HAL open science

Factorisation in M'(Fq)[X]. Construction of quasi-cyclic codes

Christophe Chabot

To cite this version:

Christophe Chabot. Factorisation in M'(Fq)[X]. Construction of quasi-cyclic codes. WCC 2011 - Workshop on coding and cryptography, Apr 2011, Paris, France. pp.209-218. inria-00611781

HAL Id: inria-00611781

https://inria.hal.science/inria-00611781v1

Submitted on 27 Jul 2011

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.

Factorisation in $M_\ell(\mathbb{F}_q)[X]$. Construction of quasi-cyclic codes

Christophe Chabot

LJK-CASYS-Université Joseph Fourier (Grenoble)
christophechabotcc@gmail.com

Abstract. Quasi-cyclic codes are viewed as codes cancelled by polynomials with matricial coefficients. This construction leads to the problem of factorisation of $X^m - 1$ in $M_\ell(\mathbb{F}_q)[X]$. In this paper we deal with the general factorisation in $M_\ell(\mathbb{F}_q)[X]$. Then we give results on the roots and the factorisation of the particular polynomial $X^m - 1$. These factorisations permit the construction of such quasi-cyclic codes. We show that in most cases, these codes meet best known bounds for minimum distances. We even found two new codes with parameters better than known $[30, 22, 6]_{\mathbb{F}_4}$ and $[29, 21, 6]_{\mathbb{F}_4}$.

Keywords: Quasi-cyclic codes, factorisation, non-integral ring, polynomials with matricial coefficients.

1 Introduction

Let q be a power of a prime number. Let $n = m\ell$ be an integer. We define the shift map from $\mathbb{F}_q^n$ to $\mathbb{F}_q^n$ denoted by T by:

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

Let C be a code of length $n = m\ell$ over $\mathbb{F}_q$. The code C is said ℓ-quasi-cyclic if

$$\forall c \in C, \quad T^\ell(c) \in C.$$

These codes were studied lately because of several reasons. First of all, they are meant to be a generalisation of cyclic codes. In [4], they see them as concatenation of cyclic codes. In [8], they regard them as linear codes over an auxiliary ring. In [2], the approach is similar, but furthermore they construct a subfamily of quasi-cyclic codes cancelled by polynomials with matricial coefficients. That may be seen as a generalisation of the polynomial representation of cyclic codes. The main results are summarized in the next section.

Secondly quasi-cyclic codes have been proposed to be used in cryptographic schemes as in [5] and [1]. The main interest of their use is that they allow a key reduction compared to the general case of McEliece cryptosystem [9]. Indeed, thanks to their particular automorphism group (it contains at least $\langle T^\ell \rangle$), a generator matrix can be represented only by its first rows. Nevertheless, several

attacks have been detailed in [10] and [3]. These attacks were possible because the subfamilies of quasi-cyclic codes considered were too much structured (for instance, in [3], they use the fact that the codes are alternant). Using quasi-cyclic codes in cryptography is then still an open problem. The aim is to find a large family of quasi-cyclic codes with large minimum distance and a good decoding algorithm, but still indistinguishable from random codes. This paper details the construction of a large family of quasi-cyclic codes. Nonetheless, decoding and indistinguishability are still open problems.

In this paper, we continue the study of quasi-cyclic codes cancelled by polynomials with matricial coefficients presented in [2]. We study the factorisation of polynomials in $M_\ell(\mathbb{F}_q)[X]$ and recall results from the scalar case which can be generalised. Then we deal with the particular case of $X^m - 1$ by giving results on its roots and its factorisations. This latter is easier by using the identification between $M_\ell(\mathbb{F}_q)[X]$ and $M_\ell(\mathbb{F}_q[X])$. This leads to a practicable way to construct such 2-quasi-cyclic codes and then 2-quasi-cyclic Euclidean selfdual codes. Most of found codes meet the best bounds for minimum distances. According to the tables in [7], two codes beat the best known minimum distances: $[30, 22, 6]_{\mathbb{F}_4}$ and $[29, 21, 6]_{\mathbb{F}_4}$.

