Quasi-cyclic codes as codes over rings of matrices

Pierre-Louis Cayrel[a], Christophe Chabot[1], Abdelkader Necer[1]

[a] *Center for Advanced Security Research Darmstadt*
Mornewegstrasse, 32
64293 Darmstadt
Germany
[b] *Université de Limoges, XLIM-DMI,*
123, Av. Albert Thomas
87060 Limoges Cedex, France

Abstract

Quasi cyclic codes over a finite field are viewed as cyclic codes over a non commutative ring of matrices over a finite field. This point of view permits to generalize some known results about linear recurring sequences and to propose a new construction of some quasi cyclic codes and self dual codes.

1. Introduction

Let p be a prime number, $r \in \mathbb{N}$, $q = p^r$ and $\mathbb{F}_q$ the Galois field with q elements.
Let $n \in \mathbb{N}$. As usual, we define the shift map from $\mathbb{F}_q^n$ to $\mathbb{F}_q^n$ denoted T by:

$$\forall c = (c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_q^n, \quad Tc = (c_{n-1}, c_0, \ldots, c_{n-2}). \tag{1}$$

Let $\mathcal{C}$ be a code of length n over $\mathbb{F}_q$. Let $\ell \in \mathbb{N}^*$. We say that $\mathcal{C}$ is a quasi-cyclic code of index ℓ over $\mathbb{F}_q$ if $T^\ell \mathcal{C} = \mathcal{C}$ (if $\ell = 1$, $\mathcal{C}$ is cyclic). It is well known that ℓ divides n. In the sequel, we write $n = m\ell$.

Quasi-cyclic codes are well-known and studied since the 60's. We can find, for example in [5] an introduction to their applications, their interests and a good bibliography about this subject. Since the articles of J. Conan and G. Séguin in 1993 (see [2]) for the algebraic structure of quasi-cyclic codes and their enumeration, many authors have proposed different approaches to describe this structure and to propose different constructions.
For example in [10] codes are considered as concatenated codes. In [3] the authors consider a quasi-cyclic code of index ℓ over $\mathbb{F}_q$ as a sub-module of the quotient ring of $\mathbb{F}_{q^\ell}[X]$ by the ideal generated by the polynomial $X^m - 1$ which permits to give a complete classification of self-dual codes of index 2. In [5] and [6], the authors consider the quasi-cyclic codes as linear codes over a commutative ring and use the canonical decomposition of $\mathbb{F}_{q^\ell}[X]/(X^m - 1)$ to study the structure of quasi-cyclic codes and so deduce the construction of codes of this type.

In this article we propose a new approach. We consider quasi-cyclic codes as cyclic codes over a ring of matrices over $\mathbb{F}_q$.

Let $\mathbb{A} = \mathbb{F}_q^\ell$. For $v = (v_0, \ldots, v_{\ell-1})$ a row vector of $\mathbb{A}$, we design by ${}^t(v_0, \ldots, v_{\ell-1})$ the corresponding column vector.

We consider the isomorphism (of vector spaces) Θ of $\mathbb{F}_q^n$ in $\mathbb{A}^m$ given by:

$$\forall c = (c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_q^n, \qquad \Theta c = ({}^t(c_0, \ldots, c_{\ell-1}), {}^t(c_\ell, \ldots, c_{2\ell-1}), \ldots, {}^t(c_{(m-1)\ell}, \ldots, c_{m\ell-1})).$$

Email addresses: cayrelpierrelouis@gmail.com (Pierre-Louis Cayrel), christophe.chabot@unilim.fr (Christophe Chabot), abdelkader.necer@unilim.fr (Abdelkader Necer)

We extend the shift map defined above (equation (1)) to $\mathbb{A}^m$ by:

$$\forall v = ({}^t v_0, \ldots, {}^t v_{m-1}) \in \mathbb{A}^m, \quad Tv = ({}^t v_{m-1}, {}^t v_0, \ldots, {}^t v_{m-2}).$$

So, it easy to see that for a given code $\mathcal{C}$ of length n over $\mathbb{F}_q$, $\mathcal{C}$ is a quasi-cyclic code of index ℓ over $\mathbb{F}_q$ if and only if $\Theta(\mathcal{C})$ is a cyclic code over $\mathbb{A}$.

As $\Theta(\mathcal{C})$ is composed of words of *vectors*, the matricial formalism is a natural interpretation. We will deal with $\Theta(\mathcal{C})$ (identified with $\mathcal{C}$) as a code over $\mathbb{F}_q$ (classical approach) and over $\mathbb{M}_\ell(\mathbb{F}_q)$ the non commutative ring of $\ell \times \ell$ matrices with coefficients in $\mathbb{F}_q$.

By identifying the shift with the indeterminate X, we define over $\Theta(\mathcal{C})$ a structure of left module over the algebra $\mathbb{M}_\ell(\mathbb{F}_q)[X]$ of the polynomials with matricial coefficients. This permits first, to see a quasi-cyclic code as a cyclic code over $\mathbb{M}_\ell(\mathbb{F}_q)$ and secondly, to describe the quasi-cyclic codes for which the *annihilator* is generated by a single matricial polynomial. Finally it gives a new construction of self-dual codes (Euclidean or Hermitian).

The correspondence between linear recurring sequences over a finite field (sequences generated by a linear feedback shift register) and cyclic codes is well known. The characteristic polynomial of a linear recurring sequence u of period $L \in \mathbb{N}^*$ is, up to reciprocation, the quotient of the polynomial $X^L - 1$ by the generator polynomial of the cyclic code corresponding to u. One of the main results of this article is to generalize this correspondence to the case of linear recurring sequences over a ring of matrices.

In the first section we deal with linear recurring sequences over the ring $\mathbb{M}_\ell(\mathbb{F}_q)$. This "point of view" is not new : we can find in [9] an application of these sequences to the generation of pseudo-random numbers. However we show in this part directly (it's a new construction to our knowledge) the existence of the exponent for a polynomial with matricial coefficients.

In the second section of this article, after the definition of the structure of $\mathbb{M}_\ell(\mathbb{F}_q)[X]/(X^m - 1)$ as left module over $\mathbb{A}^m$, we present some results on the families of $(\mathbb{F}_q^\ell)^m$ cancelled by matricial polynomials of $\mathbb{M}_\ell(\mathbb{F}_q)[X]/(X^m - 1)$. And then we deal with the opposite problem which is, given a subset C of $(\mathbb{F}_q^\ell)^m$, to determine the ideal of $\mathbb{M}_\ell(\mathbb{F}_q)[X]/(X^m - 1)$ formed by the polynomials cancelling C.

