exchange row i and row 1. Then $P_{1,i}Q(X) \in I$ and $\mathrm{row}_1(P_{1,i}Q(X)) = \mathrm{row}_i(Q(X))$. Thus $\mathrm{row}_i(I) \subset \mathrm{row}_1(I)$ for all $i \in \{1, \dots, \ell\}$. □

Remark 3. *Using the same notations as above, we see that:*

- row_1 *is a $\mathbb{F}_q$-linear map.*
- *I is a $\mathbb{F}_q$-linear space, so is $\mathcal{C}_I$.*
- *Multiplication by X in I corresponds to ℓ-right shift in $\mathcal{C}_I$.*
- *Multiplication by a matrix in I corresponds to a linear combinations of words in $\mathcal{C}_I$.*

Corollary 2.2. *Let I be an ideal of $M_\ell(\mathbb{F}_q)[X]/(X^m-1)$. Then there exists $P_1(X), \dots, P_r(X)$ such that $I = (P_1(X), \dots, P_r(X))$ and $\mathcal{C}_I$ is spanned by $\{\mathrm{row}_k(X^i P_j(X)) \;\;/\;\; i = 0, \dots, m-1, \;\; j = 1, \dots, r, \;\; k = 1, \dots, \ell\}$ as a $\mathbb{F}_q$-linear space and is a ℓ-quasi-cyclic code of length $m\ell$ over $\mathbb{F}_q$.*

Example 1. *Let $\mathbb{F}_4 = \mathbb{F}_2[\omega]$ and $I = \langle P(X), Q(X) \rangle \subset M_3(\mathbb{F}_4)[X]/(X^5-1)$ with*

$$P(X) = \begin{pmatrix} \omega & 0 & 1 \\ \omega & \omega & 0 \\ \omega^2 & \omega^2 & 0 \end{pmatrix} X^4 + \begin{pmatrix} \omega & \omega^2 & \omega^2 \\ 0 & \omega & 1 \\ \omega^2 & 0 & \omega \end{pmatrix} X^3 + \begin{pmatrix} 0 & \omega^2 & \omega \\ \omega & \omega^2 & \omega^2 \\ 0 & 1 & \omega^2 \end{pmatrix} X^2 + \begin{pmatrix} 1 & 0 & \omega^2 \\ 0 & \omega & 1 \\ 0 & \omega & 1 \end{pmatrix} X + \begin{pmatrix} 1 & 0 & \omega^2 \\ 0 & 1 & \omega^2 \\ 0 & 0 & 0 \end{pmatrix}$$

and

$$Q(X) = \begin{pmatrix} \omega & 0 & 1 \\ \omega & \omega & 0 \\ \omega^2 & \omega^2 & 0 \end{pmatrix} X^4 + \begin{pmatrix} 0 & 1 & \omega^2 \\ 0 & 1 & \omega^2 \\ 0 & \omega & 1 \end{pmatrix} X^3 + \begin{pmatrix} \omega & \omega^2 & \omega^2 \\ 1 & \omega & \omega \\ \omega & \omega^2 & \omega^2 \end{pmatrix} X^2 + \begin{pmatrix} 1 & \omega^2 & 1 \\ 0 & \omega^2 & \omega \\ 0 & 1 & \omega^2 \end{pmatrix} X + \begin{pmatrix} 1 & 1 & 0 \\ \omega & \omega^2 & \omega^2 \\ \omega^2 & 1 & 1 \end{pmatrix}.$$

Then $\mathcal{C}_I$ is a code over $\mathbb{F}_4$ of length 15 spanned by

$$(\omega, 0, 1, \omega, \omega^2, \omega^2, 0, \omega^2, \omega, 1, 0, \omega^2, 1, 0, \omega^2)$$
$$(\omega, \omega, 0, 0, \omega, 1, \omega, \omega^2, \omega^2, 0, \omega, 1, 0, 1, \omega^2)$$
$$\ldots$$

2.2 Building a principal ideal from a quasi-cyclic code

In this subsection $\mathcal{C}$ denotes a ℓ-quasi-cyclic code of length $m\ell$ over $\mathbb{F}_q$.

Let r be the block rank of $\mathcal{C}$, the following algorithm compute a basis of $\mathcal{C}$ from r vectors of $\mathcal{C}$ and their shifted. We call the *first index* of a nonzero vector $(x_1, \ldots, x_{m\ell})$ the least integer $0 \leq i \leq m-1$ such that $(x_{i\ell+1}, \ldots, x_{(i+1)\ell}) \neq 0$ and denote it by $\mathcal{F}(x_1, \ldots, x_{m\ell})$. Let

$$\begin{array}{rcc} p : \mathbb{F}_q^{m\ell} & \longrightarrow & \mathbb{F}_q^{\ell} \\ (x_1, \ldots, x_{m\ell}) & \longmapsto & (x_{i\ell+1}, \ldots, x_{(i+1)\ell}), \end{array}$$

where $i = \mathcal{F}(x_1, \ldots, x_n)$ and $p(0) = 0$.

Proposition 2.3. *Algorithm 2.2 returns r linearly independent vectors $F = (g_1, \ldots, g_r)$ of $\mathcal{C}$ and a basis G of $\mathcal{C}$ made of $g_1, \ldots, g_r$ and some of their shifted.*

Proof. We will proove by induction on j that $\#p(F) = \#F$ and $\langle G \rangle = \langle \{g_i | \mathcal{F}(g_i) \geq j\} \rangle$. When $j = m-1$ we have $\#B'' = \#B$, $F_T = \emptyset$ and $G = B$. Thus $\langle G \rangle = \langle \{g_i | \mathcal{F}(g_i) \geq m-1\} \rangle$. Moreover we have $F = B$, thus $\#p(F) = \#p(B) = \#B = \#F$.

Now let $j < m-1$. We first have to proove that $\#B' \leq \#F$ for step 11. Remark that $F \neq \emptyset$ and consider the projection $\mathrm{pr} : \langle p(B') \rangle \subset \langle p(F) \rangle \oplus \langle p(B'') \rangle \to \langle p(F) \rangle$. If $\mathrm{pr}(x) = 0$ then $x \in \langle p(B'') \rangle$. But $x \in \langle p(B') \rangle$. As $\langle p(B') \rangle$ and $\langle p(B'') \rangle$ are direct summands we must have $x = 0$. Thus pr is injective. As the matrix G formed by the g_i's is in row-echelon form we have $\#p(B) = B$. By the inductive hypothesis, $\#p(F) = \#F$. Therefore we have $\#B' \leq \#F$ and one can pick $\#B'$ vectors from F.