2 Quasi-cyclic codes cancelled by polynomials with matricial coefficients

A generalisation of cyclic codes with a polynomial representation was given in [2] for quasi-cyclic codes. However, unlike cyclic codes which are ideals of polynomials, quasi-cyclic codes are linear subspaces cancelled by polynomials with matricial coefficients. Indeed, for any $m \in \mathbb{N}^*$, there is an action of $M_\ell(\mathbb{F}_q)[X]$ on $\mathbb{F}_q^{m\ell}$ as following: (where T is the circular shift)

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

Definition 1 *Let $P \in M_\ell(\mathbb{F}_q)[X]$. We note $\Omega(P) = \{c \in \mathbb{F}_q^{m\ell} \quad | \quad P * c = 0\}$. The code $\Omega(P)$ is ℓ-quasi-cyclic if $P(X)$ divides $X^m - 1$.*

Proposition 1 *Let $P, Q \in M_\ell(\mathbb{F}_q)[X]$ be monic polynomials such that $X^m - 1 = P(X).Q(X)$. Then $dim(\Omega(P)) = \ell \deg(P)$ and*

$$G_{\Omega(P)} = \begin{pmatrix} {}^tQ_0 & {}^tQ_1 & {}^tQ_2 & \cdots & {}^tQ_{\deg(Q)} & 0 & 0 & \cdots & 0 \\ 0 & {}^tQ_0 & {}^tQ_1 & \cdots & {}^tQ_{\deg(Q)-1} & {}^tQ_{\deg(Q)} & 0 & \cdots & 0 \\ & & \ddots & & & & \ddots & & \end{pmatrix}$$

is a generator matrix of $\Omega(P)$.

Remark 1 *Note that the code $\Omega(P)$ can be represented only by the coefficients of P (or Q depending on which of them has the smallest degree). It is smaller than the key reduction for general quasi-cyclic codes anyway.*

Now, it is obvious that the construction of such codes depends strongly on the factorisation of $X^m - 1$ in $M_\ell(\mathbb{F}_q)[X]$. In the next section, we study first the general factorisation in this ring.

3 Factorisation in $M_\ell(\mathbb{F}_q)[X]$

The ring $M_\ell(\mathbb{F}_q)[X]$ is neither integral nor commutative, however one can still define an Euclidean division in the following case:

Proposition 2 *Let $P, S \in M_\ell(\mathbb{F}_q)[X]$. Let us assume that S is monic. Then, there exist unique $Q_r, R_r, Q_l, R_l \in M_\ell(\mathbb{F}_q)[X]$ such that:*

$$P = Q_r S + R_r \quad \textit{with } \deg(R_r) < \deg(S). \textit{ (Right division)}$$

$$P = S Q_l + R_l \quad \textit{with } \deg(R_l) < \deg(S). \textit{ (Left division)}$$

Remark 2 *The quotients and remainders obtained may be different between the right and left divisions.*

$$P(X) = X^3 + \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} X^2 + \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \quad S(X) = X + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \in M_2(\mathbb{F}_2)[X].$$
$$Q_r(X) = X^2 + \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} X \textit{ and } Q_l(X) = X^2 + \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} X + \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$
$$R_r(X) = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \textit{ and } R_l(X) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Unlike general polynomials, the indeterminate X commutes with every coefficients in $M_\ell(\mathbb{F}_q)[X]$ and more generally:

Proposition 3 *The center of $M_\ell(\mathbb{F}_q)[X]$ is exactly $\mathbb{F}_q[X]$.*

Hence, we can define right and left evaluations as following:

Definition 2 *Let $P(X) = \sum_{i=0}^{\deg(P)} P_i X^i \in M_\ell(\mathbb{F}_q)[X]$ and $A \in M_\ell(\mathbb{F}_q)$.*

- *The right evaluation of P in A is: $P(A)_r := \sum_{0 \le i \le \deg(P)} P_i A^i$.*
- *The left evaluation of P in A is: $P(A)_l := \sum_{0 \le i \le \deg(P)} A^i P_i$.*
- *A is a right root of P if $P(A)_r = 0$.*
- *A is a left root of P if $P(A)_l = 0$.*
- *Right and left concepts are the same if P is central.*

The evaluation of products of polynomials behaves as following:

Proposition 4 *Let $P, Q \in M_\ell(\mathbb{F}_q)[X]$ defined by*
$P(X) = \sum_{i=0}^{\deg(P)} P_i X^i$ *and* $Q(X) = \sum_{i=0}^{\deg(Q)} Q_i X^i$. *If $A \in M_\ell(\mathbb{F}_q)$, we define:*
$P_{Q,A,r}(X) = \sum_{i=0}^{\deg(P)} P_i Q(A)_r X^i$ *and* $Q_{P,A,\ell}(X) = \sum_{i=0}^{\deg(Q)} X^i P(A)_\ell Q_i$.

Then $(PQ)(A)_r = P_{Q,A,r}(A)_r$ and $(PQ)(A)_\ell = Q_{P,A,\ell}(A)_\ell$.

Corollary 1 *With the previous notations,*

- *If A is a right root of Q, then A is a right root of PQ.*
- *If A is a left root of P, then A is a left root of PQ.*

As in the scalar case, we have a bond between roots and divisibility by $(X - A)$.

Proposition 5 *Let $P(X) = \sum_{i=0}^{\deg(P)} P_i X^i \in M_\ell(\mathbb{F}_q)[X]$ and $A \in M_\ell(\mathbb{F}_q)$.*

- *A is a right root of $P \iff \exists\, Q \in M_\ell(\mathbb{F}_q)[X]$ such that $P(X) = Q(X) * (X - A)$*
- *A is a left root of $P \iff \exists\, Q \in M_\ell(\mathbb{F}_q)[X]$ such that $P(X) = (X - A) * Q(X)$.*

Proof. Let us assume that A is a right root of P. We want to prove that $\exists\, Q \in M_\ell(\mathbb{F}_q)[X]$ such that $P(X) = Q(X) * (X - A)$.
The polynomial $(X - A)$ is monic, then there exist $Q, R \in M_\ell(\mathbb{F}_q)[X]$ such that $P(X) = Q(X) * (X - A) + R(X)$ with $\deg(R) < 1$. Then R is a constant.
Hence $P(A)_r = (Q * (X - A))(A)_r + R(A)_r$.
However $P(A)_r = 0$ since A is a right root of P. And thanks to Corollary 1, $(Q(X) * (X - A))(A)_r = 0$ since $(X - A)(A)_r = 0$. Then $R(A)_r = 0$ and R is a constant, obviously $R(X) = 0$ and

$$P(X) = Q(X) * (X - A).$$

Now, assume that $\exists\, Q \in M_\ell(\mathbb{F}_q)[X]$ such that $P(X) = Q(X) * (X - A)$. We want to prove that A is a right root of P.
If $P(X) = Q(X) * (X - A)$, since A is obviously a right root of $(X - A)$, from Corollary 1 again,

$$P(A)_r = 0.$$

The proof is similar for the left root.

Mostly, factors do not commute with the others. However, when the dividend is central, we have the following results:

Proposition 6 *Let $P, Q, R \in M_\ell(\mathbb{F}_q)[X]$. Suppose that P is a central polynomial and that Q and R are monic. Then:*

$$P = Q.R \quad \iff \quad P = R.Q.$$

Proof.
$P = Q.R \Rightarrow R.P = R.Q.R$
$\Rightarrow P.R = (R.Q).R$ since P is central

Since R is monic, there is a unique quotient in the Euclidean division of $P.R$ by R and then $P = R.Q$.
The proof is similar for the other way.

Corollary 2 *Let $P, P_1, \ldots, P_n \in M_\ell(\mathbb{F}_q)[X]$. Suppose that P is a central polynomial and that $P_1, \ldots, P_n$ are monic. Then:*

$$P = P_1.P_2 \ldots P_n \Longleftrightarrow P = P_2.P_3 \ldots P_1 \Longleftrightarrow \cdots \Longleftrightarrow P = P_n.P_1 \ldots P_{n-1}$$

Example 1 *In $M_2(\mathbb{F}_4)[X]$ where $\mathbb{F}_4 = \mathbb{F}_2[\omega]$,*

$$X^3 - 1 = (X-A)(X-B)(X-C) = (X-B)(X-C)(X-A) = (X-C)(X-A)(X-B).$$

where $A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & \omega^2 \\ 1 & \omega \end{pmatrix}$ *and* $C = \begin{pmatrix} 1 & \omega \\ 0 & \omega \end{pmatrix}$.