The last section is devoted to the construction of new quasi-cyclic codes and self-dual Euclidean codes (and Hermitian over $\mathbb{F}_4$). Our construction permits to find, for instance, new self-dual Euclidean codes with parameters $[28, 14, 9]$ over $\mathbb{F}_4$.

This construction is essentially based on the result which generalizes the one announced above for the linear recurring sequences: if $X^m - 1 = fg$ in $\mathbb{M}_\ell(\mathbb{F}_q)[X]/(X^m - 1)$, so the dual (Euclidean or Hermitian) of the family of the vectors of $(\mathbb{F}_q^\ell)^m$ cancelled by f is a family of vectors cancelled by a completely determined polynomial.

2. Linear recurring sequences with matricial coefficients

Let $\mathbb{A} = \mathbb{F}_q^\ell$ and $S(\mathbb{A}) = \mathbb{A}^{\mathbb{N}}$ be the set of sequences of $\mathbb{A}$. In this section, after setting over $S(\mathbb{A})$ a structure of left module on the ring of polynomials with coefficients in $\mathbb{M}_\ell(\mathbb{F}_q)$, we will show *directly* that any polynomial (reversible) with coefficients in this ring has an exponent. Therefore each linear recurring sequence with matricial coefficients is periodic and we give the dimension of the associated cyclic code.

Let $v = (v(n))_{n \geq 0}$ in $S(\mathbb{A})$. We define the sequence Tv by: $\forall n \in \mathbb{N}, Tv(n) = v(n+1)$. This morphism of vector spaces will allow us to provide $S(\mathbb{A})$ with a multiplication by the elements of $\mathbb{M}_\ell(\mathbb{F}_q)[X]$ by setting:

$$\forall p \in \mathbb{M}_\ell(\mathbb{F}_q)[X], \quad \forall v \in S(\mathbb{A}), \quad p(X)v = p(T)v.$$

Example 2.1. *For $\ell = 2$ and $p(X) = A.X + B$ where $A = (a_{i,j})_{1\leq i,j\leq 2}$ and $B = (b_{i,j})_{1\leq i,j\leq 2}$ are two 2×2 matrices and for $(v(n))_n =^t (v_1(n)_n, v_2(n)_n)$, if we let $p.v =^t (w_1, w_2)$ then:*

$$\begin{array}{rcl} \forall n \in \mathbb{N}, \quad w_1(n) & = & a_{11}v_1(n+1) + a_{12}v_2(n+1) + b_{11}v_1(n) + b_{12}v_2(n) \\ w_2(n) & = & a_{21}v_1(n+1) + a_{22}v_2(n+1) + b_{21}v_1(n) + b_{22}v_2(n). \end{array}$$

We can easily check that we obtain the next proposition.

Proposition 1.
With the notation above, $S(\mathbb{A})$ provided with the usual operations and multiplication by a matrix polynomial is an $\mathbb{M}_\ell(\mathbb{F}_q)[X]$-left module.

Definition 1. *Let $v \in S(\mathbb{A})$. We say that v is a linear recurring sequence (with matricial coefficients) if its annihilator in $\mathbb{M}_\ell(\mathbb{F}_q)[X]$ contains a monic polynomial.*

Remark 2.1.
1. *It has been shown (see* [7] *or* [9]*) that a sequence over $\mathbb{A}$ is a linear recurring sequence if and only if the scalar components sequences are linear recurring sequences over $\mathbb{F}_q$. The computation of the period of each of this sequences permits to find the period of the sequence of vectors. However we will give a direct proof of this result via the computation of the exponent of a matrix polynomial.*

2. *The annihilator of a linear recurring sequence, unlike in the classical case $\ell = 1$, is not a principal ideal (left or right). However, we can say something about this ideal in some cases.*

Definition 2.
We call a polynomial $f \in \mathbb{M}_\ell(\mathbb{F}_q)[X]$ reversible if its leading and constant coefficients are invertible matrices.

We can now give the following proposition.

Proposition 2.
Let $f \in \mathbb{M}_\ell(\mathbb{F}_q)[X]$. We suppose that f is reversible. Then, there exists $e \in \mathbb{N}^*$ such that $f|(X^e - 1)$.

Proof
We can suppose without loss of generality that f is monic.

Consider the sequence $(X^n)_{n\in\mathbb{N}}$. The quotient set $\mathbb{M}_\ell(\mathbb{F}_q)[X]/f\mathbb{M}_\ell(\mathbb{F}_q)[X]$ has a particular structure of module and of $\mathbb{F}_q$-vector space. Moreover, it is an $\mathbb{F}_q$-vector space of finite dimension. There exist two integers s and $t \in \mathbb{N}^*$ such that: $X^t = X^s \bmod f$. Therefore, f divides $X^t - X^s$. It is assumed that $t > s$ then $f|X^s(X^{t-s} - 1)$.
Now we claim that:

$$f|X^s(X^{t-s} - 1) \Rightarrow f|(X^{t-s} - 1).$$

Suppose that $X^t - X^s = q(X)f(X)$ with $f(0)$ invertible, f monic and $s < t$. First, if $s = 0$, there is nothing to prove. Let us suppose that $s \geq 1$. Then:

$$X^s(1 - X^{s-t}) = q(X)f(X) \tag{2}$$

Secondly, the Euclidean division of $(1 - X^{t-s})$ by $f(X)$, which is possible because f is monic, is:

$$(1 - X^{t-s}) = b(X)f(X) + r(X) \text{ with } \deg(r) < \deg(f).$$

Thus

$$X^s(1 - X^{s-t}) = X^s b(X)f(X) + X^s r(X) \tag{3}$$

By evaluating at $X = 0$, we find, $q(0)f(0) = 0$. Since $f(0)$ is invertible, $q(0) = 0$.

Consequently, $q(X) = X.q'(X)$. Since $s \geq 1$, we have:

$$X([X^{s-1}b(X) - q'(X)]f(X) + X^{s-1}r(X)) = 0.$$

We are therefore reduced to the equality:

$$[X^{s-1}b(X) - q'(X)]f(X) + X^{s-1}r(X) = 0.$$

If $s = 1$, then the result is shown: $(1 - X^{s-t}) = q'(X)f(X)$.
Otherwise, we iterate the reasoning until $q(X) = X^s h(X)$. Then, by putting X^s in factor, we obtain:

$$[b(X) - h(X)]f(X) + r(X) = 0.$$

If $b(X) \neq h(X)$, then we can see that $\deg([b(X) - h(X)]f(X)) \geq \deg(f)$ because f is monic (hence the leading term cannot be canceled) $\deg(r) < \deg(f)$ which is impossible.

