4-16-2021

Matrix Product Structure of a Permuted Quasi Cyclic Code and Its dual

Perian Perdhiku
University of Missouri-St. Louis, pp4h9@umsystem.edu

Matrix Product Structure of a Permuted Quasi Cyclic Code and Its Dual

Perian Perdhiku

M.A., Mathematics, University of Missouri - St Louis, Dec. 2016
B.S.B.A., Mathematics, University of Tirane Albania, June 2009

A Dissertation Submitted to
The Graduate School at the University of Missouri-St. Louis in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Mathematical and Computational Sciences with an emphasis in Mathematics.

May 2021

Advisory Committee

Ravindra Girivaru, PhD.
chairperson

Prabhakar Rao, PhD.

Adrian Clingher, PhD.

David Covert, PhD.

Contents

1 Introduction

Coding theory studies the property of codes, which are very important in a lot of applications in fields such as data compression, error detection and correction, cryptography and networking. In my dissertation, I study families of cyclic codes and their generalizations. These types of codes are special types of linear codes. Linear Codes are sets of codewords such that any linear combination of codewords is still a codeword. These kind of codes are very useful in error detection and correction. Error Detection and Correction is a technique that first detects the corrupted data sent from some transmitter over unreliable communication channels and then corrects the errors and reconstructs the original data. The best contribution for the linear codes was given by Richard W. Hamming who invented the so called Hamming Codes. In 1968 he also won the Turing Award, which is an annual prize given by Association for Computing Machinery. Unlike Hamming codes, cyclic codes are used to correct errors where the pattern is not clear and the error occurs in a short segment of the message.

One generalization of cyclic codes is the family of quasi cyclic codes, the length of which is usually a big number. In order to make the study of these codes easier, one approach is to break it down into cyclic codes with small length so that the structure of quasi cyclic code can be understand from these cyclic codes.

One way of breaking down big codes is to write them down as matrix product of small codes. However the structure of quasi cyclic codes is not right for that. That is why I manipulated them by using a permutation. I called these new types of codes *Permuted Quasi Cyclic Codes* .

From any permuted quasi cyclic code we can define some special cyclic codes. For my thesis I will try to find sufficient and necessary conditions so any permuted quasi cyclic code can be written as a matrix product of those codes.

Another generalization of cyclic codes is the family of multi cyclic codes. These types of codes are more complicated than the previous one so I will propose to limit myself on finding the structure of multi cyclic codes of length 4 over $\mathbb{F}_3$.

One technique of constructing new linear codes from a given linear code is by finding the so called Euclidean dual of a linear code. In my thesis I will also analyze the euclidean dual of the families above.

2 Finite Fields

Finite Fields play a very important role in Coding Theory. In this chapter I will recall some very important results about finite fields. Most of the work in this chapter is refereed to [4, chapter 3].

2.1 Cardinality of Finite Fields.

Definition 1. Let F be a finite set and let '$+$' and '$\cdot$' be two operations. We say $(F, +, \cdot)$ is a *finite field* (or simply F is a finite field) if and only if the following conditions are true:

1. $(F, +)$ is an abelian group. Let us denote with 0 the additive neutral element.
2. $(F^*, \cdot)$ is also an abelian group, where $F^* = F - \{0\}$. Let us denote with 1 the multiplicative neutral element.
3. $a \cdot (b + c) = a \cdot b + a \cdot c$ for any $a, b, c \in F$.

Definition 2. A subset K of a finite field F is called a *subfield* of F if and only if K is a finite field under the operations of F.

Lemma 1. *If K is a subfield of a finite field F then F is a vector space over K.*

Proof. Straightforward from definition. □

Theorem 1. *If F is a finite field then its cardinality is p^m for some prime number p and some positive integer m.*

Proof. For any positive integer s, let $1_s = 1 + 1 + ... + 1$, where the sum is taken s times.

Since F is finite, there exist positive integers p_1, p_2 such that, $p_1 < p_2$ and $1_{p_1} = 1_{p_2}$. It is easy to see that $p_0 = p_2 - p_1$ is a positive integer and $1_{p_0} = 0$. Let p be the smallest positive integer such that $1_p = 0$.

Since we want p to be prime, let us assume by contradiction that $p = ab$ where a, b are both positive integers strictly less than p. Because p is the smallest integer with above property, we have $1_a \neq 0$ and $1_b \neq 0$. It follows that $1_p = 1_a \cdot 1_b \neq 0$, which is a contradiction. So the above p is a prime number.

Let $P = \{0, 1, 1_2, 1_3, ..., 1_{p-1}\}$. It is easy to see that $card(P) = p$. We can also claim that P is a subfield of F because for any two positive integers a and b such that $a, b < p$, the following hold

1. $1_a + 1_b = 1_{(a+b) mod p}$,
2. $1_a 1_b = 1_{(ab) mod p}$,
3. $-1_a = 1_{p-a}$,

4. $(1_a)^{-1} = 1_{\alpha mod p}$ where $\alpha a + \beta p = 1$.

From Lemma 1 we can say that F is a vector space over P. If $m = dim(F)$ over P, then m is finite since F is a finite set. Let $b_1, b_2, ..., b_m$ be a basis for F. Any element $b \in F$ can be written uniquely as $b = \alpha_1 b_1 + \alpha_2 b_2 + ... + \alpha_m b_m$, for some $\alpha_i \in P$. Since for any α_i we have p choices it follows $card(F) = p^m$. □

The subfield P of the above theorem is called the *the prime subfield* of F. Also the prime number p of the above theorem is called the characteristic of F, since we can show that for any $a \in F$, $a + a + ... + a = 0$, where the sum is taken p times.