Before step 13, the matrix formed by the elements of F is in row echelon

Algorithm 2.1 Basis computation with the block rank

Compute a generator matrix G' of $\mathcal{C}$ in row echelon form
and denote by $g_1, \ldots, g_k$ its rows.

1: $F, G \leftarrow \emptyset$.
2: **for** $j = m-1 \rightarrow 0$ **do**
3: $\quad B \leftarrow \{g_i | \mathcal{F}(g_i) = j\}$.
4: $\quad B'' \leftarrow \emptyset$.
5: $\quad$ **for** each element x of B **do**
6: $\quad\quad$ **if** $p(F) \cup p(B'') \cup \{p(x)\}$ are independant **then**
7: $\quad\quad\quad B'' \leftarrow B'' \cup \{x\}$.
8: $\quad\quad$ **end if**
9: $\quad$ **end for**
10: $\quad B' \leftarrow B \backslash B''$.
11: $\quad$ Take a subset $\bar{F}$ of F such that $\#\bar{F} = \#B'$.
12: $\quad F_T \leftarrow \{T^{(j-\mathcal{F}(x))\ell}(x) | x \in \bar{F}\}$.
13: $\quad G \leftarrow G \cup B'' \cup F_T$.
14: $\quad F \leftarrow F \cup B''$.
15: **end for**
16: **return** F, G.

form thus the vectors of $G \cup B'' \cup F_T$ are linearly independent and we have

$$\begin{array}{rclcl} \#(G \cup B'' \cup F_T) & = & \#G & + & \#B'' + \#F_T \\ \#(G \cup B'' \cup F_T) & = & \#G & + & \#B'' + \#B' \\ & = & \#\{g_i | \mathcal{F}(g_i) \geq j+1\} & + & \#B \\ & = & \#\{g_i | \mathcal{F}(g_i) \geq j+1\} & + & \#\{g_i | \mathcal{F}(g_i) = j\} \\ & = & \#\{g_i | \mathcal{F}(g_i) \geq j\} & & \end{array}$$

by the inductive hypothesis. Thus after step 13 we have $\langle G \rangle = \langle \{g_i | \mathcal{F}(g_i) \geq j\} \rangle$.

Before step 12, the construction of B'' in steps 4 to 9 implies that

$$\#p(F \cup B'') = \#p(F) + \#p(B'') = \#F + \#B''.$$

Thus after step 13 we have $\#p(F) = \#F$. $\square$

Corollary 2.4. *There exists $g_1, \ldots, g_r$ linearly independent vectors of $\mathcal{C}$ such that $g_1, \ldots, g_r, T^\ell(g_1), \ldots, T^\ell(g_r), \ldots, T^{(m-1)\ell}(g_1), \ldots, T^{(m-1)\ell}(g_r)$ spans $\mathcal{C}$.*

Corollary 2.5. *We denote by $g_{i,j}$ the j'th coordinate of g_i. Let*

$$G_i \triangleq \begin{pmatrix} g_{1,i\ell+1} & \cdots & g_{1,(i+1)\ell} \\ \vdots & & \vdots \\ g_{r,i\ell+1} & \cdots & g_{r,(i+1)\ell} \\ & 0 & \end{pmatrix} \in M_\ell(\mathbb{F}_q)$$

and

$$g(X) \triangleq \frac{1}{X^\nu} \sum_{i=0}^{m-1} G_i X^i \in M_\ell(\mathbb{F}_q)[X],$$

where ν is the least integer such that $G_i \neq 0$. Then $\mathcal{C} = \mathcal{C}_{\langle G \rangle}$.

Definition 2.2 (Generator)**.** *Let $\mathcal{C}$ be a quasi-cyclic code. Let $g_1, \dots, g_r$ be such that $g_1, \dots, g_r, T^{\ell}(g_1), \dots, T^{\ell}(g_r), \dots, T^{(m-1)\ell}(g_1), \dots, T^{(m-1)\ell}(g_r)$ span $\mathcal{C}$. We call the polynomial $g(X) \in M_\ell(\mathbb{F}_q)[X]$ from Corollary 2.5 a* generator *of $\mathcal{C}$.*

Theorem 2.6. *There exists a one-to-one correspondence between ℓ-quasi-cyclic codes of length $m\ell$ over $\mathbb{F}_q$ and ideals of $M_\ell(\mathbb{F}_q)[X]/(X^m-1)$. Moreover any ideal of $M_\ell(\mathbb{F}_q)[X]/(X^m-1)$ is principal.*

Proof. Let I be an ideal of $M_\ell(\mathbb{F}_q[X])/(X^m-1)$, $\mathcal{C}_I$ be the ℓ-quasi-cyclic associated to I and $g(X)$ be a generator of $\mathcal{C}_I$.

Let $P(X) \in I$. By definition of $g(X)$, there exist $c_{jk}^{(i)} \in \mathbb{F}_q$ such that

$$\mathrm{row}_k(P(X)) = \sum_{i=0}^{m-1} \sum_{j=1}^{r} c_{jk}^{(i)} T^{i\ell}(g_j)$$

for $k = 1, \dots, \ell$. And then

$$P(X) = \left[\sum_{i=0}^{m-1} \begin{pmatrix} c_{11}^{(i)} & \dots & c_{\ell 1}^{(i)} \\ \vdots & & \vdots \\ c_{1\ell}^{(i)} & \dots & c_{\ell\ell}^{(i)} \end{pmatrix} X^i \right] g(X).$$

Thus $I \subset \langle g(X) \rangle$. Conversely let $P_1(X), \dots, P_n(X)$ be generators of I. By definition of $g(X)$, there exist $b_i^{(j)} \in \mathbb{F}_q$ such that

$$\mathrm{row}_j(g(X)) = \sum_{i=1}^{n} b_i^{(j)} \, \mathrm{row}_j(P_i(X)).$$

Thus we have

$$g(X) = \sum_{i=1}^{n} \begin{pmatrix} b_1^{(i)} & b_2^{(i)} & \dots & b_\ell^{(i)} \\ b_1^{(i)} & b_2^{(i)} & \dots & b_\ell^{(i)} \\ \dots & \dots & \dots & \dots \\ b_1^{(i)} & b_2^{(i)} & \dots & b_\ell^{(i)} \end{pmatrix} P_i(X)$$

and $g(X) \in I$.