Consequently, $b(X) = h(X)$ and $r(X) = 0$. Thus, we have

$$f|(X^e - 1).$$

□

Definition 3. *The exponent of a reversible matricial polynomial f is the smallest non-zero e such that f divides $X^e - 1$ on the right side.*

Definition 4. *Let $f \in \mathbb{M}_\ell(\mathbb{F}_q)[X]$. We define the socle of f to be the set $\{u \in S(\mathbb{A}) \quad ; \quad f.u = 0\}$ which we denote $\Omega(f)$.*

Proposition 3.
Let $f \in \mathbb{M}_\ell(\mathbb{F}_q)[X]$ be reversible then we have the following.

1. *There exists $m \in \mathbb{N}$ such that each element of $\Omega(f)$ is periodic of period m.*
2. *The set $\mathcal{C}(f) = \{(u(0), \ldots, u(m-1)) \in \mathbb{A}^m \quad ; \quad u \in \Omega(f)\}$ is a cyclic code (over $\mathbb{F}_q$ and over $\mathbb{M}_\ell(\mathbb{F}_q)$).*
3. *We have: $\dim_{\mathbb{F}_q} \Omega(f) = \ell \deg(f)$.*

Proof
For 1., we just have to take m equal to the exponent of f. We can check easily the 2. and we can exhibit a basis to show the third point. □

Remark 2.2.

1. *The set $\Omega(f)$ is in fact a quasi-cyclic code of index l and length ℓm over $\mathbb{F}_q$.*
2. *The computation of the period of a linear recurring sequence with matricial coefficients can be obtained, like in [9], through the computation of the determinant polynomial of the companion matrix of the linear recurring sequence.*
3. *Let p a polynomial in $\mathbb{F}_q[x]$. We denote by p^* its reciprocal polynomial. When we replace $\mathbb{M}_\ell(\mathbb{F}_q)$ by $\mathbb{F}_q$ we know that $\Omega(f)$ is an $\mathbb{F}_q$-vector space of dimension $\deg(f)$ and that $\mathcal{C}(f)$ is a cyclic code generated by $\left(\frac{X^m - 1}{f}\right)^*$. We will see in the next section how to generalize this result in the case of matricial cyclic codes.*

4. *We know, in the scalar case, that a sequence is linear recurring if and only if its generator series is a rational fraction. By using methods similar to those developed in the proof of Proposition 2, we get a direct proof of the proposition which is a generalization of this result to the case of sequences of vectors with matricial coefficients.*

3. Construction of quasi-cyclic codes

3.1. Quasi-cyclic codes as cyclic codes over a ring

Let $\mathbb{A} = \mathbb{F}_q^l$, $n = \ell m$, $\mathcal{C}$ a code over $\mathbb{F}_q$ of length ℓ and Θ the isomorphism of linear vector spaces from $\mathbb{F}_q^n$ to $\mathbb{A}^m$ defined by:

$$\forall c = (c_0, c_1, \ldots, c_{n-1}), \quad \Theta c = ({}^t(c_0, \ldots, c_{\ell-1}), {}^t(c_\ell, \ldots, c_{2\ell-1}), \ldots, {}^t(c_{(m-1)\ell}, \ldots, c_{m\ell-1})).$$

We show that $\mathcal{C}$ is a quasi-cyclic code of index ℓ if and only if $\Theta\mathcal{C}$ is a cyclic code over $\mathbb{A}$.
Let $V_0, V_1, \ldots, V_{m-1}$ be m column vectors of $\mathbb{A}$, we denote by $V = (V_0, V_1, \ldots, V_{m-1})$ a vector of $\mathbb{A}^m$.
Let T be the shift operator in $\mathbb{A}^m$ defined by:

$$\forall V = (V_0, V_1, \ldots, V_{m-1}) \in \mathbb{F}_q^n, \quad TV = (V_{m-1}, V_0, \ldots, V_{m-2}). \tag{4}$$

Let $M \in \mathbb{M}_\ell(\mathbb{F}_q)$. For V as above, we define MV by

$$MV = (MV_0, \ldots, MV_{m-1}).$$

Now let $d \in \mathbb{N}$ and $P(X) = M_0 + M_1.X + \cdots + M_d.X^d$ in $\mathbb{M}_\ell(\mathbb{F}_q)[X]$ the polynomial algebra of $\ell \times \ell$ matrices over $\mathbb{F}_q$ (the indeterminate X commutes with matrices).

$$P(X).V = P(T)(V). \tag{5}$$

Let $X^m - 1 = I_\ell X^m - I_\ell$ where I_ℓ is the identity matrix of order ℓ. Let $\mathcal{I}$ be the two-sided ideal of $\mathbb{M}_\ell(\mathbb{F}_q)[X]$ generated by $X^m - 1$ and $\mathcal{B}$ the ring $\mathbb{M}_\ell(\mathbb{F}_q)[X]/\mathcal{I}$. We have the following result.

Proposition 4. *With the usual addition and the product defined above (5), the $\mathbb{F}_q$–vector space $\mathbb{A}^m$ is a left $\mathcal{B}$-module.*

Let $F \subset \mathcal{B}$ and $C \subset \mathbb{A}^m$. We define as in the case of linear recurring sequences, the socle of F and the annihilator of C as follows.

Definition 5. *Let $F \subset \mathcal{B}$ and $C \subset \mathbb{A}^m$.*
The annihilator of C is the set $\mathrm{Ann}(C) = \{P \in \mathcal{B} / \quad \forall c \in \mathcal{C}, \quad P.c = 0\}$. *The socle of F, denoted by $\Omega(F)$ is the subset of $\mathbb{A}^m$ given by* $\Omega(F) = \{y \in A^m / \quad \forall f \in F, \quad f.y = 0\}$.

An interesting question is to know when the two equalities hold:

$$\mathrm{Ann}(\Omega(F)) = F \text{ and } \Omega(\mathrm{Ann}(C)) = C.$$

It will be found in ([8]) some results about this question. Here we are interested in the "principal" case: the subset F is reduced to a single element. In this situation, we have some good results.
For example, as in the case of linear recurring sequences, we have the following proposition.