The converse of the last theorem is also true. So for any prime number p and any positive integer s we can find a finite field F such that its cardinality is p^s. See ([4, Theorem 3.4.4, page 109]).

Another true fact about finite fields is that any two finite fields F and F' with the same cardinality are isomorphic, i.e., there exists an one-to-one and onto map f from F to F' such that for any $a, b \in F$, $f(a + b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$. See ([4, Theorem 3.1.1, page 101]);

In this case we can consider both fields identical, therefore we can denote with F_q all the finite fields with cardinality q.

The next theorem will give us more details about the multiplicative group of a finite field.

Theorem 2. *If* F_q *is a finite field then* $(F^*, \cdot)$ *is a cyclic group.*

Proof. For any $a \in F^*$ let us define with $o(a)$ the smallest positive integer such that $a^{o(a)} = 1$. It exists because we are working on a finite field. If $m = max\{o(a)|a \in F^*\}$ then $m \mid (q - 1)$, from Lagrange's Theorem.

Let $b \in F^*$ such that $o(b) = m$ and let c be a random element in F^*. Since F^* is a finite abelian group, there exists $d \in F^*$ such that $o(d) = lcm(o(b), o(c)) = lcm(m, o(c))$. So $o(d) \geqslant m$, but because m is the maximum we have $o(d) = m$.

From $m = lcm(m, o(c))$, we have that $o(c)|m$, so for any $c \in F^*$, $c^m = 1$.

Finally let us consider the equation $x^m - 1 = 0$. This equation has at least $q-1$ solutions in F since all the elements of F^* satisfy it, so $m \geqslant q - 1$. This inequality combined with the fact that $m \mid (q - 1)$ are enough to say that $m = q - 1$. Hence b is a generator of F^*, which makes $(F^*, \cdot)$ a cyclic group.

□

Observation 1. In order to find d of the above theorem do the following:

1. If $gcd(o(b), o(c)) = 1$, then let us take $d = b \cdot c$. We can show that $o(d) = o(c) \cdot o(b) = lcm(o(c), o(b))$.

2. If $o(c)|o(b)$ take $d = b$ and if $o(b)|o(c)$ take $d = c$.

3. Otherwise, let $o(b) = m = p_1^{\alpha_1} p_2^{\alpha_t} ... p_t^{\alpha_t}$ and $o(c) = n = p_1^{\beta_1} p_2^{\beta_2} ... p_t^{\beta_t}$, where the exponents may also be zero. Let us define:

$$m' = \prod_{\alpha_i \geqslant \beta_i} p_i^{\alpha_i} \text{ and } n' = \prod_{\beta_i > \alpha_i} p_i^{\alpha_i}.$$

Since the previous case is excluded, n' and m' are both well defined. We can easily check the following:

$n'|n$, $m'|m$, $m' \cdot n' = \mathrm{lcm}(m, n)$, $\gcd(m', n') = 1$, $o(c^{\frac{n}{n'}}) = n'$, $o(b^{\frac{m}{m'}}) = m'$. So in this case we can take $d = c^{\frac{n}{n'}} \cdot b^{\frac{m}{m'}}$.

2.2 Cardinality of Subfields

Theorem 3. *Let F_q be a finite field with $q = p^m$. Any subfield K of F_q has cardinality p^l where $l|m$.*

Proof. Let $P = \{0, 1, 1_2, ..., 1_{p-1}\}$ be the prime subfield of F_q as in Theorem 1. Since $1 \in K$ we can say that P is also a subfield of K. So $card(K) = p^l$ for some positive integer l.

If we use Lagrange's Theorem on the fact that K is an additive subgroup of F we have $p^l \mid p^m$. Also if we use the same theorem on the fact that K^* is a multiplicative subgroup of F^* we have $(p^l - 1) \mid (p^m - 1)$.

Let $m = Q \cdot l + R$ with $R < l$. For some positive integer A, B we have

$$B(p^l-1) = p^m-1 = p^{Ql}p^R-1 = p^{Ql}p^R-p^R+p^R-1 = ((p^l)^Q-1)p^R+(p^R-1) = A(p^l-1)+(p^R-1).$$

It follows that $(B - A)(p^l - 1) = p^R - 1$, so $(p^l - 1) \mid (p^R - 1)$. Unless $R = 0$ we have $l \leqslant R$ which is a contradiction. So $l|m$.

□

The converse of this theorem is also true, but in order to prove that we need a lemma first.

Lemma 2. *Let F_q be a finite field, a, b any two random elements in F_q and l a random positive integer. The following hold:*

1. $(a + b)^{p^l} = a^{p^l} + b^{p^l}$.
2. $(-a)^{p^l} = -a^{p^l}$.

Proof. 1. Let us show the first equality for $l = 1$ first. From the binomial theorem we have that

$(a + b)^p = a^p + k_1 a^{p-1} b + k_2 a^{p-2} b^2 + ... + k_{p-2} a^2 b^{p-2} + k_{p-1} a b^{p-1} + b^p$, where $k_i = \binom{p}{i} \bmod p$, for $i = 1, 2, ..., p - 1$.

Since $\binom{p}{i} = \frac{p(p-1)...(p-i+1)}{i!}$ is always a positive integer we have that $i!$ divides $p(p - 1)...(p - i + 1)$. From the fact that p is prime we have that $\gcd(p, i!) = 1$

hence $i!$ divides $(p-1)...(p-i+1)$. It follows that $t = \frac{(p-1)...(p-i+1)}{i!}$ is a positive integer, therefore
$k_i = \binom{p}{i} \mathrm{mod} p = tp \mathrm{mod} p = 0$, for any $i = 1, 2, ..., p-1$.

The first equality of the lemma can be proved using the method of mathematical induction on l.