Thus the map $\mathcal{C} \mapsto \langle g(X) \rangle$ is the inverse of $\mathcal{C} \mapsto \mathcal{C}_I$ by Corollary 2.5. $\square$

Example 2. *If $I = \langle P(X), Q(X) \rangle \subset M_3(\mathbb{F}_4)[X]/(X^5-1)$ is as in the previous example, the row echelon form generator matrix of $\mathcal{C}_I$ is*

$$G = \left(\begin{array}{ccc|ccc|ccc|ccc|ccc} 1 & 0 & \omega^2 & 0 & 0 & 0 & 0 & \omega^2 & \omega & \omega & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & \omega^2 & 0 & 0 & 0 & 0 & 0 & 0 & \omega & \omega & 0 & 1 & 0 & \omega^2 \\ \hline 0 & 0 & 0 & 1 & 0 & \omega^2 & 0 & 0 & 0 & 0 & \omega^2 & \omega & \omega & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & \omega^2 & 0 & \omega^2 & \omega & \omega & 0 & 1 & \omega & \omega & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & \omega^2 & 0 & \omega & 0 & \omega^2 & \omega \end{array} \right).$$

Algorithm 2.2 gives that $(g_4, g_5, T(g_4), T(g_5), T^2(g_5))$ is a basis of $\mathcal{C}_I$. Moreover

$$g(X) = \begin{pmatrix} 0 & 1 & \omega^2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & \omega^2 & \omega \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} X + \begin{pmatrix} \omega & 0 & 1 \\ \omega & 0 & \omega \\ 0 & 0 & 0 \end{pmatrix} X^2 + \begin{pmatrix} \omega & \omega & 0 \\ 0 & \omega^2 & \omega \\ 0 & 0 & 0 \end{pmatrix} X^3.$$

is a generator of $\mathcal{C}_I$ and $I = \langle P(X), Q(X) \rangle = \langle g(X) \rangle$.

2.3 Properties of generators

Proposition 2.7. *Let $\mathcal{C}$ be a ℓ-quasi-cyclic code of length $m\ell$ over $\mathbb{F}_q$. Let $P(X)$ be a generator of $\mathcal{C}$ and $Q(X)$ a generator of its dual. Then there exists $U(X) \in M_\ell(\mathbb{F}_q)[X]$ such that*

$$P(X)\left({}^tQ^*(X)\right) = U(X)(X^m - 1)$$

where Q^* denotes the reciprocal polynomial of Q and ${}^tQ$ the polynomial whose coefficients are the transposes of the coefficients of Q.

Proof. Since $P(X) = \sum_{i=0}^{m-1} P_i X^i$ is a generator of $\mathcal{C}$, the rows of the matrix

$$\begin{pmatrix} P_0 & P_1 & \dots & P_{m-1} \end{pmatrix}$$

and their shifted span $\mathcal{C}$. Similarly $Q(X) = \sum_{i=0}^{m-1} Q_i X^i$ and the rows of

$$\begin{pmatrix} Q_0 & Q_1 & \dots & Q_{m-1} \end{pmatrix}$$

and their shifted span $\mathcal{C}^\perp$. By definition of a dual code, we have

$$\begin{pmatrix} P_0 & P_1 & \cdots & P_{m-1} \end{pmatrix} \begin{pmatrix} {}^tQ_0 \\ {}^tQ_1 \\ \vdots \\ {}^tQ_{m-1} \end{pmatrix} = \sum_{i=0}^{m-1} P_i \left({}^tQ_i\right) = 0.$$

As $\mathcal{C}$ and $\mathcal{C}^\perp$ are ℓ-quasi cyclic codes we also have

$$\sum_{i=0}^{m-1} P_i \left({}^tQ_{i+j \mod m}\right) = 0$$

for all $j \in \mathbb{Z}$. Therefore

$$P(X)\left({}^tQ^\star(X)\right) = \sum_{j=0}^{m-1} \sum_{i=0}^{m-1} P_i \left({}^tQ_{i-j \mod m}\right) = 0 \mod (X^m - 1)$$

Hence the proposition. $\square$

3 Quasi-BCH

Since the quasi-cyclic codes can be viewed as a generalisation of cyclic codes, it is interesting to focus on the generalisation of BCH codes. We start with an explicit definition of this family of codes, then we study the parameters of such codes and finally we present a decoding algorithm designed for these codes.

3.1 Definition

Definition 3.1 (Primitive root of unity). *Let ℓ, m and e be positive integers. Let q be a power of a prime integer. A matrix $A \in M_\ell(\mathbb{F}_{q^e})$ is called a* primitive m-th root of unity *if*

- $A^m = I_\ell$,
- $A^i \neq I_\ell$ *if* $i < m$,
- $\det(A^i - A^j) \neq 0$ *whenever* $i \neq j$

Proposition 3.1. *Let q be a power of a prime and e, ℓ and m be positive integers such that $q^{e\ell} = 1 \mod m$. Then there exists a primitive m-th root of unity in $M_\ell(\mathbb{F}_{q^e})$.*

Proof. There exists a primitive m-th root of unity $\alpha \in \mathbb{F}_{q^{e\ell}}$. Let $A \in M_\ell(\mathbb{F}_{q^e})$ be the companion matrix of the irreducible polynomial $f(X) \in \mathbb{F}_{q^e}[X]$ of α over $\mathbb{F}_{q^e}$. There exists $P \in \mathrm{GL}_\ell(\mathbb{F}_{q^{e\ell}})$ and an upper triangular matrix $U \in M_\ell(\mathbb{F}_{q^{e\ell}})$ whose diagonal coefficients are the eigenvalues of A such that $A = P^{-1}UP$. The eigenvalues of A are exactly the roots of f and then are primitive m-th roots of unity. Therefore A satifies the three conditions of Definition 3.1. □

Definition 3.2 (block minimum distance). *Let $\mathcal{C}$ be a linear code over $\mathbb{F}_q$ of length $m\ell$. We define the ℓ-*block minimum distance *of $\mathcal{C}$ to be the minimum distance of the folded code of $\mathcal{C}$.*

Definition 3.3 (Left quasi-BCH codes). *Let A be a primitive m-th root of unity in $M_\ell(\mathbb{F}_{q^e})$ and $\delta \leq m$. We define the left ℓ-quasi-BCH code of length $m\ell$ defined by A with designed minimum distance δ over $\mathbb{F}_q$ by*

$$\text{Q-BCH}_q(m, \ell, \delta, A) \triangleq \left\{ (c_1, \ldots, c_m) \in (\mathbb{F}_q^\ell)^m \;\middle|\; \sum_{j=0}^{m-1} A^{ij} c_j = 0 \;\; \textit{for } i = 1, \ldots, \delta - 1 \right\}$$

We call the linear map

$$\begin{array}{rcl} \mathcal{S}_A : (\mathbb{F}_q^\ell)^m & \to & \mathbb{F}_{q^e}^\ell \\ c = (c_1, \ldots, c_m) & \mapsto & \sum_{j=0}^{m-1} A^{ij} c_j \end{array}$$

the syndrome *map of* Q-BCH(m, ℓ, δ, A).