4 Roots of $X^m - 1$

In this section we deal with the factorisation of $X^m - 1$ in $M_\ell(\mathbb{F}_q)[X]$ and more particularly with its roots. There roots are basically an extension of the roots of unity over $\mathbb{F}_q$ as shown above.

Proposition 7 *Let $A \in M_\ell(\mathbb{F}_q)$ be a root of $X^m - 1$. Then the eigenvalues of A are m-th roots of unity over $\mathbb{F}_q$.*

Remark 3 *The number of roots is much larger than in the scalar case.*
For instance, consider $P(X) = X^3 - 1 \in M_2(\mathbb{F}_4)[X]$. $\mathbb{F}_4 = \mathbb{F}_2[\omega]$.

- *In the scalar case, there are 3 roots $\{1, \omega, \omega^2\}$.*
- *In $M_2(\mathbb{F}_4)$, there are 63 roots such as:*

Eigenvalues	$(1,\omega)$	$(1,\omega^2)$	(ω,ω^2)	$(1,1)$	(ω,ω)	(ω^2,ω^2)
Number of roots	*20*	*20*	*20*	*1*	*1*	*1*

- *In $M_2(\mathbb{F}_{16})$, there are 819 roots.*
- *In $M_2(\mathbb{F}_{64})$, there are 12483 roots.*

These roots were found by exhaustive search using Magma.

Remark 4 *A complete factorisation of $X^m - 1$ is obtained by a multiplication of factors of the form $(X - A)$ (where A is a root of $X^m - 1$) such that the set of all the eigenvalues of the used roots is exactly the whole set of the m-th roots of unity each with multiplicity ℓ. However, they need to be multiplied in the right order and some of these combinations of roots do not give a factorisation either. Some example and counterexample are following:*

Consider $P(X) = X^3 - 1 \in M_2(\mathbb{F}_4)[X]$. $\mathbb{F}_4 = \mathbb{F}_2[\omega]$. The roots $\left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & \omega^2 \\ 1 & \omega \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & \omega \\ 0 & \omega \end{smallmatrix}\right)$ have respectively eigenvalues (ω, ω^2), $(1, \omega^2)$ and $(1, \omega)$.

$$\left(X - \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)\right)\left(X - \left(\begin{smallmatrix} 0 & \omega^2 \\ 1 & \omega \end{smallmatrix}\right)\right)\left(X - \left(\begin{smallmatrix} 1 & \omega \\ 0 & \omega \end{smallmatrix}\right)\right) = X^3 - 1.$$

But $\left(X - \left(\begin{smallmatrix} 0 & \omega^2 \\ 1 & \omega \end{smallmatrix}\right)\right)\left(X - \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)\right)\left(X - \left(\begin{smallmatrix} 1 & \omega \\ 0 & \omega \end{smallmatrix}\right)\right) = X^3 + \left(\begin{smallmatrix} \omega & 1 \\ \omega^2 & \omega \end{smallmatrix}\right) X + \left(\begin{smallmatrix} \omega^2 & 1 \\ \omega^2 & \omega^2 \end{smallmatrix}\right) \neq X^3 - 1.$

The number of roots is incredibly large even for small degree polynomials. Moreover so far, finding a complete factorisation requires an exhaustive search on the combinations of roots which is intractable even for small degrees. However, factorising in the ring of matrices with polynomial coefficients seems easier. Results are presented in the following section.

5 Factorisation of $X^m - 1$

From now on, we note I_ℓ the identity matrix of size $\ell \times \ell$ and $Adj(A)$ the adjugate matrix of A (the transpose of the matrix of cofactors).

In order to factorise $X^m - 1$, we consider the following identification:

$$\begin{aligned} \varphi : \ M_\ell(\mathbb{F}_q)[X] &\longrightarrow M_\ell(\mathbb{F}_q[X]) \\ \sum_{i=0}^{\deg(P)} P_i X^i &\longmapsto \left(\sum_{i=0}^{\deg(P)} (P_i)_{a,b} X^i \right)_{1 \le a,b \le \ell} \end{aligned}$$

Since φ is a ring isomorphism, factorising $X^m - 1$ in both rings is similar and from now on, we use both representations.