2. If p is odd then p^l is still odd, therefore our second equality is true in this case.
If p is even then p^l is also even so $(-a)^{p^l} = a^{p^l}$. Since p is also prime we have that $p = 2$, so $a^{p^l} = -a^{p^l}$, hence $(-a)^{p^l} = -a^{p^l}$.

□

Theorem 4. *Let* F *be any finite field of order* $q = p^m$ *and* l *any positive integer such that* $l|m$. *Then there exist* K *a subfield of* F *such that* $\mathrm{card}(K) = p^l$.

Proof. Let us define

$$K = \{x \in F, x^\delta = x\}, \text{ where } \delta = p^l.$$

Thanks to the above Lemma we can easily show that K is a subfield of F. It is easy to see that $\mathrm{card}(K) \leqslant \delta = p^l$ since the number of zeros of a polynomial can not exceed the degree. In order to prove the other inequality let y be one of the generators of F^*, i.e. $q-1$ is the smallest positive integer such that $y^{q-1} = 1$.

If $z = y^{\frac{p^m-1}{p^l-1}}$ we have that $o(z) = p^l - 1 = \delta - 1$. So the elements $0, 1, z, z^2, ..., z^{\delta-2}$ are all pairwise distinct and they are all in K because

$$(z^s)^\delta = (z^\delta)^s = (z^{\delta-1}z)^s = z^s.$$

So we can also say that $\mathrm{card}(G) \geqslant \delta = p^l$ which proves the Theorem. □

2.3 The Minimal Polynomial

Definition 3. Let $F_{q'}$ be an extension field of F_q (meaning that F_q is a subfield of $F_{q'}$) and let $a \in F^*_{q'}$. A nonzero monic polynomial $M_a(x) \in F_q[x]$ is called the minimal polynomial of a if and only if $M_a(x)$ is the least degree polynomial in $F_q[x]$ such that a is a zero.

Observation 2. From the above theorem we can show that $q' = q^t$, for some positive integer t.

Theorem 5. *With the same notation as Definition 3 we have*

1. *The minimal polynomial always exists and it is unique.*

2. *The minimal polynomial is irreducible in* $F_q[x]$.

3. *If* $s(x) \in F_q[x]$ *with* $s(a) = 0$ *then* $M_a(x)|s(x)$.

Proof. 1. Proof of existence: From Lagrange's Theorem for groups we can easily see $m(a) = 0$, where $m(x) = x^{q'} - x \in F_q[x]$. Since F_q is finite, the number of monic polynomials in $F_q[x]$ with degree less than or equal to q' is finite, so we can always select the monic smallest degree polynomial such that a is a zero.

Proof of uniqueness: Assume by contradiction that a has 2 non-identical minimal polynomials $M_1(x)$ and $M_2(x)$ with same degree d. Let $M(x) = M_1(x) - M_2(x) \in F_q[x]$. Since $M_1(x)$ and $M_2(x)$ are both monic with the same degree d, it follows that $degM(x) < d$. Hence $M(x)$ can not be a minimal polynomial for a. However $M(a) = M_1(a) - M_2(a) = 0 - 0 = 0$ which implies that $M(x)$ is equivalent to the zero polynomial. That is a contradiction since $M_1(x)$ and $M_2(x)$ are non-identical.

2. Assume $M_a(x) = f(x)g(x)$ is reducible in $F_q[x]$. Since $M_a(a) = 0$ then either $f(a) = 0$ or $g(a) = 0$ which contradicts the minimality.

3. For the last one let $s(x) = q(x)M_a(x) + r(x)$ in $F_q[x]$ with $deg(r(x)) < deg(M_a(x))$. Since $s(a) = M_a(a) = 0$ we have $r(a) = 0$ which contradicts the minimality of $M_a(x)$ unless $r(x) = 0$. So $M_a(x)|s(x)$.

□

We do have an algorithm on how to find the minimal polynomial. First let us denote with ω, one of the generators of $F^*_{q'}$, where $q' = q^t$ for some positive integer t . Let s be a positive integer such that $a = \omega^s$. With this notation we have

$$M_a(x) = (x - a)(x - a^q)(x - a^{2q})(x - a^{3q})...(x - a^{(k-1)q})$$

where k is the smallest positive integer such that $sq^k \equiv s(mod(q^t - 1))$. See ([4, Theorem 3.7.6, page 115]).

3 Cyclic Codes

In this chapter I will talk about Cyclic Codes, which is a very important class of Linear Codes. They are extremely useful in Coding Theory. Most of the work in this chapter is refereed to [4, chapter 4].

3.1 Definition of Linear and Cyclic Codes

Definition 4. Let F_q be a finite field with cardinality $q = p^m$. A *linear code* of length n over F_q is a subspace of the vector space ${F_q}^n$. Its elements are called codewords.

Definition 5. *Generator Matrix* of a linear code C is a matrix in which its rows are vectors of any given basis. The generator matrix is not unique.

Definition 6. *The minimum distance* of a linear code C is defined as

$$d_{min}(C) = min\{w(c), c \in C, c \neq 0\},$$

where $w(c)$ is called the weight of a codeword c and it is the number of nonzero entries in c.

Any linear code C is characterized by 3 quantities. Its length n, its dimension (as a linear subspace) k and its minimum distance d. We say C is a $[n, k, d]$ linear code.

Definition 7. Let C be a $[n, k, d]$ linear code over some finite field. C is called a *cyclic code* if and only if $(c_0, c_1, ..., c_{n-1}) \in C$ implies $(c_{n-1}, c_0, c_1, ..., c_{n-2}) \in C$.