Proposition 3.2. *Using the same notations as above* $\text{Q-BCH}_q(m,\ell,\delta,A)$ *has dimension at least* $(m-e(\delta-1))\ell$ *and* ℓ*-block minimum distance at least* δ*. In other words* $\text{Q-BCH}_q(m,\ell,\delta,A)$ *is a* $[m\ell,(m-e(\delta-1))\ell,\geq\delta]_{\mathbb{F}_q}$*-code.*

Proof. According to the definition of left quasi-BCH codes,

$$H=\begin{pmatrix} I_\ell & A & \cdots & A^{m-1} \\ I_\ell & A^2 & \cdots & A^{2(m-1)} \\ \vdots & \vdots & & \vdots \\ I_\ell & A^{\delta-1} & \cdots & A^{(\delta-1)(m-1)} \end{pmatrix} \in M_{(\delta-1)\ell,m\ell}(\mathbb{F}_{q^e})$$

is a parity check matrix of $\text{Q-BCH}_q(m,\ell,\delta,A)$. Let

$$V=\begin{pmatrix} I_\ell & A & \cdots & A^{\delta-1} \\ I_\ell & A^2 & \cdots & A^{2(m-1)} \\ \vdots & \vdots & & \vdots \\ I_\ell & A^{\delta-1} & \cdots & A^{(\delta-1)^2} \end{pmatrix}.$$

Using the Vandermonde matrix trick we find that

$$\det_{\mathbb{F}_{q^e}} V=\prod_{i<j}\det_{\mathbb{F}_{q^e}}(A^i-A^j)$$

By the definition of A we have $\det_{\mathbb{F}_{q^e}} V\neq 0$ and H has full rank over $\mathbb{F}_{q^e}$. Let $i:\mathbb{F}_q^{m\ell}\to\mathbb{F}_{q^e}^{m\ell}$ be the canonical injection and denote by $h:\mathbb{F}_{q^e}^{m\ell}\to\mathbb{F}_{q^e}^{(\delta-1)\ell}$ the $\mathbb{F}_q$-linear map given by H. Then we have $\dim_{\mathbb{F}_q}(\operatorname{Im} h)=e(\delta-1)\ell$. Thus $\dim_{\mathbb{F}_{q^e}}(\operatorname{Im} h\circ i)\leq(\delta-1)\ell$ and $\dim_{\mathbb{F}_q}(\operatorname{Im} h\circ i)\leq e(\delta-1)\ell$. Therefore $\dim_{\mathbb{F}_q}(\ker h\circ i)\geq m\ell-e(\delta-1)\ell$. Suppose that there exists a codeword $c=(c_1,\ldots,c_m)\in\mathcal{C}\setminus\{0\}$ with ℓ-block weight $b\leq\delta-1$. Note $i_1,\ldots,i_b$ the indices such that $c_{i_j}\neq 0$ for $i=1,\ldots,b$. This implies that the matrix

$$\begin{pmatrix} A^{i_1} & A^{i_2} & \cdots & A^{i_b} \\ A^{2i_1} & A^{2i_2} & \cdots & A^{2i_b} \\ \vdots & \vdots & & \vdots \\ A^{(\delta-1)i_1} & A^{(\delta-1)i_2} & \cdots & A^{(\delta-1)i_b} \end{pmatrix}$$

has not full rank which is absurd. □

Example 3. *Consider the left* 3*-quasi-BCH codes defined by primitive roots in* $M_3(\mathbb{F}_{2^2})$ *of length* 63 *over* $\mathbb{F}_2$ *with designed minimum distance* 6 *defined by a* 21*-th root of unity in* $\mathbb{F}_{2^2}$*. In other words, taking the above notations, we have* $q=2, m=21, \ell=3, e=2$ *and* $\delta=6$*. There are* 22 *non-equivalent codes splitting as following:*

Number of codes	*Parameters*
2	$[63,33,6]_{\mathbb{F}_2}$
18	$[63,33,7]_{\mathbb{F}_2}$
2	$[63,36,6]_{\mathbb{F}_2}$

Notice that their dimension is always at least $(m - e(\delta - 1))\ell = 33$ *and their minimum distance is at least* $\delta = 6$.

Example 4. *Let* $q = 5, m = 7, \ell = 3, e = 2$ *and* $\delta = 3$. *Let* $\omega \in \mathbb{F}_{5^2}$ *be a primitive* $(5^2 - 1)$*-th root of unity and*

$$A = \begin{pmatrix} \omega^9 & \omega^4 & \omega^{22} \\ \omega^{11} & \omega^{11} & \omega^{15} \\ \omega^2 & \omega^{19} & 1 \end{pmatrix} \in M_3(\mathbb{F}_{5^2}).$$

Then the left 3*-quasi-BCH code of length* 21 *defined by* A *with designed minimum distance* 3 *over* $\mathbb{F}_5$ *has parameters* $[21, 9, 7]_{\mathbb{F}_5}$. *It is in fact* $\mathcal{C}_{\langle g(X) \rangle}$ *with*

$$g(X) = \begin{pmatrix} 1 & 4 & 3 \\ 3 & 3 & 4 \\ 1 & 1 & 4 \end{pmatrix} X^4 + \begin{pmatrix} 4 & 0 & 0 \\ 4 & 0 & 0 \\ 4 & 0 & 4 \end{pmatrix} X^3 + \begin{pmatrix} 3 & 0 & 4 \\ 0 & 3 & 4 \\ 0 & 0 & 0 \end{pmatrix} X^2 + \begin{pmatrix} 2 & 3 & 2 \\ 4 & 4 & 4 \\ 3 & 1 & 1 \end{pmatrix} X + \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in M_3(\mathbb{F}_5)[X].$$

And we have ${}^t g(A) = {}^t g(A^2) = 0$. *Note that this is true for all quasi-BCH codes up to* $A^{\delta - 1}$.