Proposition 5. *Let $f \in \mathcal{B}$ and $\mathcal{C}$ an $\mathbb{F}_q$ vector subspace of $\mathbb{A}^m$, then:*

1. *the set $\Omega(f)$ is an $\mathbb{F}_q$ vector space of dimension $\ell \deg(f)$,*
2. *the set $\mathrm{Ann}(\mathcal{C})$ is a left ideal of $\mathcal{B}$.*

Proof
Similar to the proof of proposition 3.

□

Another example of results about this question will be found in the following section.

Remark 3.1.
1. A cyclic code $\mathcal{C}$ of length m over $\mathbb{A}$ can be seen as a particular vector subspace of $S(\mathbb{A})$ the set of the sequences over $\mathbb{A}$ in the following way:

For $c = (c_0, \ldots, c_{m-1}) \in \mathcal{C}$, we associate $u \in S(\mathbb{A})$, such that

$$\forall i \in \mathbb{N}, \qquad u_i = c_{i \mod m}.$$

2. The ideal $\mathrm{Ann}(\mathcal{C})$ *is not necessarily principal.*

In spite of the fact that $\mathrm{Ann}(\mathcal{C})$ is not a principal ideal we have the following result.

Proposition 6.
Let f in $\mathcal{B}$ be reversible. Assume that there exists g reversible in $\mathcal{B}$ such that $fg = X^m - 1$. Then $\mathrm{Ann}(\Omega(f))$ is a principal ideal in $\mathcal{B}$ and is exactly the ideal generated by f:

$$\mathrm{Ann}(\Omega(f)) =< f > .$$

Proof
Based on the fact that $\mathrm{Ann}(\Omega(f))$ cannot contain a polynomial of degree smaller than the degree of f. □

3.2. Construction of $\Omega(P)$-codes
In this section we will only consider factorization of the form $X^m - 1 = P.Q$ with P and Q reversibles. We will show how to construct such codes and consider particular families with good minimal distances.

3.2.1. Generator Matrix
This first result is similar to the cyclic case. Indeed, in the cyclic case, if $X^n - 1 = P.Q$, it implies that $< P >$ is the ideal cancelled by Q. It means : $\forall R, \quad R \in < P > \Longleftrightarrow Q.R = 0$.

Proposition 7. *Let P and Q such that $X^m - 1 = PQ$ in $\mathbb{M}_l(\mathbb{F}_q)[X]$. Then:*

$$\Omega(P) = Q.\mathbb{A}^m = \{Q.x | x \in \mathbb{A}^m\}.$$

Proof
(cf. Appendix).

Let $Q(X) = \sum_{i=0}^{m-1} q_i X^i \in \mathbb{M}_\ell(\mathbb{F}_q)[X]$ where, for $i \in \{1, \ldots, m-1\}$, q_i is the matrix $(q^i_{a,b})_{a,b=0,\ldots,\ell-1}$.
Let, for $i \in \{1, \ldots, m-1\}$, ${}^t q_i$ be the transpose of q_i. Then, with the same notations as above we have the following corollary.

Corollary 3.1. *A generator matrix of $\Omega(P)$ is*

$$G_{\Omega(P)} = \begin{pmatrix} {}^t q_0 & {}^t q_1 & {}^t q_2 & \cdots & {}^t q_{degQ} & 0 & 0 & \cdots & 0 \\ 0 & {}^t q_0 & {}^t q_1 & \cdots & {}^t q_{degQ-1} & {}^t q_{deg(Q)} & 0 & \cdots & 0 \\ & & \ddots & & & & \ddots & & \end{pmatrix}$$

Proof
If $P.Q = X^m - 1$ with P and Q two reversible polynomials, from Proposition 7, we have $\Omega(P) = Q.\mathbb{A}^m$. Let $c_{i,j} \in \mathbb{A}^m$ ($i \in \{0, \ldots, deg(P)-1\}, j \in \{0, \ldots, \ell-1\}$) be the vectors $(0, \ldots, 0, 1, 0, \ldots, 0)$ where the '1'

is in position $i\ell + j$.
Hence, all $Q.c_{i,j}$ are codewords of $\Omega(P)$ and $Q.c_{i,j}$ is the codeword

$$(\underbrace{0,\ldots,0}_{i\ell \text{ zeros}}, col_j(q_0), col_j(q_1), \ldots, col_j(q_{deg(Q)}), 0, \ldots, 0)$$

where $col_j(A)$ is the j^{th} column of the matrix A.
The codewords $Q.c_{0,0}, \ldots, Q.c_{0,\ell-1}$ are linearly independent since q_0 and $q_{\deg Q}$ are invertible. Hence all $Q.c_{i,j}$ are linearly independent. Finally, since $\dim(\Omega(P)) = \ell deg(P)$, $\Omega(P)$ is spanned by all these $Q.c_{i,j}$. □

3.2.2. Constructions of general codes
The most difficult part of the construction of such codes is the factorization of $X^m - 1$ into polynomials with matricial coefficients. In a first part, we will use an easy but expensive way to factorize it. And then, for the particular case of self-dual codes, we will use Groebner basis tools to solve a multivariate polynomial system. But it is well known that it becomes uncomputable very fast when the number of variables and the degree of equations grow.

3.2.2.a. With prescribed length

In this case, we use the most naive way to factorize $X^m - 1$.

Input: ℓ, m, deg_{max}
Algorithm:
    $list_{poly} \leftarrow [\,]$;
    for d from 1 to deg_{max} do
        for $P \in \mathbb{M}_\ell(\mathbb{F}_q)[X]$ monic of degree d do
            if P divides $X^m - 1$ then Add P into $list_{poly}$;
        end for;
    end for;
Output: $list_{poly}$

Figure 1: Algorithm 1

It is easy to understand that one cannot reach high lengths and degrees of polynomials this way.

3.2.2.b. With prescribed dimension

In this method, we will set the degree of our polynomial P but we won't be able to control the length of our code, and in most of the cases, the length of the code obtained is very large. This algorithm is based on Proposition 5 and uses the existence of an exponent for every reversible polynomial.