3.2 The Canonical Generator

Definition 8. For any positive integer n and any finite field F_q let $R_n = F_q[x]/ < x^n - 1 >$ be the quotient ring modulo $x^n - 1$. We can define a map $\pi : {F_q}^n \to R_n$ such that

$$\pi((c_0, c_1, ..., c_{n-1})) = c_0 + c_1 x + ... + c_{n-1} x^{n-1}.$$

It is obvious that π is an isomrphism of vector spaces, however π is important because R_n is also a ring.

Theorem 6. *Let* C *be a* $[n, k, d]$ *cyclic code over some finite field* F_q. *The subset* $\pi(C) = \{\pi(c), c \in C\} \subseteq R_n$, *is an ideal of* R_n.

Proof. Since C is a subspace of F_q^n, $\pi(C)$ is a subspace of R_n, so it is enough to prove that $f(x) * \pi(c) \in \pi(C)$ for any $f(x) \in R_n$ and $c \in C$. With $*$ we denoted the usual multiplication in R_n.

Case 1

$f(x) = x$. If $c = (c_0, c_1, ..., c_{n-1})$ then

$$x*\pi(c) = x*(c_0+c_1x+...+c_{n-1}x^{n-1}) = (c_0x+c_1x^2+...+c_{n-2}x^{n-1}+c_{n-1}\cdot x^n)(mod(x^n-1))$$

$$= c_{n-1} + c_0x + ... + c_{n-2}x^{n-1} = \pi(c_{n-1}, c_0, c_1, ..., c_{n-2}) \in \pi(C)$$

since C is a cyclic code.

Case 2

$f(x) = x^s$ for some positive integer s. The proof in this case can be done very easily by using the method of mathematical induction on s.

Case 3

If $f(x) = f_0 + f_1x + ... + f_sx^s$ then

$$f(x) * \pi(c) = f_0(\pi(c)) + f_1(x * \pi(c)) + ... + f_s(x^s * \pi(c)).$$

From the previous cases and the fact that $\pi(C)$ is a subspace of R_n we can conclude that $f(x) * \pi(c) \in \pi(C)$.

□

Note that since π is an isomorphism we can identify C and $\pi(C)$.

It is well known that R_n is a principal ideal domain, which means that any ideal of R_n can be generated by only one polynomial.

In other words, for any cyclic code C over some F_q, there exists a polynomial $g_0(x) \in C$, such that $C =< g_0(x) >$, where

$$< g_0(x) >= \{f(x) * g_0(x) | f(x) \in R_n\}.$$

The above $g_0(x)$ is called a generator of C, but it may not be the only generator. In the next theorem we will try to find the generator that best describes the cyclic code. We will call that the canonical generator and will denote it with $g(x)$.

Theorem 7. *If* C *be a cyclic code of length* n *over some* F_q *then:*

1. *There exists a unique* $g = g(x) \in C$*, such that* $g(x)$ *is monic and* $deg(g(x)) \leqslant deg(c(x))$ *for any non-zero* $c = c(x) \in C$.

2. $C =< g(x) >$.

This $g(x)$ *is called the canonical generator.*

Proof. 1. The existence of $g(x)$ is obvious because we are working with finite sets. In case $g(x)$ is not monic, we can multiply $g(x)$ by the inverse of the leading coeficient and this new polynomial it is monic and will still be in C, because C is linear.

For the uniqueness part, we can use the same trick we used before. Assume we have 2 such non-identical polynomials $g_1(x)$ and $g_2(x)$ with above properties. So they are both monic and $deg(g_1(x)) = deg(g_2(x)) = d$. If $g(x) = g_1(x) - g_2(x)$ then we can easily see that $deg(g(x)) < d$. From the linearity of C, $g(x) \in C$. Also since $g_1(x), g_2(x)$ have minimal degree in C, it follows that $g(x)$ is identically the 0 polynomial. In that case we would have $g_1(x) \equiv g_2(x)$, which is a contradiction.

2. Since C is an ideal it is obvious that $< g(x) >\subseteq$ C.

   In order to prove the other inclusion let $f(x) \in$ C. We can write $f(x) = q(x)g(x) + r(x)$ where $\deg(r(x)) < \deg(g(x))$. Since $\deg(r(x)) < n$ and $\deg(f(x)) < n$ we have $\deg(q(x)g(x)) = \deg(f(x) - r(x)) < n$, so $g(x)q(x) = g(x) * r(x)$. It follows that $r(x) = f(x) - g(x) * q(x) \in$ C. Since $g(x)$ is the non-zero smallest degree polynomial in C we have $r(x) = 0$, therefore $f(x) = g(x)*q(x) \in< g(x) >$. □

Next we will use the canonical generator in order to find a basis and the dimension of a cyclic code.

Lemma 3. *The canonical generator* $g(x)$ *of the previous theorem divides* $x^n - 1$.

Proof. Write $x^n - 1 = g(x)h(x) + r(x)$ with $\deg(r(x)) < \deg(g(x))$. $r(x)$ does not belong in C unless it is the zero polynomial.

But $r(x) = -g(x)h(x) + (x^n - 1) = g(x) * (-h(x)) \in$ C. So $r(x) = 0$ and that concludes the proof. □

Definition 9. Let $g(x)$ be a canonical generator of some cyclic code C with length n. The polynomial $h(x) = \frac{x^n-1}{g(x)}$ is called the *check polynomial.*

Lemma 4. *Let* C *be a cyclic code of length* n*. Let* $g(x)$ *and* $h(x)$ *be respectively the canonical generator and check polynomial. Then*

$$C = \{g(x)f(x), \deg(f(x)) < \deg(h(x))\}.$$

Proof. It is enough to show $C \subseteq \{g(x)f(x), \deg(f(x)) < \deg(h(x))\}$.