3.2 Decoding algorithm

In the case that the folded code of a ℓ-quasi-BCH code $\mathcal{C}$ over $\mathbb{F}_q$ is a BCH code over $\mathbb{F}_{q^\ell}$, we propose a decoding algorithm for BCH codes in order to decode the quasi-BCH codes. Indeed, let $c \in \mathcal{C}$ be a codeword of a quasi-BCH code, $e \in (\mathbb{F}_q^\ell)^m$ be an error vector and $y \triangleq c + e$ be the received word. Then we obtain thanks to the folding function

$$\begin{aligned} \phi(y) &= \phi(c) + \phi(e) \\ \mathrm{dec}(\phi(y)) &= \phi(c) \\ \phi^{-1}(\mathrm{dec}(\phi(y))) &= c, \end{aligned}$$

where dec is a decoding map of $\phi(\mathcal{C})$ which is able to decode up to the Hamming weight of $\phi(e)$ which is at most $\mathrm{w}(e)$.

As the BCH codes are alternant, we can also use the list decoding algorithm proposed in [1]. Thus we are able to decode the quasi-BCH codes up to the q^ℓ–ary Johnson bound, which is

$$\frac{q^\ell - 1}{q^\ell} m \left(1 - \sqrt{1 - \frac{q^\ell}{q^\ell - 1} \frac{\delta}{m}} \right),$$

in polynomial time in m.

It may happen that $\phi(\mathcal{C})$ is not a BCH code or the BCH code obtained is trivial (that is $\phi(\mathcal{C}) = \{0\}$). In order to tackle these problems we propose a decoding algorithm based on a key equation. As in the scalar case, we propose first, to compute the localisator and evaluator polynomials by solving the key equation and finally to compute the error vector e with to the two previous polynomials.

3.3 The key equation

As in the scalar case, we propose to exhibit a key equation for the quasi-BCH codes and a method to solve it. So we are able to decode these codes up to the half the designed minimum distance. Fix a Q-BCH$_q(m, \ell, \delta, A)$ code. We first need to introduce some notations.

In the sequel of the article, all vectors are considered to be column vectors. Consider $\mathbb{F}_q^\ell$ as a product ring of ℓ copies of $\mathbb{F}_q$. Let $f = \sum f_i X^i \in \mathbb{F}_q^\ell[[X]]$ and $g = \sum g_j X^j \in M_\ell(\mathbb{F}_{q^e})[[X]]$. We define a map

$$\begin{array}{rcl} \Psi : \mathbb{F}_q^\ell[[X]] \times M_\ell(\mathbb{F}_{q^e})[[X]] & \to & \mathbb{F}_{q^e}^\ell[[X]] \\ (g, f) & \mapsto & \sum_{i,j} g_j f_i X^{i+j} \end{array}$$

where the $g_i f_j$ are matrix-vector products. In the sequel we will denote $\Psi(g, f)$ simply by $g \diamond f$. Note that we have $(fh)\diamond g = f \diamond (h \diamond g)$ for any $h \in M_\ell(\mathbb{F}_{q^e})$. Let c be a codeword of Q-BCH(m, ℓ, δ, A) sent over a channel, $y \in (\mathbb{F}_q^\ell)^m$ the received codeword and the error vector $e = y - c$ such that $\mathrm{w}(e) = w \leq \lfloor (\delta - 1)/2 \rfloor$. Let $\mathrm{Supp}(e) = \{i_1, \ldots, i_w\}$, $\alpha_j = A^{i_j}$ and $y_j = e_{i_j} \in \mathbb{F}_q^\ell$ for $j = 1, \ldots, w$.

Definition 3.4. *We define the* localisator polynomial *by*

$$\Lambda(X) \triangleq \prod_{i=1}^{w} (1 - \alpha_i X) \in M_\ell(\mathbb{F}_{q^e})$$

and the evaluator polynomial *by*

$$L(X) \triangleq \sum_{i=1}^{w} \left(\prod_{j \neq i}^{w} \alpha_i (1 - \alpha_j) X \right) \diamond y_i \in \mathbb{F}_q^\ell[X].$$

Lemma 3.3. *Let $B \in M_\ell(\mathbb{F}_q)$, a nonzero matrix, then $1 - BX$ is invertible in $M_\ell(\mathbb{F}_q)[[X]]$ and its inverse is*

$$\sum_{j=0}^{+\infty} B^j X^j.$$

Note that the inverse is a right- and also a left-inverse of $1 - BX$.

By the previous lemma, the localisator polynomial $\Lambda(X)$ is invertible in the power series ring $M_\ell(\mathbb{F}_{q^e})[[X]]$ and we have

$$
\begin{aligned}
\left(\Lambda(X)^{-1}\right) \diamond L(X) &= \sum_{i=1}^{w} \left(\alpha_i(1-\alpha_i X)^{-1}\right) \diamond y_i \\
&= \sum_{i=1}^{w} \left(\sum_{j=0}^{+\infty} \alpha_i^{j+1} X^j\right) \diamond y_i \\
&= \sum_{j=0}^{+\infty} \sum_{i=1}^{w} \alpha_i^{j+1} y_i X^j
\end{aligned}
$$

Using the fact that $y = c + e$ and that by definition $\mathcal{S}_{A^i}(y) = \mathcal{S}_{A^i}(e)$ for any $i = 1, \dots,$ we have

$$\left(\Lambda(X)^{-1}\right) \diamond L(X) = \sum_{j=0}^{+\infty} \mathcal{S}_{A^{j+1}}(e) X^j \triangleq S_\infty(X).$$

Proposition 3.4. *For any* Q-BCH(m, ℓ, δ, A) *we have that*

$$\boxed{\Lambda(X) \diamond S_\infty(X) = L(X)}$$

and therefore

$$\Lambda(X) \diamond S_\infty(X) \equiv L(X) \mod X^\delta. \tag{1}$$

We will refer to this equation by the key equation*.*

3.3.1 Solving the key equation

We take the same notations as in the previous section. In the scalar case, the extended Euclid or Berlekamp-Massey algorithms can be used to solve the key equation for BCH codes. There is no Euclidean algorithm over matrix rings [9] so we propose an algorithm to solve equation (1). We denote by $S_\delta(X)$ the polynomial $S_\infty(X) \mod X^\delta$.