Input: ℓ, deg, nb_{steps}
Algorithm:
    $list \leftarrow [\,]$;
    for i from 1 to nb_{steps} do
        Pick a random reversible polynomial $P \in \mathbb{M}_\ell(\mathbb{F}_q)[X]$ of degree deg;
        Compute m its exponent;
        Add $[P, m]$ into $list$;
    end for;
Output: $list$

Figure 2: Algorithm 2

At the end of this algorithm, every element $[P, m]$ of *list* corresponds to the ℓ-quasi-cyclic code of length $\ell.m$ and dimension $\ell.deg$ cancelled by P.
With this method, we find one code at every step but we cannot control the length, and this it is large very often.

Example 3.1. *Let $q = 4$ and $\ell = 2$. Let $\mathbb{F}_4 = \mathbb{F}_2[w]$ where $w^2 + w + 1 = 0$.*

- *Let* $f(X) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} X^5 + \begin{pmatrix} w & w^2 \\ 0 & w^2 \end{pmatrix} X^4 + \begin{pmatrix} 0 & w \\ 0 & w^2 \end{pmatrix} X^3 + \begin{pmatrix} w^2 & 0 \\ 1 & w^2 \end{pmatrix} X^2 + \begin{pmatrix} w^2 & w^2 \\ w & 1 \end{pmatrix} X + \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$.

  Calculation gives $m = 255, f(X)|(X^{255} - 1)$ and we obtain a $[510, 10, 204]$ 2-quasicyclic code.

- *Let* $f(X) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} X^5 + \begin{pmatrix} w^2 & 0 \\ 1 & w \end{pmatrix} X^4 + \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} X^3 + \begin{pmatrix} 1 & w \\ 1 & 0 \end{pmatrix} X^2 + \begin{pmatrix} w^2 & 1 \\ 1 & 0 \end{pmatrix} X + \begin{pmatrix} w & w \\ 0 & 1 \end{pmatrix}$.

  Here $m = 1020, f(X)|(X^{1020} - 1)$ and we obtain a $[2040, 10, 1020]$ 2-quasicyclic code.

3.2.3. Construction of self-dual codes
Self-Dual codes are codes such that they are equal to their dual code. In order to study these codes, we need to know more about the dual code of a $\Omega(P)$-code. Fortunately, it is still a $\Omega(P')$-code. Furthermore this P' is easy to compute. We will study two types of duals, those for the Euclidean inner product and those for the Hermitian one.

3.2.3.a. Construction of Euclidean self-dual codes

Definition 6. *Let $\mathcal{R}$ be a commutative ring and $n \in \mathbb{N}^*$. The Euclidean inner product in $\mathcal{R}^n$ is defined by:*

$$\forall a = (a_1, \ldots, a_n) \in \mathcal{R}^n, \forall b = (b_1, \ldots, b_n) \in \mathcal{R}^n, \quad < a, b >_e = \sum_{i=1}^{n} a_i b_i$$

Definition 7. *Let $\mathcal{R}$ be a commutative ring and $n \in \mathbb{N}^*$. Let C and D be codes over $\mathcal{R}$ ($\mathcal{R}$-submodules of $\mathcal{R}^n$).*
Then D is said to be the Euclidean dual code of C (and noted $D = C^{\perp_e}$) if

$$\forall c \in C, \quad \forall d \in D, \quad < c, d >_e = 0.$$

In our case, we have this following Theorem:

Theorem 1. *With our notations, if $X^m - 1 = P.Q$ in $\mathbb{M}_\ell(\mathbb{F}_q)[X]$ then*

$$\Omega(P)^{\perp_e} = \Omega({}^tQ^*)$$

Proof
(cf. Appendix).

From now on, m has to be even; $m = 2m'$. Hence, in order to find Euclidean self-dual codes, we have to find P's of degree m' such that $X^m - 1 = P.{}^tP^*$. This method requires the solving, with a Groebner basis, of a multivariate polynomial system with about $\ell^2 m'$ variables and $\ell^2 m$ equations of degree 2.
However, if $P = {}^tP^*$, it is sufficient to construct such codes and fortunately most of the best codes (with good minimal distance) are in this family. And this way, the number of variables is considerably reduced. Indeed, we have about $\ell^2 m'/2$ and still $\ell^2 m$ equations of degree 2. Good codes were found only on $\mathbb{F}_4$ and results obtained with this method can be found in the following table.

n	Bounds	Largest Distance	Number of Codes	Remarks
8	4	**4**	2	Remark 3.2
12	6	4	2	
16	6	**6**	3	
20	8	7	2	
24	8-10	**8**	9	
28	9-11	**9**	2	Remark 3.3
32	10-12	**10**	8	
36	10-14	**10**	22	
40	12-16	**12**	8	

Figure 3: Table of Euclidean self-dual codes obtained by our construction

Here "Largest Distance" means largest distance found with our codes. Il the first column, in the notation $a - b$, the number a is the best known distance and b is ths theorical upper bound (see [11] for more supplementary information).
In most of cases, the highest bound known is reached by at least one of such codes (except $n = 12, 20$). It was not unexpected because the family of quasicyclic codes is known to contain good codes [4].

Remark 3.2. *One of these* $[8, 4, 4]$*-codes has a binary generator polynomial*

$$f(X) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} X^2 + \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} X + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Hence, its generator matrix is:

$$G_{\Omega(f)} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Remark 3.3. *In* [1]*, Boucher and Ulmer found four* $[28, 14, 9]$*-Euclidean self-dual codes on* $\mathbb{F}_4$*. These codes were constructed from skew polynomial rings. The two codes we found are conjugated and not equivalent (by permutations) to theirs. They are all not equivalent to the extended quadratic residue code. Let* $\mathbb{F}_4 = \mathbb{F}_2[w]$ *(*$w^2 + w + 1 = 0$*). Our codes are respectively canceled by*

$$f_1(X) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} X^7 + \begin{pmatrix} w & w^2 \\ 1 & w \end{pmatrix} X^6 + \begin{pmatrix} 1 & w^2 \\ 1 & 1 \end{pmatrix} X^5 + \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} X^4 + \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} X^3 + \begin{pmatrix} 1 & 1 \\ w^2 & 1 \end{pmatrix} X^2 + \begin{pmatrix} w & 1 \\ w^2 & w \end{pmatrix} X + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\text{and } f_2(X) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} X^7 + \begin{pmatrix} w^2 & w \\ 1 & w^2 \end{pmatrix} X^6 + \begin{pmatrix} 1 & w \\ 1 & 1 \end{pmatrix} X^5 + \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} X^4 + \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} X^3 + \begin{pmatrix} 1 & 1 \\ w & 1 \end{pmatrix} X^2 + \begin{pmatrix} w^2 & 1 \\ w & w^2 \end{pmatrix} X + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

3.2.3.b. Construction of Hermitian self-dual codes

In this part, we will only deal with codes on $\mathbb{F}_4$. We note θ the Froebenius map on $\mathbb{F}_4$ ($\theta(x) = x^2$).