Remark 5 *Let $A, B \in M_\ell(\mathbb{F}_q[X])$ such that $(X^m - 1).I_\ell = A.B$. Hence*

$$\det(A) \text{ and } \det(B) \text{ both divide } (X^m - 1)^\ell.$$

Proposition 8 *Let $A \in M_\ell(\mathbb{F}_q[X])$ be a matrix whose determinant divides $(X^m - 1)^\ell$. We have:*

$$(X^m - 1).I_\ell = A.B \quad \text{with } B = Adj(A)\tfrac{X^m - 1}{\det(A)} \in M_\ell(\mathbb{F}_q(X)).$$

Proof. $A.Adj(A)\frac{X^m-1}{\det(A)} = \det(A).I_\ell \frac{X^m-1}{\det(A)} = (X^m - 1).I_\ell$.

Note that the coefficients of B are not necessarily polynomials (they may be ratios of polynomials). However the following proposition gives a sufficient condition for B to be polynomial.

Proposition 9 *Let $A \in M_\ell(\mathbb{F}_q[X])$ with determinant dividing $(X^m - 1)^\ell$. Then:*

$$\frac{\det(A)}{\gcd(\det(A), X^m - 1)} \text{ divides all the coefficients of } Adj(A)$$

$$\Updownarrow$$

$$\text{The matrix } B = Adj(A)\frac{X^m - 1}{\det(A)} \text{ verifies } (X^m - 1).I_\ell = A.B \text{ and } B \in M_\ell(\mathbb{F}_q[X]).$$

Proof. Since A is polynomial, so does $Adj(A)$. Hence, the dividing assumption is meaningful. Thus, one deduces that there exists $C \in M_\ell(\mathbb{F}_q[X])$ such that

$$Adj(A) = \frac{\det(A)}{\gcd(\det(A), X^m - 1)} C.$$

Hence, $B = \frac{X^m-1}{\det(A)} \frac{\det(A)}{\gcd(\det(A), X^m-1)} C = \frac{X^m-1}{\gcd(\det(A), X^m-1)} C$.

Obviously, $\frac{X^m-1}{\gcd(\det(A), X^m-1)}$ is a polynomial, so is B.

The other way is now obvious.

Remark 6 *Note that all these previous results hold if we consider any central polynomial instead of* $X^m - 1$.

This condition on the comatrix is difficult to use in the general case. Nevertheless, when $\ell = 2$ it becomes easier.

6 Construction of 2-quasi-cyclic codes

In this section, we consider only matrices of size 2×2.
Let $A = \begin{pmatrix} a(X) & b(X) \\ c(X) & d(X) \end{pmatrix} \in M_2(\mathbb{F}_q[X])$. Then $Adj(A) = \begin{pmatrix} d(X) & -b(X) \\ -c(X) & a(X) \end{pmatrix}$ and

$$\begin{aligned} &\frac{\det(A)}{\gcd(\det(A), X^m-1)} \text{ divides all the coefficients of } Adj(A) \\ \Longleftrightarrow\ &\frac{\det(A)}{\gcd(\det(A), X^m-1)} \text{ divides all the coefficients of } A. \end{aligned}$$

Then we have a more conveninent form of *Proposition 9*:

Proposition 10 *Let* $A \in M_2(\mathbb{F}_q[X])$ *with determinant dividing* $(X^m-1)^2$. *Then*

$$\frac{\det(A)}{\gcd(\det(A), X^m-1)} \textit{ divides all the coefficients of } A$$
$$\Updownarrow$$
The matrix $B = Adj(A)\frac{X^m-1}{\det(A)}$ *verifies* $(X^m - 1).I_2 = A.B$ *and* $B \in M_2(\mathbb{F}_q[X])$.