As in the scalar case we can solve the key eqaution with linear algebra. The key equation can be rewritten as

$$\begin{pmatrix} \Lambda_0 & \dots & \Lambda_{\delta-1} & | & L_0 & \dots & L_{\delta-1} \end{pmatrix} \left(\begin{array}{cccc} S_0 & S_1 & \dots & S_{\delta-1} \\ & S_0 & & \vdots \\ & & \ddots & \vdots \\ & & & S_0 \\ \hline -1 & 0 & \dots & 0 \\ 0 & -1 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \dots & 0 & -1 \end{array}\right) = 0 \tag{2}$$

Where the S_i's and L_i's are columns vectors such that the S_i's are the coefficients of S_δ in $\mathbb{F}_{q^e}^\ell$ and the L_i's are the coefficients in $\mathbb{F}_{q^e}^\ell$ of $L(X)$. The Λ_i's are the coefficients of $\Lambda(X)$ in $M_\ell(\mathbb{F}_{q^e})$. This system of linear equations over $\mathbb{F}_q$ has many solutions since there are $\ell\delta + \delta$ unknows and only δ equations for each row of

$$\begin{pmatrix} \Lambda_0 & \dots & \Lambda_{\delta-1} & | & L_0 & \dots & L_{\delta-1} \end{pmatrix}.$$

However, we are only interested in the solution such that $(\Lambda_0, \dots, \Lambda_{\delta-1})$ is an error locator polynomial. In other words, if we let $\mathfrak{B}$ be the solutions of Equation 2 and

$$\mathfrak{S} = \left\{ \prod_{i \in W} (1 - A^i X) \in M_\ell(\mathbb{F}_{q^e}) \middle| W \subset \{1, \dots, m\} \text{ and } \#W \leq \lfloor (\delta-1)/2 \rfloor \right\}$$

be the set of all possible locator polynomials corresponding to errors of weight at most $\lfloor (\delta-1)/2 \rfloor$, we are interested in the elements of $\mathfrak{B} \cap \mathfrak{S}$.

Proposition 3.5. *Taking the same notations as above, it exists one and only one solution of Equation (2) in* $\mathfrak{S}$.

Proof. Equation 1 ensures that there exists at least one element in $\mathfrak{B} \cap \mathfrak{S}$. If there were more than one solution in $\mathfrak{S}$ there would exist more than one codeword in a Hamming ball of radius $\lfloor (\delta-1)/2 \rfloor$ which is absurd. $\square$

3.3.2 Unambiguous decoding algorithm

In this subsection, we prove that, as in the scalar case, the roots of the localisator polynomial (in $\mathbb{F}_{q^e}[A]$) give us precious information about the localisation of errors. The factorisation of polynomials of $M_\ell(\mathbb{F}_q)[X]$ is not unique, all the roots of the localisator polynomial do not indicate an error position. In this sense the following proposition is helpful.

Proposition 3.6. *Let* Q-BCH(m, ℓ, δ, A) *be a quasi-BCH code, e be an error vector in* $(\mathbb{F}_q^\ell)^m$ *and* $\Lambda(X)$ *be the localisator polynomial associated to e. We have*

$$e_i \neq 0 \iff \Lambda_l(A^{-i}) = 0.$$

Proof. By definition, we have $\Lambda(A^{-i}) = 0$ if $e_i \neq 0$. Conversely, if $e_i = 0$ then $\alpha_j A^{-i} \neq I_\ell$ for $j = i_1, \dots, i_w$. Thus $1 - \alpha_j A^{-i}$ is a unit in $\mathbb{F}_{q^e}[A]$ by definition of A. Therefore $\Lambda(A^{-i}) \neq 0$. $\square$

These roots can be found by an exhaustive search on the powers of A in at most m attempts. At this step the support of the error vector e is known. The last step to complete the decoding is to find the value of e_i for all i in the support of error W.

Proposition 3.7. *Let* Q-BCH(m, ℓ, δ, A) *be a quasi-BCH code, e be a error vector in* $(\mathbb{F}_q^\ell)^m$, $W = \mathrm{Supp}(e)$ *be the support of the error vector,* $\Lambda(X)$ *be the* *localisator and $L(X)$ be the evaluator polynomials associated to e. If A^{-i} is a root of $\Lambda(X)$ for $i \in W$, then*

$$e_i = \prod_{j \in W \setminus \{i\}} (A^i - A^j)^{-1} L(A^{-i})$$

where $L(A^j)$ denotes $\sum (A^j)^i L_i$.

Proof. Let $i_0 \in W$. We have

$$\begin{aligned} L(A^{-i_0}) &= \sum_{i=1}^{w} \prod_{j \neq i}^{w} \alpha_i (1 - A^{-i_0} \alpha_j) y_i \\ &= \prod_{j \in W \setminus \{i_0\}} A^{i_0} (1 - A^{-i_0} A^j) e_{i_0} \\ &= \prod_{j \in W \setminus \{i_0\}} (A^{i_0} - A^j) e_{i_0} \end{aligned}$$

By definition of A, $A^{i_0} - A^j$ is invertible for all $j \in W$ hence the result. □

Algorithm 3.1 Decoding algorithm for quasi-BCH codes

Input: the received word y and the quasi-BCH code with designed minimum distance δ
Output: The codeword c, if it exists such that $d(y, c) \leq \lfloor (\delta - 1)/2 \rfloor$.

```
S_δ(X) ← Syndrome of y.
Compute Λ(X) and L(X) with linear algebra (section 3.3.1).
𝔑 ← roots of Λ(X) in F_{q^e}[A].
W ← {i | A^{-i} ∈ 𝔑}.
e ← (0, ..., 0).
for i ∈ W do
    e_i = ∏_{j∈W\{i}} (A^i − A^j)^{-1} L(A^{-i}).
end for
return y − e.
```

4 Evaluation codes

4.1 Definition

Is is also possible to construct quasi-cyclic codes which are a generalization of evaluation codes. First, let us define

$$(\mathbb{F}_q[A])[X]_{<k} \triangleq \{P(X) \in (\mathbb{F}_q[A])[X] \mid \deg(P(X)) < k\}.$$