Definition 8. *Let* $\mathcal{R}$ *be a commutative ring,* $n \in \mathbb{N}^*$ *and* θ *be a automorphism of* $\mathcal{R}$ *of order 2. The Hermitian inner product in* $\mathcal{R}^n$ *is defined by:*

$$\forall a = (a_1, \ldots, a_n) \in \mathcal{R}^n, \forall b = (b_1, \ldots, b_n) \in \mathcal{R}^n, \quad < a, b >_h = \sum_{i=1}^{n} a_i \theta(b_i).$$

$$\text{If } \mathcal{R} = \mathbb{F}_4,\ \theta(x) = x^2 \text{ and } < a, b >_h = \sum_{i=1}^{n} a_i b_i^2$$

Definition 9. *Let $\mathcal{R}$ be a commutative ring and $n \in \mathbb{N}^*$. Let C be a code over $\mathcal{R}$ (a $\mathcal{R}$-submodule of $\mathcal{R}^n$).*
D is said to be the Hermitian dual code of C and noted $D = C^{\perp_h}$ if

$$\forall c \in C, \quad \forall d \in D, \qquad < c, d >_h = 0.$$

In our case, we have this following Theorem:

Theorem 2. *Let $X^m - 1 = P.Q$ in $\mathbb{M}_\ell(\mathbb{F}_q)[X]$ then*

$$\Omega(P)^{\perp_h} = \Omega(\theta({}^tQ^*))$$

(θ is applied to every component of every matricial coefficient of ${}^tQ^*$).

Proof
(cf. Appendix).

Like in the Euclidean part, we look for P's of degree m' such that $X^m - 1 = P.\theta({}^tP^*)$. This method requires the solving, with a Groebner basis, of a multivariate polynomial system with about $\ell^2 m'$ variables and $\ell^2 m$ equations of degree 3 (because of the existence of θ).
However in this case it is not useful to look for P's such that $P = \theta({}^tP^*)$, because it implies that all components of matrices are in $\mathbb{F}_2$, and these polynomials do not give good codes. Hence, we keep $\ell^2 m'$ variables, and computations are longer than in the Euclidean case.

n	Bounds	Largest Distance	Number of Codes
8	4	**4**	1
12	4	**4**	1
16	6	**6**	1
20	8	**8**	1
24	8	**8**	7
28	10	**10**	2

Figure 4: Table of Hermitian self-dual codes obtained by our construction

Remark 3.4. *1. In this case, we cannot reach large length of codes because of the number of variables of the Groebner basis we have to compute. But for all of these values, we reach the highest distance known.*

2. It is easy to construct codes with a trivial annihilator.

3. The quasicyclic codes are not all $\Omega(P)$-codes where P is a polynomial : the dimension of an $\Omega(P)$-code is $l \deg(P)$.

Acknowledgments
We would like to thank T.P. Berger, P. Gaborit and the referees for their remarks and suggestions.

References

[1] D. Boucher and F. Ulmer, Coding with skew polynomial rings. To appear in Journal of Symbolic Computation.

[2] J. Conan and G. Séguin, Structural properties and enumeration of quasicyclic codes. Appl. Algebra Eng. Comm. Comput. 4, 1993.

[3] P. Fitzpatrick and K. Lally, Algebraic structure of quasicyclic codes. Disc. Appl. Math., 111(2001), pp 157–175.

[4] P. Gaborit and G. Zemor, Asymptotic improvement of the Gilbert-Varshamov bound for binary linear codes. Information Theory, 2006 IEEE International Symposium on Information Theory July 2006, pp 287–291.

[5] S. Ling and P. Solé, Decomposing quasi-cyclic codes. International workshop on coding and cryptography. Paris, 8-12 January 2001.

[6] S. Ling and P. Solé, On the algebraic structure of quasy-cyclic codes I: finite fields. IEEE Transactions on Information Theory, 47, 2751-2760, 2001.

[7] A. Necer, Systèmes récursifs et algèbre de Hadamard de suites récurrentes linéaires sur des anneaux commutatifs. Communications in Algebra, 27 (12), 6175–6189, 1999.

[8] A. A. Nechaev, Finite quasi-frobenius modules, applications to codes and linear recurrences Fundamentalnaya i prikladnaya matematika, 1: pp 229–254, 1995.

[9] H. Niederreiter, The Multiple-Recursive Matrix Method for Pseudorandom Number Generation. Finite fields and their applications 1, 3–30, 1995.

[10] G. Skersys, Etudes de codes quasi-cycliques comme codes concaténés. Preprint. Université de Limoges 1997.

[11] http://www.unilim.fr/pagesperso/philippe.gaborit/SD/index.html

4. Appendix

Notations

If $Q \in \mathbb{M}_\ell(\mathbb{F}_q)[X], Q(X) = \sum_{i=0}^{m-1} q_i X^i$, with $q_i \in \mathbb{M}_\ell(\mathbb{F}_q)$, where $q_i = (q^i_{a,b})_{a,b=0,\ldots,\ell-1}$.

If $c \in \mathbb{A}^m, c = (c_0, c_1, \ldots, c_{m-1})$ with $c_i \in \mathbb{A}, \forall i = 0, \ldots, m-1$ and for $i \in \{0, \ldots, m-1\}$, we denote $c_i = (c_{i,0}, \ldots, c_{i,l-1})$ with $c_{i,j} \in \mathbb{F}_q, \forall i = 0, \ldots, m-1$, $\forall j = 0, \ldots, l-1$.

If $Q(X) = \sum_{i=0}^{m-1} q_i X^i \in \mathbb{M}_\ell(\mathbb{F}_q)[X]$, we assimilate q_j by $q_{j \mod m}$ (caught between 0 and $m-1$).

Similarly if $c = (c_0, \ldots, c_{m-1}) \in \mathbb{A}^m$, we assimilate c_j by $c_{j \mod m}$ (caught between 0 and $m-1$).