Let $p(x) = g(x) * l(x) \in C$ for some $l(x) \in R_n$. Now let $l(x) = q(x)h(x) + r(x)$ where $\deg(r(x)) < \deg(h(x))$. So

$$p(x) = g(x)*(q(x)h(x)+r(x)) = g(x)*q(x)*h(x)+g(x)*r(x) = (x^n-1)*q(x)+g(x)*r(x)$$

$$= 0 + g(x) * r(x) = g(x)r(x).$$

This finishes the proof since $\deg(r(x)) < \deg(h(x))$. □

Lemma 5. *Let* C *be a cyclic code with length* n*, and let* $g(x)$ *and* $h(x)$ *be as above. Then* $\dim(C) = k$ *where* $k = \deg(h(x))$ *and a basis for* C *will be the set*

$$\Delta = \{g(x), x * g(x), x^2 * g(x), ..., x^{k-1} * g(x)\}.$$

Observation 3. We can show that $x * g(x) = xg(x)$, $x^2 * g(x) = x^2g(x)$,...,$x^{k-1} * g(x) = x^{x-1}g(x)$ that is why $card(\Delta) = k$.

Proof. The above lemma tells us that Δ spans C. So it is enough to prove that Δ is linearly independent.

Let $f_0 g(x) + f_1 x * g(x) + ... + f_{k-1} x^{k-1} * g(x) = 0$. The last equation can be written in the form $f(x) * g(x) = 0$, where $f(x) = f_0 + f_1 x + ... + f_{k-1} x^{k-1}$. So $(x^n - 1) | f(x)g(x)$.

Unless $f(x) = 0$, we have

$$n = \deg(x^n - 1) \leqslant \deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x)) < \deg(h(x)) + \deg(g(x)) =$$

$$\deg(h(x)g(x)) = \deg(x^n - 1) = n$$

This contradiction proves $f(x) = 0$ i.e. $f_0 = f_1 = ... = f_{k-1} = 0$. So Δ is linearly independent. □

The next theorem will describes all the generators of a cyclic code.

Theorem 8. *Let* $g(x)$ *be the canonical generator of a* $[n, k, d]$ *cyclic code* C*, with check polynomial* $h(x)$*. Another polynomial* $t(x) \in C$ *is a generator for* C *if and only if* $t(x) = g(x) \cdot p(x)$ *for some polynomial* $p(x)$ *with* $\gcd(p(x), h(x)) = 1$ *and* $\deg(p(x)) < \deg(h(x))$.

Proof. **Necessary condition**

Since $C =< t(x) >=< g(x) >$ and $g(x)$ is the canonical generator of C we have $t(x) = g(x) * p(x) = g(x)p(x)$ where $p(x)$ can be chosen such that $\deg(p(x)) < \deg(h(x))$. Now let us prove that $\gcd(p(x), h(x)) = 1$.

$t(x) = g(x) * p(x)$ but also $g(x) = t(x) * u(x)$ for some polynomial $u(x)$. So $g(x) = g(x) * p(x) * u(x)$. i.e.

$$g(x) = g(x)p(x)u(x) + s(x)(x^n - 1) = g(x)p(x)u(x) + s(x)h(x)g(x)$$

Since $F_q[x]$ has no zero-divisors, we can cancel $g(x)$ on both sides, so

$1 = p(x)u(x) + s(x)h(x)$, which implies that $\gcd(h(x), p(x)) = 1$.

Sufficient condition

Say $t(x) = g(x) \cdot p(x)$ with $\gcd(p(x)), h(x)) = 1$. Because we also have that $\deg(p(x)) < \deg(h(x))$ we can write $t(x) = g(x) * p(x)$. Let us show now that $C =< t(x) >$.

First let us take $f(x) \in< t(x) >$ so $f(x) = t(x) * v(x) = g(x) * p(x) * v(x) \in< g(x) >= C$.

Now let us prove the other inclusion by taking $f(x) \in C =< g(x) >$, $f(x) = f_0(x) * g(x)$, for some $f_0(x)$.

Since $\gcd(p(x), h(x)) = 1$ we can find polynomials $p_0(x), h_0(x)$ such that $p(x)p_0(x) + h(x)h_0(x) = 1$. Multiplying both sides by $g(x)$, we have

$$g(x) = p(x)p_0(x)g(x) + h_0(x)h(x)g(x) = p(x)g(x)p_0(x) + h_0(x)(x^n - 1).$$

So $g(x) = p(x) * g(x) * p_0(x) = [p(x) * g(x)] * p_0(x) = t(x) * p_0(x)$.

Finally $f(x) = f_0(x) * g(x) = f_0(x) * p_0(x) * t(x) \in< t(x) >$. □

Lemma 6. *Let $g(x)$ be a monic polynomial with coeficients in F_q such that $g(x)|(x^n - 1)$. Define C to be the linear code generated by $g(x)$. C is cyclic and its canonical generator is $g(x)$.*

Proof. It is very easy to check that C is a cyclic code. Now we need to show that $g(x)$ has the least degree in C.

Assume that $g_0(x)$ is the canonical generator of C. Since both $g(x)$ and $g_0(x)$ are generators for the same code C we have $g_0(x) = f(x) * g(x)$, for some $f(x) \in R_n$. Also if $h(x) = \frac{x^n-1}{g(x)}$ then $g_0(x) * h(x) = g(x) * f(x) * h(x) = 0$.

So $g_0(x)h(x) = s(x)(x^n-1) = h(x)g(x)s(x)$ i.e. $g_0(x) = g(x)s(x)$, hence $g(x)|g_0(x)$. In an identical way we can prove that $g_0(x)|g(x)$. Because $g(x), g_0(x)$ are both monic we have $g(x) = g_0(x)$ which is exactly what we need to show.