Proposition 4.1. *Let q be a power of a prime and ℓ, m be positive integers such that $m = q^\ell - 1$. Let $A \in M_\ell(\mathbb{F}_q)$ be a primitive m-th root of unity. Then*

$$\mathbb{F}_q[A] \simeq \mathbb{F}_{q^\ell}.$$

Proof. Let $\mu(X)$ be the caracteristic polynomial of A. We have $\mu(X) \mid X^m - 1$, thus the eigenvalues of A are all distinct. They are also primitive m-th root of unity and are therefore in $\mathbb{F}_{q^\ell}$ but not in any subfield. Hence $\mu(X)$ is irreducible over $\mathbb{F}_q$ and $\mathbb{F}_q[A]$ is a field. □

Definition 4.1 (Quasi-cyclic evaluation codes)**.** *Let ℓ be a positive integer and q be a power of a prime. Let $m = q^\ell - 1$ and $k \le m$. Let $A \in M_\ell(\mathbb{F}_q)$ with order m. Let π be a $\mathbb{F}_q$-linear map from $\mathbb{F}_q[A]$ into $\mathbb{F}_q^\ell$. We denote by $C_{A,k,\pi}$ the image of:*

$$\begin{array}{ccccc} (\mathbb{F}_q[A])[X]_{<k} & \xrightarrow{\mathrm{ev}_A} & (\mathbb{F}_q[A])^m & \xrightarrow{\pi^{\times m}} & (\mathbb{F}_q^\ell)^m \\ P(X) & \longmapsto & \left(P(A^0), \dots, P(A^{m-1})\right) & \longmapsto & \left(\pi(P(A^0)), \dots, \pi(P(A^{m-1}))\right). \end{array}$$

Proposition 4.2. *$C_{A,k,\pi}$ is a ℓ-quasi cyclic code over $\mathbb{F}_q$ of length ℓm and dimension at least $k\ell - \dim_{\mathbb{F}_q}(\ker \pi^{\times m})$.*

Proof. By Proposition 4.1 the statement about the dimension of $C_{A,k,\pi}$ is obvious. Let

$$P(X) = \sum_{i=0}^{k-1} \sum_{j=0}^{m-1} P_{ij} A^j X^i \in \mathbb{F}_q[A][X]_{<k}$$

with $P_{ij} \in \mathbb{F}_q$. Then

$$Q(X) = \sum_{i=0}^{k-1} \sum_{j=0}^{m-1} P_{ij} A^{j+i} X^i \in \mathbb{F}_q[A][X]_{<k}$$

is such that $Q(A^i) = P(A^{i+1})$ for all $i \in \mathbb{Z}$ and $C_{A,k,\pi}$ is ℓ-quasi cyclic. □

4.2 Proposition and remarks

Proposition 4.3. *Using the notations from Definition 4.1, if π is such that for $B = (b_{ij}) \in \mathbb{F}_q[A]$*

- *$\pi(B) = (b_{i1}, \dots, b_{i\ell})$ for some i,*
- *or $\pi(B) = (b_{1j}, \dots, b_{\ell j})$ for some j,*

then $\dim C_{A,k,\pi} \ge k\ell$ and $C_{A,k,\pi}$ has minimum distance $d \ge m - k + 1$.

Proof. In both cases, it suffices to notice that $\pi^{\times m}$ is injective. If $\pi^{\times m}(B_1, \dots, B_m) = 0$ then $\det B_i = 0$ for $i = 1, \dots, m$. As $\mathbb{F}_q[A]$ is a field we must have $B_i = 0$ for $i = 1, \dots, m$.

In fact under the assumptions of the proposition $\pi^{\times m}$ is an isomorphism since $\#(F_q[A])^m = q^{m\ell} = \#(F_q^\ell)^m$. □

Remark 4. • *For some particular choices of π, especially when the dimension decreases, we observe that the minimum distance may be multiplied by $\ell - 1$. In that way, with*

$$A = \begin{pmatrix} 0 & \omega & 0 \\ \omega & \omega^2 & \omega^2 \\ 1 & \omega^2 & 1 \end{pmatrix} \in M_3(\mathbb{F}_4) \text{ with } \mathbb{F}_4 = \mathbb{F}_2[\omega],$$

$k = 4$ and $\pi((b_{ij})) = (b_{2,1}, b_{1,2}, b_{2,3})$, we found a $[189, 11, 125]_{\mathbb{F}_4}$-code. According to [7], the previous best known minimum distance was 121.

- *As in the scalar case, one can evaluate the polynomials at less than $m = q^\ell - 1$ points. In that way, we found the following new best codes together with the previous best known minimum distance:*

$$\begin{array}{c} [186, 11, 122]_{\mathbb{F}_4},\ 120 \\ [183, 11, 119]_{\mathbb{F}_4},\ 117 \\ [180, 11, 116]_{\mathbb{F}_4},\ 114 \\ [177, 11, 113]_{\mathbb{F}_4},\ 112 \end{array}$$

- *Using different constructions from previous codes – as for example puncturing [8] – we found with the help of Markus Grassl 49 new codes. There are listed in Table 1. All these constructions are detailed in [7].*

New codes over $\mathbb{F}_4$				
$[171, 11, 109]_4$	$[172, 11, 110]_4$	$[173, 11, 110]_4$	$[174, 11, 111]_4$	$[175, 11, 112]_4$
$[176, 11, 113]_4$	$[177, 11, 114]_4$	$[178, 11, 115]_4$	$[179, 11, 115]_4$	$[180, 11, 116]_4$
$[181, 11, 117]_4$	$[182, 11, 118]_4$	$[183, 11, 119]_4$	$[184, 10, 121]_4$	$[184, 11, 120]_4$
$[185, 10, 122]_4$	$[185, 11, 121]_4$	$[186, 10, 123]_4$	$[186, 11, 122]_4$	$[187, 10, 124]_4$
$[187, 11, 123]_4$	$[188, 10, 125]_4$	$[188, 11, 124]_4$	$[189, 10, 126]_4$	$[189, 11, 125]_4$
$[190, 10, 127]_4$	$[190, 11, 126]_4$	$[191, 10, 128]_4$	$[191, 11, 127]_4$	$[192, 11, 128]_4$
$[193, 11, 128]_4$	$[194, 11, 128]_4$	$[195, 11, 128]_4$	$[196, 11, 129]_4$	$[197, 11, 130]_4$
$[198, 11, 130]_4$	$[199, 11, 131]_4$	$[200, 11, 132]_4$	$[201, 10, 133]_4$	$[201, 11, 132]_4$
$[202, 10, 134]_4$	$[202, 11, 132]_4$	$[203, 10, 135]_4$	$[204, 10, 136]_4$	$[204, 11, 133]_4$
$[205, 11, 134]_4$	$[210, 11, 137]_4$	$[213, 11, 139]_4$	$[214, 11, 140]_4$	

Table 1: The 49 new codes over $\mathbb{F}_4$ which have a larger minimum distance than the previously known ones.