In order to factorise $X^m - 1$ with polynomials with matricial coefficients, we will search for matrices verifying the conditions of the latter proposition. In this case,

$$A = \frac{\det(A)}{\gcd(\det(A), X^m - 1)} A' \text{ with } \det(A') = \frac{(\gcd(\det(A), X^m - 1))^2}{\det(A)}.$$

Proposition 11 *In these conditions,* $\det(A')$ *and* $\frac{\det(A)}{\gcd(\det(A), X^m-1)}$ *divide* $X^m - 1$.

Proof. Since $\det(A)$ divides $(X^m - 1)^2$, there exists a polynomial $P(X)$ such that
$\det(A) = \gcd(\det(A), X^m - 1) * P$ and P divides $\gcd(\det(A), X^m - 1)$. Hence $\det(A')$ is a polynomial as well.

Then $\det(A') = \frac{(\gcd(\det(A), X^m-1))^2}{\det(A)}$ divides
$\frac{\det(A) * \gcd(\det(A), X^m-1)}{\det(A)} = \gcd(\det(A), X^m - 1)$. Hence $\det(A')$ divides $X^m - 1$.

It is obvious that $\frac{\det(A)}{\gcd(\det(A), X^m-1)}$ is a polynomial and divides $X^m - 1$.

From these results, we have the following theorem:

Theorem 1 *All factors of $X^m - 1$ in $M_2(\mathbb{F}_q[X])$ are of the form $P(X) * A'$ with $P(X)$ and $\det(A')$ dividing $X^m - 1$. Furthermore $P(X)$ and $\det(A')$ are relatively prime.*

Remark 7 *In order to construct $\Omega(P)$-codes, we need monic factors of $X^m - 1$. Thus, we need to find matrices A' of the form*

$$A' = \begin{pmatrix} X^n + a(X) & b(X) \\ c(X) & X^n + d(X) \end{pmatrix} \text{ with } \deg(a), \deg(b), \deg(c), \deg(d) \leq n - 1.$$

Note that $\det(A')$ the determinant of such a matrix is of even degree $2n$.

Remark 8 *Suppose that m and q are relatively prime. Let A be a factor of $X^m - 1 \in M_\ell(\mathbb{F}_q[X])$ with a fixed determinant. According to previous theorem, $A = P(X) * A'$ and*

- *$\det(A')$ is the product of the factors of $\det(A)$ having multiplicity 1.*
- *$P(X)$ is the product of the factors of $\det(A)$ having multiplicity 2.*

Example 2 *Consider the case of 2-quasi-cyclic codes of length 22 over $\mathbb{F}_4$. Let $\mathbb{F}_4 = \mathbb{F}_2[\omega]$. In $\mathbb{F}_4[Y]$,*

$$\begin{aligned} Y^{11} - 1 &= \underbrace{(Y+1)}_{P_1(Y)} \underbrace{(Y^5 + \omega Y^4 + Y^3 + Y^2 + \omega^2 Y + 1)}_{P_2(Y)} \underbrace{(X^5 + \omega^2 Y^4 + Y^3 + Y^2 + \omega Y + 1)}_{P_3(Y)} \end{aligned}$$

In order to find all the monic factors of $X^{11} - 1$ in $M_2(\mathbb{F}_4)[X]$, according to Theorem 1, we have to consider matrices A' such that $\det(A')$ divides $X^{11} - 1$ with even degree. The only possibilities for $\det(A')$ are then 1 of degree 0, P_1P_2, P_1P_3 of degree 6 and P_2P_3 of degree 10. Hence we obtain the following table of values where the bounds were taken from the tables in [7]:

Dimension	2	4	6	8	10	12	14	16	18	20
Bounds on minimum distance	17	15	12-13	11	9	7-8	6	4-5	3	2
Best minimum distance found	11		12		9	7		4		2
Number of determinants	1	0	2	0	3	3	0	2	0	1
Number of codes	1	0	15360	0	1576962	1576962	0	15360	0	1

Table 1. Quasi-cyclic codes of length 22 over $\mathbb{F}_4$.

These codes were obtained in Magma using previous tricks.