□

3.3 Factorizing $x^n - 1$

From before, in order to find cyclic codes, we need to find divisors of $x^n - 1$ over some $F_q[x]$. The following theorem will show us how to factorize $x^n - 1$ into irreducible factors.

Theorem 9. *Let F_q be a finite field and n a positive integer with $gcd(q, n) = 1$. $x^n - 1$ can be factorized into linear factors over some extension field F_{q^t} of F_q.*

Proof. Since $gcd(q, n) = 1$ we can say that $q mod(n)$ has a multiplicative inverse in ring Z_n, thus $q mod(n)$ is an element of the group Z_n^*. Here Z_n^* is the subset of Z_n containing only those elements which admit multiplicative inverse.

Since Z_n^* is finite, there exists a positive integer t such that $q^t \equiv 1 mod(n)$. For example $t = card(Z_n^*)$ will work. With no loss of generality we can assume t to be the smallest positive integer with the above property. The notation for t is $t = ord_n q$.

Now let us look at the field F_{q^t}. Recall that $(F_{q^t}^*, \cdot)$ is a cyclic multiplicative group, hence there exists g_0 a generator of $(F_{q^t}^*, \cdot)$. Let us define $g = g_0^{\frac{q^t-1}{n}}$. It is easy to check that $g^n = 1$. Furthermore n is the smallest positive integer such that $g^n = 1$ otherwise g_0 would not be a generator. In this case we say the order of g under the multiplicative group $(F_{q^t}^*, \cdot)$ is equals to n.

Let analyze the set $\Lambda = \{g^i, 0 \leqslant i \leqslant n-1\}$. Because the order of g under the above multiplicative group is n, all the elements in Λ are pairwise distinct and $(g^i)^n = (g^n)^i = 1^n = 1$ for any i, $0 \leqslant i \leqslant n-1$. This tells us that the polynomial $x^n - 1$ has n distinct roots, which are $g^0 = 1$ g, g^2, g^3,...,g^{n-1}. So

$$(x^n - 1) = (x-1)(x-g)(x-g^2)...(x-g^{n-1}).$$

□

Since $x-1$ is irreducible in F_q, in order to factorize x^n-1 as a product of irreducible polynomials in $F_q[x]$ first let us analyze the minimal polynomial of g, denoted by $M_g(x)$.

From the properties of the minimal polynomials we know that $M_g(x)$ is irreducible in $F_q[x]$ and $M_g(x)|x^n-1$. So $M_g(x)$ contains some of the terms of the above x^n-1. Next we will find the minimal polynomial of g^s, where s is the first index such that $(x-g^s)$ is not in $M_g(x)$. We will keep doing that until all the terms of x^n-1 are taken.

4 Euclidean and Hermitian Dual of Linear Codes

It is well known that for any subspace M of some Real/Complex vector space W we can define the so called Euclidean Dual Space/Hermitian Dual Space. It is seen that if we apply the same ideas on linear codes we can obtain other, very interesting linear codes. Most of the work in this Chapter is refereed to [4, chapter 1.3].

4.1 Euclidean Dual of Linear Codes

Definition 10. Let F_q be a finite field and let $u = (u_0, u_1, ..., u_{n-1})$ and $v = (v_0, v_1, ..., v_{n-1})$ be two elements of F_q^n. The inner product of those two vectors is the scalar in F_q denoted by $< u, v >$ and defined as

$$< u, v >= u_0v_0 + u_1v_1 + ... + u_{n-1}v_{n-1}.$$

There is only one property that the inner product satisfies over the field of real numbers, but not over finite fields. We may find a non-zero codeword $u \in F_q^n$ such that $< u, u >= 0$. For example, in F_q^q take $u = (1, 1, 1, ..., 1)$.

Definition 11. If C is a linear code of length n over F_q we can define

$$C^\perp = \{x \in F_q^n, \text{such that } < x, c >= 0, \text{for any } c \in C\}$$

.

$C^\perp$ is called *the Euclidean dual* or simply *the dual* of the linear code C.

Over finite fields, because the failed property of the inner product, the intersection of C and $C^\perp$ is not necessarily $\{0\}$, however the other properties are satisfied.

Proposition 1. *If C is a linear of length n over F_q then:*

1. *$C^\perp$ is a linear code of length n over F_q.*
2. *$\dim(C^\perp) = n - \dim(C)$.*
3. *$(C^\perp)^\perp = C$.*
4. *If C_1 and C_2 are linear codes such that $C_1 \subseteq C_2$ then $C_2^\perp \subseteq C_1^\perp$.*

Proof. Properties 1,3 and 4 are straight forward from the definition. For property 2, let $k = \dim(C)$ and let $B = \{b_1...., b_k\}$ be a basis for C. We know that $x \in C^\perp$ if and only if $< x, b_i >= 0$ for any $i = 1, 2, .., k$. If we consider x to be a variable, the equations $< x, b_i >= 0$ will give us an homogeneous linear system. The rank of the coefficients matrix of the above linear system is k (since B is a basis) and $C^\perp$ is the solution space the same linear system. Hence $\dim(C^\perp) = n - k$. □

Next we will recall a result that says the dual of a cyclic code is still a cyclic code.