Remark 5. *We have proven in Proposition 4.1 that $\mathbb{F}_q[A]$ is a field such that $[\mathbb{F}_q[A] : \mathbb{F}_q] = \ell$. Thus there is a $\mathbb{F}_q$-linear isomorphism from $\mathbb{F}_q[A]$ into $\mathbb{F}_q^\ell$. Consider the following one:*

$$\begin{array}{ccc} \mathbb{F}_q[A] & \xrightarrow{\psi} & \mathbb{F}_q^\ell \\ B = b_0 I_\ell + b_1 A + \cdots + b_{\ell-1} A^{\ell-1} & \longmapsto & (b_0, b_1, \ldots, b_{\ell-1}). \end{array}$$

Then

$$C_{A,k,\psi} = \psi^{\times m}(\mathrm{ev}_A(\mathbb{F}_q[A][X]_{<k}))$$

is still a ℓ-quasi cyclic code of length $m\ell$ and dimension $k\ell$.

Chosing a $\mathbb{F}_q$-linear map π as in Definition 4.1 here comes to choose a $\ell \times \ell$ matrix Π over $\mathbb{F}_q$. Note π the map from $\mathbb{F}_q^\ell$ into $\mathbb{F}_q^\ell$ corresponding to the right multiplication by Π. Then

$$C_{A,k,\psi,\pi} = \pi^{\times m}(\psi^{\times m}(\mathrm{ev}_A(\mathbb{F}_q[A][X]_{<k})))$$

is a ℓ-quasi cyclic code of length $m\ell$ and dimension $\geq k\ell - \dim(\ker \pi)$.

Given A, we noticed that there exist matrices Π for which the obtained minimum distance is always greater than a bound (that is much higher than $m-k+1$). For instance, taking $\ell = 3$, $q = 4$ and the matrix

$$\Pi = \begin{pmatrix} 1 & \omega^2 & \omega \\ \omega^2 & \omega & 1 \\ 1 & 1 & 1 \end{pmatrix},$$

give codes with minimum distance close to $2(m-k+1)$. Observe that this matrix has rank 2 and its columns span a code of minimum distance 2.

5 Conclusion

In this paper we dealt with the generalization of results for cyclic codes to quasi-cyclic codes. We proved a correspondence between quasi-cyclic codes and ideals of a matricial polynomial ring, which happen to be all principal. Then we built new classes of codes, quasi-BCH codes and evaluation codes and gave decoding algorithms. Finally those constructions allowed us to find a lot of new codes beating previous minimum distance bounds. A deeper study of the decoding algorithms for such codes remains an open problem.

References

[1] Daniel Augot, Morgan Barbier, and Alain Couvreur. List-Decoding of binary Goppa codes up to the binary Johnson bound. In *2011 IEEE Information Theory Workshop (IEEE ITW 2011)*, Paraty, Brazil, October 2011.

[2] Thierry Berger, Pierre-Louis Cayrel, Philippe Gaborit, and Ayoub Otmani. Reducing key length of the McEliece cryptosystem. In Bart Preneel, editor, *Progress in Cryptology – AFRICACRYPT 2009*, volume 5580 of *Lecture Notes in Computer Science*, pages 77–97. Springer Berlin / Heidelberg, 2009.

[3] Pierre-Louis Cayrel, Christophe Chabot, and Abdelkader Necer. Quasi-cyclic codes as codes over rings of matrices. *Finite Fields and Their Applications*, 16(2):100–115, 2010.

[4] Christophe Chabot. Factorisation in $M_l(\mathbb{F}_q)[X]$. Construction of quasi-cyclic codes. In Daniel Augot and Anne Canteaut, editors, *Workshop on Coding and Cryptography 2011*, April 2011.

[5] Jean-Charles Faugère, Ayoub Otmani, Ludovic Perret, and Jean-Pierre Tillich. Algebraic cryptanalysis of McEliece variants with compact keys. In Henri Gilbert, editor, *Advances in Cryptology – EUROCRYPT 2010*, volume 6110 of *Lecture Notes in Computer Science*, pages 279–298. Springer Berlin / Heidelberg, 2010.

[6] P. Fitzpatrick and K. Lally. Algebraic structure of quasi-cyclic codes. *Discrete Applied Mathematics*, 111:157–175, 2001.

[7] Markus Grassl. Bounds on the minimum distance of linear codes and quantum codes. Online available at http://www.codetables.de, 2007. Accessed on 2011-04-19.

[8] Markus Grassl and Greg White. New good linear codes by special puncturings. In *Information Theory, 2004. ISIT 2004. Proceedings. International Symposium on*, page 454, june-2 july 2004.

[9] G. V. Kalaidzhich. Euclidean algorithm in matrix modules over a given euclidean ring. *Siberian Mathematical Journal*, 26:818–822, 1985. 10.1007/BF00969102.

[10] Yuan Xing Li, R.H. Deng, and Xin Mei Wang. On the equivalence of McEliece's and Niederreiter's public-key cryptosystems. *Information Theory, IEEE Transactions on*, 40(1):271 –273, January 1994.

[11] San Ling and Patrick Solé. On the algebraic structure of quasi-cyclic codes I: finite fields. *IEEE Transactions on Information Theory*, 47:2751–2760, 2001.

[12] San Ling and Patrick Solé. Good self-dual quasi-cyclic codes exist. *Information Theory, IEEE Transactions on*, 49(4):1052 – 1053, april 2003.

[13] Robert McEliece. A public-key cryptosystem based on algebraic coding theory. *Deep Space Network Progress Report*, 44:114–116, 1978.

[14] Harald Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. *Problems of Control and Information Theory*, pages 15(2):159–166, 1986.