Proposition 7
If $X^m - 1 = P.Q$, with P, Q reversible, then

$$\begin{aligned} \Omega(P) &= Q.\mathbb{A}^m \\ &= \{Q.x | x \in \mathbb{A}^m\}. \end{aligned}$$

Proof
Let $y \in Q.\mathbb{A}^m$, then $\exists\ y_0 \in \mathbb{A}^m$ such that $y = Q.y_0$ and thus $P.y = P.Q.y_0 = (X^m - 1).y_0 = 0$ thus $y \in \Omega(P)$. Hence $Q.\mathbb{A}^m \subseteq \Omega(P)$.
Consider :

$$\begin{aligned} \Phi_Q : \mathbb{A}^m &\to \mathbb{A}^m \\ y &\mapsto Q.y \end{aligned}$$

The application Φ_Q is $\mathbb{F}_q$ linear.

We have $\ker(\Phi_Q) = \Omega(Q)$ and $\mathrm{im}(\Phi_q) = Q.\mathbb{A}^m$ thus:

$$\begin{aligned} \dim(Q.\mathbb{A}^m) = &= \ell m - \dim(\Omega(Q)) \\ &= \ell m - \ell \deg(Q) \\ &= \ell m - \ell(m - \deg(P)) \\ &= \ell \deg(P) \\ &= \dim(\Omega(P)). \end{aligned}$$

Since $Q.\mathbb{A}^m \subseteq \Omega(P)$ and $\dim(Q.\mathbb{A}^m) = \dim(\Omega(P))$ we deduce the equality :

$$\Omega(P) = Q.\mathbb{A}^m$$

□

Theorem 1 (Euclidean case)
Let $P, Q \in \mathbb{M}_\ell(\mathbb{F}_q)[X]$ be reversibles such that $P.Q = X^m - 1$. Then :

$$\Omega(P)^{\perp_e} = \Omega({}^tQ^*)$$

Proof

Lemma 1
Let $d \in (\mathbb{F}_q^l)^m$, then :

$$d \in \Omega(P)^{\perp_e} \Leftrightarrow \forall y \in \mathbb{A}^m, \quad \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} \sum_{a=0}^{\ell-1} \sum_{b=0}^{\ell-1} q_{a,b}^j y_{i+j,b} d_{i,a} = 0.$$

Proof

Let $\mathcal{A}$ be $\mathbb{A}^m$ or $\mathbb{A}$. We will denote $< .;. >_{\mathcal{A}}$ the Euclidean inner product in $\mathcal{A}$.

$$\begin{aligned}
d \in \Omega(P)^{\perp_e} &\Leftrightarrow \forall c \in \Omega(P), \quad < c; d >_{\mathbb{A}^m} = 0 \\
&\Leftrightarrow \forall y \in \mathbb{A}^m, \quad < Q.y; d >_{\mathbb{A}^m} = 0 \\
&\Leftrightarrow \forall y \in \mathbb{A}^m, \quad \sum_{i=0}^{m-1} < (Q.y)_i; d_i >_{\mathbb{A}} = 0 \\
&\Leftrightarrow \forall y \in \mathbb{A}^m, \quad \sum_{i=0}^{m-1} < \sum_{j=0}^{m-1} q_j.y_{i+j}; d_i >_{\mathbb{A}} = 0 \\
&\Leftrightarrow \forall y \in \mathbb{A}^m, \quad \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} < q_j.y_{i+j}; d_i >_{\mathbb{A}} = 0 \\
&\Leftrightarrow \forall y \in \mathbb{A}^m, \quad \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} < (\sum_{b=0}^{\ell-1} q_{a,b}^j.y_{i+j,b})_{a=0,\ldots,\ell-1}; (d_{i,a})_{a=0,\ldots,\ell-1} >_{\mathbb{A}} = 0 \\
&\Leftrightarrow \forall y \in \mathbb{A}^m, \quad \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} \sum_{a=0}^{\ell-1} \sum_{b=0}^{\ell-1} q_{a,b}^j y_{i+j,b} d_{i,a} = 0
\end{aligned}$$

□

Lemma 2
Let $d \in \mathbb{A}^m$, then :

$$d \in \Omega({}^tQ^*) \Leftrightarrow \ \forall j, k = 0, \ldots, m-1, \quad \sum_{i=0}^{m-1} \sum_{a=0}^{\ell-1} q_{a,j}^{-i} d_{i+k,a} = 0.$$

Proof
Let $R \in \mathbb{M}_\ell(\mathbb{F}_q)[X]$ and $d \in \mathbb{A}^m$. We have:

$$
\begin{aligned}
R.d &= (\sum_{i=0}^{m-1} r_i X^i)(d) \\
&= (\sum_{i=0}^{m-1} r_i X^i)(d_0, \ldots, d_{m-1}) \\
&= (\sum_{i=0}^{m-1} r_i d_{i+k})_{k=0,\ldots,m-1} \\
&= (\sum_{i=0}^{m-1} (\sum_{a=0}^{\ell-1} r_{j,a}^i d_{i+k,a})_{j=0,\ldots,m-1})_{k=0,\ldots,m-1}
\end{aligned}
$$

$$
\text{Hence } R.d = 0 \quad \Leftrightarrow \quad \forall j, k = 0, \ldots, m-1, \quad \sum_{i=0}^{m-1} \sum_{a=0}^{\ell-1} r_{j,a}^i d_{i+k,a} = 0
$$

Computing ${}^tQ^* * d$, we have:

$$
Q(X) = \sum_{i=0}^{m-1} q_i X^i, q_i = (q_{j,a}^i)_{j=0,\ldots,m-1;a=0,\ldots,m-1}
$$

$${}^tQ(X) = \sum_{i=0}^{m-1} {}^tq_i X^i, \text{ with } {}^tq_i = (q_{a,j}^i)_{j=0,\ldots,m-1;a=0,\ldots,m-1}$$

$${}^tQ^*(X) = \sum_{i=0}^{m-1} {}^tq_{\deg(Q)-i} X^i, \text{ with } {}^tq_{\deg(Q)-i} = (q_{a,j}^{\deg(Q)-i})_{j=0,\ldots,m-1;a=0,\ldots,m-1}$$

hence,

$$
\begin{aligned}
{}^tQ^* * d = 0 \quad &\Leftrightarrow \quad \forall j, k = 0, \ldots, m-1, \quad \sum_{i=0}^{m-1} \sum_{a=0}^{\ell-1} q_{a,j}^{\deg(Q)-i} d_{i+k,a} = 0 \\
&\Leftrightarrow \quad \forall j, k = 0, \ldots, m-1, \quad \sum_{i=0}^{m-1} \sum_{a=0}^{\ell-1} q_{a,j}^{-i} d_{i+\deg(Q)+k,a} = 0 \\
&\Leftrightarrow \quad \forall j, k = 0, \ldots, m-1, \quad \sum_{i=0}^{m-1} \sum_{a=0}^{\ell-1} q_{a,j}^{-i} d_{i+k,a} = 0
\end{aligned}
$$

□

We now have all the tools to demonstrate the main theorem.