Notation 1. For any codeword $f = (f_0, f_1, ..., f_{n-1})$ in F_q^n let

$$f^{[1]} = (f_{n-1}, f_0, f_1, ...f_{n-2}),$$
$$f^{[2]} = (f^{[1]})^{[1]} = (f_{n-2}, f_{n-1}, f_0, ..., f_{n-3}),$$
$$f^{[3]} = (f^{[2]})^{[1]} = (f_{n-3}, f_{n-2}, f_{n-1}, ..., f_{n-4}),$$
$$...$$
$$f^{[n]} = (f^{[n-1]})^{[1]} \text{ for any positive integer } n .$$

Proposition 2. *The following statements are true:*

1. *Let* C *be a linear code of length* n *over* F_q. C *is a cyclic code if and only if* $f \in C$ *implies* $f^{[1]} \in C$.

2. *Let* C *be a cyclic code of length* n *over* F_q. *If* $f \in C$, *then* $f^{[m]} \in C$ *for any positive integer* m.

3. *If* f *is an element in* F_q^n, *then* $f^{[n]} = f$. *Also for any two positive integers* s, t *we have* $f^{[p+s]} = (f^{[p]})^{[s]}$.

4. *If* f *and* g *are two elements in* F_q^n, *then* $< f, g >=< f^{[1]}, g^{[1]} >$. *Furthermore for any positive integer* m *we have* $< f, g >=< f^{[m]}, g^{[m]} >$.

5. *Let* π *be the vector space isomorphism of Definition 8 from* F_q^n *to* R_n *and let* $*$ *be the multiplication in* R_n. *For any* $c \in F_q^n$ *let us define* $\pi(c) = c(x)$. *If* $d, t \in F_q^n$ *and* j *is a positive integer, then*

$$t(x) = x^j * d(x) \textit{ if and only if } t = d^{[j]}.$$

Proof. Properties 1 through 4 are obvious. Property 5 is proved first for $j = 1$, using the same technique as in Case 1 of Theorem 6. After that we can use the method of mathematical induction. □

Theorem 10. *Let* C *be a cyclic code of length* n *over some finite field* F_q^n. *Then* $C^\perp$ *is also a cyclic code of length* n *over the same* F_q.

Proof. It is enough to show that $f \in C^\perp$ implies $f^{[1]} \in C^\perp$. In other words we have to show that, for any $c \in C$, $< f^{[1]}, c >= 0$

From the property 2 of Proposition 2 we can say that $c^{[n-1]} \in C$. Since $f \in C^\perp$ we have $< f, c^{[n-1]} >= 0$. From property 4 of Proposition 2 we have $< f^{[1]}, (c^{[n-1]})^{[1]} >= 0$. Finally if we apply both conclusions of property 3 of Proposition 2 we have $< f^{[1]}, c >= 0$. □

4.2 Hermitian Dual of Linear Codes

Definition 12. Let F_{q^2}, be a finite field with cardinallity q^2 where q is a prime power. Also let $a \in F_{q^2}$. The element a^q is called *the conjugate* of a.

This conjugate satisfies all the properties of the conjugate in the field of complex numbers.

1. $(a+b)^q = a^q + b^q$. This is true from Lemma 2.
2. $(-a)^q = -a^q$. Also true from Lemma 2.
3. $(ab)^q = a^q b^q$ and $(\frac{a}{b})^q = \frac{a^q}{b^q}$
4. If $a \in F_q$, where F_q is the subfield of F_{q^2} of cardinallity q, then $a^q = a$. This is true from Lagrange's theorem for groups.

With the above information we can now define the Hermitian dual code of a linear code.

Definition 13. Let F_{q^2} be a finite field as above and let $u = (u_0, u_1, ..., u_{n-1})$ and $v = (v_0, v_1, ..., v_{n-1})$ be two elements of $F_{q^2}^n$. The *Hermitian inner product* is the scalar in F_{q^2} denoted by $< u, v >_H$ and defined as

$$< u, v >_H = u_0^q v_0 + u_1^q v_1 + ... + u_{n-1}^q v_{n-1}.$$

Definition 14. If C is a linear code of length n over F_{q^2} then we can define

$$C^{\perp_H} = \{x \in F_{q^2}^n, \text{ such that } < x, c >_H = 0, \text{ for any } c \in C\}.$$

This $C^{\perp_H}$ is called the *Hermitian Dual* of the linear code C.

The properties we had for the Euclidean dual work fine for the Hermitian dual too. So if C is a linear code of length n over some F_{q^2} then

1. $C^{\perp_H}$ is a linear code of length n over $F_{q^2}^n$.
2. $\dim(C^{\perp_H}) = n - \dim(C)$.
3. $(C^{\perp_H})^{\perp_H} = C$.
4. If C_1, C_2 are linear codes such that $C_1 \subseteq C_2$ then $C_2^{\perp_H} \subseteq C_1^{\perp_H}$.

The following theorem is also true.

Theorem 11. *Let C be a cyclic code of length n over some finite field F_{q^2}. Then $C^{\perp_H}$ is also a cyclic code of length n over the same F_{q^2}.*

Proof. Since property 4 of Proposition 2 is also true for the Hermitian inner product, the proof of this theorem can be done in the same way as in the Euclidean case. □

5 Matrix Product Codes

One way of constructing linear codes is by combining existing codes. In 2001, Blackmore and Norton [13] introduced the interesting and useful construction of matrix-product codes over finite fields. Some previously well-known constructions such as the Plotkins construction and the Reed-Muller ternary construction are special cases of such construction.

5.1 Definition and Dimension of Matrix Product Codes

Definition 15. Let $C_1, C_2, ..., C_n$ be linear codes of length m over some F_q and A be an nxn matrix. Let us denoted by C the set of all elements of the type $(c_1, c_2, ..., c_n)A$, where for $i = 1, 2, .., n$, $c_i \in C_i$ and it is taken as a column. It is obvious that the elements of C are mxn matrices, but we can see them as rows by reading them in column-major order.