Example 3 *Consider the case of 2-quasi-cyclic codes of length 30 over $\mathbb{F}_4$. Let $\mathbb{F}_4 = \mathbb{F}_2[\omega]$.*
The polynomial

$$\begin{aligned} P(X) = X^{11} &+ \begin{pmatrix} 0 & \omega^2 \\ 1 & 1 \end{pmatrix} X^{10} + \begin{pmatrix} \omega & \omega^2 \\ 0 & 1 \end{pmatrix} X^9 + \begin{pmatrix} 1 & \omega^2 \\ \omega & \omega^2 \end{pmatrix} X^8 + \begin{pmatrix} \omega^2 & \omega^2 \\ \omega^2 & 0 \end{pmatrix} X^7 + \begin{pmatrix} \omega^2 & \omega^2 \\ \omega & 0 \end{pmatrix} X^6 \\ &+ \begin{pmatrix} \omega^2 & \omega \\ 0 & 0 \end{pmatrix} X^5 + \begin{pmatrix} \omega & \omega^2 \\ \omega & \omega^2 \end{pmatrix} X^4 + \begin{pmatrix} \omega^2 & 1 \\ \omega^2 & \omega \end{pmatrix} X^3 + \begin{pmatrix} \omega & \omega \\ \omega & 1 \end{pmatrix} X^2 + \begin{pmatrix} \omega^2 & \omega \\ 0 & \omega^2 \end{pmatrix} X + \begin{pmatrix} 1 & \omega^2 \\ 1 & 1 \end{pmatrix} \end{aligned}$$

divides $X^{15} - 1$. And $\Omega(P)$ has parameters $[30, 22, 6]_{\mathbb{F}_4}$ which beats the previous known bound on the minimum distance according to the tables of linear codes in [7]. Shorten codes of $\Omega(P)$ all give codes with parameters $[29, 21, 6]_{\mathbb{F}_4}$ which beat the previous known bound as well.

Example 4 *In previous constructions of $\Omega(P)$-codes, we got interested in monic factors of $X^m - 1$. This implies that the sum of the degrees of the factors is equal to m. However, it is possible to find factorisations that do not respect this condition. That happens, for instance, as in the following example:*

Let $m = 5, \ell = 2, q = 2$. We have the following factorisations:

$$X^5 - 1 = \left(\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} X^4 + \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} X^3 + \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} X^2 + \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} X + \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\right)$$
$$* \left(\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} X^3 + \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} X^2 + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} X + \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\right) = P(X).Q(X).$$

$$\textit{But } P(X) = \left(X^3 + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} X^2 + \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} X + \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\right)\left(\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} X + \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right) = P'(X).U(X).$$

$$\textit{and } Q(X) = \left(\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} X + \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right)\left(X^2 + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} X + \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\right) = U(X).Q'(X).$$

Moreover, $U^2 = I_2$ and $X^5 - 1 = P'(X).Q'(X)$ with P' and Q' monic. Concerning quasi-cyclic codes cancelled by those polynomials, we have the following relations: $\Omega(P) = \Omega(P')$ and $\Omega(Q) = \Omega(Q')$.

7 Construction of 2-quasi-cyclic Euclidean selfdual codes

A code C is said selfdual if it is equal to its own dual ($C = C^{\perp}$). However, for $\Omega(P)$-codes, we have the following result:

Theorem 2 *[2] Let $P, Q \in M_\ell(\mathbb{F}_q)[X]$ be monic polynomials such that $X^m - 1 = P(X).Q(X)$. Then $\Omega(P)^{\perp} = \Omega({}^tQ^*)$.*
(where all the coefficients of Q are transposed, and Q^* means the reciprocal polynomial of Q)

Hence, with these conditions, selfduality is equivalent to $\Omega(P) = \Omega({}^tQ^*)$ or yet $P = {}^tQ^*$.