Show first $\Omega(P)^{\perp_e} \subset \Omega({}^tQ^*)$.

Let $d \in \Omega(P)^{\perp_e}$, $\Omega(P)^{\perp_e}$ being ℓ-quasi-cyclic,

$$
\forall k = 0, \ldots, m-1, X^k.d \in \Omega(f)^{\perp_e}
$$

Hence from the Lemma 1,

$$
\forall y \in \mathbb{A}^m, \ \forall k = 0, \ldots, m-1, \quad \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} \sum_{a=0}^{\ell-1} \sum_{b=0}^{\ell-1} q_{a,b}^j y_{i+j,b} d_{i+k,a} = 0 \tag{6}
$$

Let $j \in \{0, \ldots, m-1\}$, for $y = (e_j; 0; \ldots; 0)$, (e_j : j^{th} vector of the canonical basis of $\mathbb{A} = \mathbb{F}_q^\ell$).
We have:

$$y_{i+j,b} \quad = \quad \delta_b^j \text{ if } i + j = 0 \mod m \text{ and 0 otherwise}$$

So for this y, the equation 6 gives us:

$$\forall k = 0, \ldots, m-1, \quad \sum_{i=0}^{m-1} \sum_{a=0}^{\ell-1} q_{a,j}^{-i} d_{i+k,a} = 0$$

But this is true for arbitrary j.
Hence :

$$\forall k = 0, \ldots, m-1, \ \forall j = 0, \ldots, m-1, \quad \sum_{i=0}^{m-1} \sum_{a=0}^{\ell-1} q_{a,j}^{-i} d_{i+k,a} = 0$$

Thus from the Lemma 2, $d \in \Omega({}^tQ^*)$. So

$$\Omega(P)^{\perp_e} \subset \Omega({}^tQ^*).$$

Hence

$$\begin{array}{rcl} \dim(\Omega(P)^{\perp_e}) & = & \ell m - \dim(\Omega(P)) \\ & = & \ell m - \ell \deg(P) \text{ via the Proposition 3} \\ & = & \ell(m - \deg(P)) \\ & = & \ell \deg(Q) \end{array}$$

and,

$$\begin{array}{rcl} \dim(\Omega({}^tQ^*)) & = & \ell \deg({}^tQ^*) \text{ via the Proposition 3} \\ & = & \ell \deg(Q) \text{ because } Q \text{ is reversible} \\ & = & \dim(\Omega(P)^{\perp_e}) \end{array}$$

Hence the equality. □

Theorem 2 (Hermitian case)
Let $P, Q \in \mathbb{M}_\ell(\mathbb{F}_q)[X]$ reversibles such that $P.Q = X^m - 1$. Then :

$$\Omega(P)^{\perp_h} = \Omega(\theta({}^tQ^*)).$$

Proof

Lemma 3
Let $d \in (\mathbb{F}_q^l)^m$, then :

$$d \in \Omega(P)^{\perp_h} \Leftrightarrow \forall y \in \mathbb{A}^m, \quad \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} \sum_{a=0}^{\ell-1} \sum_{b=0}^{\ell-1} q_{a,b}^j y_{i+j,b} \theta(d_{i,a}) = 0.$$

Proof
The proof is the same as in Lemma 1. The θ comes from the Hermitian inner product.

□

Lemma 4
Let $d \in \mathbb{A}^m$, then :

$$d \in \Omega(\theta({}^tQ^*)) \Leftrightarrow \ \forall j, k = 0, \ldots, m-1, \quad \sum_{i=0}^{m-1} \sum_{a=0}^{\ell-1} \theta(q_{a,j}^{-i}) d_{i+k,a} = 0.$$

Proof
In Lemma 2 we have

$$ {}^tQ^*(X) = \sum_{i=0}^{m-1} {}^tq_{\deg(Q)-i} X^i, \text{ with } {}^tq_{\deg(Q)-i} = (q_{a,j}^{\deg(Q)-i})_{j=0,\ldots,m-1;a=0,\ldots,m-1} $$

hence

$$ \theta({}^tQ^*)(X) = \sum_{i=0}^{m-1} \theta({}^tq_{\deg(Q)-i}) X^i, \text{ with } \theta({}^tq_{\deg(Q)-i}) = (\theta(q_{a,j}^{\deg(Q)-i}))_{j=0,\ldots,m-1;a=0,\ldots,m-1} $$

and the result follows.

□

We now have all the tools to demonstrate the main theorem.

Show first $\Omega(P)^{\perp_h} \subset \Omega(\theta({}^tQ^*))$.

Let $d \in \Omega(P)^{\perp_h}$, $\Omega(P)^{\perp_h}$ being ℓ-quasi-cyclic,

$$ \forall k = 0, \ldots, m-1, X^k.d \in \Omega(f)^{\perp_h} $$

Hence from the Lemma 3,

$$ \forall y \in \mathbb{A}^m, \ \forall k = 0, \ldots, m-1, \quad \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} \sum_{a=0}^{\ell-1} \sum_{b=0}^{\ell-1} q_{a,b}^j y_{i+j,b} \theta(d_{i+k,a}) = 0 \tag{7} $$

Let $j \in \{0, \ldots, m-1\}$, for $y = (e_j; 0; \ldots; 0)$, (e_j : j^{th} vector of the canonical basis of $\mathbb{A} = \mathbb{F}_q^\ell$).
We have:

$$ y_{i+j,b} \quad = \quad \delta_b^j \text{ if } i + j = 0 \mod m \text{ and 0 otherwise} $$

So for this y, the equation 7 gives us:

$$ \forall k = 0, \ldots, m-1, \quad \sum_{i=0}^{m-1} \sum_{a=0}^{\ell-1} q_{a,j}^{-i} \theta(d_{i+k,a}) = 0 $$

But this is true for arbitrary j.
The rest of the proof is similar to the end of the proof of the main theorem (Euclidean case). We replace $d_{i+k,a}$ by $\theta(d_{i+k,a})$.

□