In the matrix representation, if we note $A = \begin{pmatrix} a(X) & b(X) \\ c(X) & d(X) \end{pmatrix}$ and B the matrices corresponding respectively to P and Q, we have

$$(1) \quad B = \begin{pmatrix} a^*(X) & c^*(X) \\ b^*(X) & d^*(X) \end{pmatrix} \quad \text{since } Q = {}^tP^*.$$

Moreover, as shown in the previous section,

$$(2) \quad B = \frac{X^m - 1}{\det(A)} Adj(A) = \frac{X^m - 1}{\det(A)} \begin{pmatrix} d(X) & -b(X) \\ -c(X) & a(X) \end{pmatrix}.$$

However, from (1), A and B have the same degree. Hence

$$\det(A) = X^m - 1 \text{ and } \begin{cases} d(X) = a^*(X) \\ c(X) = -b^*(X) \end{cases}.$$

Example 5 *In the following tables are represented the best minimum distances found with our construction, compared to minimal bounds found in [6]. For small lengths an exhaustive search is performed on $a(X)$ and $b(X)$. For larger lengths, a random search is performed. These results were obtained with Magma.*

Length	8	12	16	20	24	28	32	36	40	44	48	52	$\cdots$	76
Minimal bound	4	6	6	8	8	9	11	11	12	14	14	14		18
Best minimum distance found	**4**	4	**6**	7	**8**	**9**	10	**11**	**12**	**14**	**14**	**14**		**18**

Table 2. Best minimum distances for Euclidean $\Omega(P)$-2-quasi-cyclic codes over $\mathbb{F}_4$.

Length	8	12	16	20	24	28	32	36	40
Minimal bound	5	6	7	8	10	11	12	13	14
Best minimum distance found	4	4	**7**	**8**	**10**	**11**	**12**	**13**	**14**

Table 3. Best minimum distances for Euclidean $\Omega(P)$-2-quasi-cyclic codes over $\mathbb{F}_8$.

We notice that in most cases (represented in bold), the best known minimum distances are reached.

8 Conclusion

In this paper we dealt with the factorisation of polynomials in $M_\ell(\mathbb{F}_q)[X]$. This led to a practical computation of monic factors of $X^m - 1$ and then quasi-cyclic codes. These constructions gave codes mostly reaching the best known minimum distances. Moreover, we found two new codes with parameters better than known $[30, 22, 6]_{\mathbb{F}_4}$ and $[29, 21, 6]_{\mathbb{F}_4}$.

References

1. T. P. Berger, P.-L. Cayrel, P. Gaborit and A. Otmani. "Reducing Key Length of the McEliece Cryptosystem." In Bart Preneel, editor, *Progress in Cryptology - Second International Conference on Cryptology in Africa (AFRICACRYPT 2009)*, volume 5580 of *Lecture Notes in Computer Science*, pages 77-97, Gammarth, Tunisia, June 21-25 2009.
2. P.-L. Cayrel, C. Chabot and A. Necer, "Quasi-cyclic codes as codes over rings of matrices." In *Finite Fields and Their Applications* Vol. 16, 2010, pp 100-115.
3. J.C. Faugère, A. Otmani, L. Perret, J.P. Tillich, "Algebraic Cryptanalysis of McEliece Variants with Compact Keys." In *Proceedings of the 29th International Conference on Cryptology - EUROCRYPT 2010*, Nice, France, May 30-June 03 2010.
4. P. Fitzpatrick and K. Lally, "Algebraic structure of quasi-cyclic codes." In *Disc. Appl. Math.*, 111(2001), pp 157–175.
5. P. Gaborit, "Shorter keys for code based cryptography." In *Proceedings of the 2005 International Workshop on Coding and Cryptography (WCC 2005)*, pages 81-91, Bergen, Norway, March 2005.
6. M. Grassl and T. A. Gulliver, "On circulant self-dual codes over small fields." In *Designs, Codes and Cryptography* Volume 52 Issue 1, July 2009.
7. M. Grassl, "Tables of linear codes and quantum codes", http://www.codetables.de.
8. S. Ling and P. Solé, "On the algebraic structure of quasi-cyclic codes I: finite fields." In *IEEE Transactions on Information Theory*, 47, 2751-2760, 2001.
9. R.J. McEliece, "A public-key cryptosystem based on algebraic coding theory", *JPLDSN Progress Report*, pages 114-116, 1978.
10. A. Otmani, J.P. Tillich and L. Dallot, "Cryptanalysis of Two McEliece Cryptosystems Based on Quasi-Cyclic Codes." In *Special issues in Symbolic Computation and Cryptography, Mathematics in Computer Science*, vol. 3, number 2, January 2010, pp. 129-140.