Column major-order means that if $d_1, d_2, ..., d_n$ are the columns in order of some matrix D, then D can be identified with the row matrix $d = (d_1^T d_2^T ... d_n^T)$.

With this agreement C is a linear code of length mn over F_q and it called the *Matrix Product Code.* The notation we are using for C is $(C_1, C_2, ..., C_n)A$.

The idea of matrix product code comes from some well-known examples.

Example 1. **Plotkin's construction.** Let C_1, C_2 be respectively (n, k_1, d_1) and (n, k_2, d_2) linear codes. Plotkin's construction is the linear code $C = \{(c_1, c_1 + c_2), c_1 \in C_1, c_2 \in C_2\}$. It is known that C is a $(2n, k_1 + k_2, min\{2d_1, d_2\})$ linear code. It turns out that $C = (C_1, C_2)\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Example 2. **Reed-Muller ternary construction**. Let C_1, C_2, C_3 be respectively (n, k_1, d_1), (n, k_2, d_2) and (n, k_3, d_3) linear codes. Reed-Muller ternary construction is the code

$C = \{(c_1 + c_2 + c_3, 2c_1 + c_2, c_1), c_1 \in C_1, c_2 \in C_2, c_3 \in C_3\}$. It is known that C is a $(3n, k_1 + k_2 + k_3, min\{3d_1, 2d_2, d_3\})$ linear code. It turns out that $C = (C_1, C_2, C_3)$ $\begin{pmatrix} 1 & 2 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$.

The first theorem is about the dimension of matrix product code.

Theorem 12. *Let* $C_1, ..., C_n$*, be linear codes of length* m *with* $dim(C_i) = k_i$*. Also let* $C = (C_1, ..., C_n)A$*, where* A *is an* nxn *matrix. With this notation we have that* $dim(C) \leqslant k_1 + k_2 + ... + k_n$*. Furthermore if* A *is non-singular we have that* $dim(C) = k_1 + k_2 + ... + k_n$.

Proof. Let us define the linear transformation $\sigma : C_1 \times C_2 \times ... \times C_n \to C$ with

$$\sigma(c_1, c_2, ..., c_n) = (c_1, c_2, ..., c_n)A.$$

It is easy to see that σ is onto, therefore from the rank nullity theorem we have $dim(C) \leqslant dim(C_1 \times C_2 \times ... \times C_n) = k_1 + k_2 + ... + k_n$. It is obvious that if A is non-singular then σ is also one to one, hence the above inequality holds as equality. □

5.2 Non-Singular by Column Matrices

Next we will prove a theorem for the minimum distance of matrix product code, but it requires the matrix A to be as in definition below.

Definition 16. A square nxn matrix M is said to be *Non-Singular by Columns (NSC)* if and only if, for any $t = 1, 2, ..., n$ the minor obtained from "intersecting" the first t rows with any t columns has a non-zero determinant.

Theorem 13. *Let* $C_1, ..., C_n$*, be linear codes of length* m *with* $d_{min}(C_i) = d_i$*. Also let* $C = (C_1, ..., C_n)A$ *where* A *is an* nxn *NSC matrix. If* $d = d_{min}(C)$ *then*
$d \geqslant d^* = min\{nd_1, (n-1)d_2, ..., 2d_{n-1}, d_n\}$.

Proof. We need to show that for any $c \in C$, $c \neq \mathbf{0}$ the number of non-zero entries in c (called the $weight(c)$) is bigger than or equal to d^*. Since $c \in C$ there exist $c_i \in C_i$, such that $c = (c_1, c_2, ..., c_n)A$. Remember that those $c_i's$ are taken in column therefore we can denote them as follows.

$$c_1 = (c_{11}, c_{21}, c_{31}, ..., c_{m1})^T,$$
$$c_2 = (c_{12}, c_{22}, c_{32}, ..., c_{m2})^T,$$
$$...$$
$$c_n = (c_{1n}, c_{2n}, c_{3n}, ..., c_{mn})^T.$$

With this notation we can see $(c_1, c_2, ..., c_n)$ as an mxn matrix with c_{ij} the $(i,j)-th$ entry. If we define the $(i,j)-th$ entry of A with a_{ij} and the $(i,j)-th$ entry of C with d_{ij} we have
$d_{ij} = c_{i1}a_{1j} + c_{i2}a_{2j} + ... + c_{in}a_{nj}$. Here we are considering the elements of C as mxn matrices.

We need to show now that $d_{ij} \neq 0$ for more then d^* values of $i = 1, 2, ..., m$ and $j = 1, 2, ..., n$.

Since $c \neq \mathbf{0}$ we can define $t = max\{h \in \{1, 2, ..., n\}, c_h \neq \mathbf{0}\}$. With this notation it is easy to check that $d_{ij} = c_{i1}a_{1j} + c_{i2}a_{2j} + ... + c_{it}a_{tj}$.

Claim: If for some $i = 1, 2, ..., n$, $c_{it} \neq 0$ then $d_{ij} \neq 0$ for at least $n - t + 1$ values of $j = 1, 2, ..., n$.

Let us finish the proof of the theorem assuming the claim is true. Since $d_{min}(C_t) = d_t$ we have that $c_{it} \neq 0$ for at least d_t values of $i = 1, 2, ..., n$. Therefore $d_{ij} \neq 0$ for at least d_t values of $i = 1, 2, .., n$ and $n - t + 1$ values of $j = 1, 2, .., n$. Hence $weight(c) \geqslant (n - t + 1)d_t \geqslant d^*$. Let now prove the claim.

Prove of the Claim: Fix i, such that $c_{it} \neq 0$ and assume by contradiction that there exist $n - (n - t + 1) + 1 = t$ values of $j = 1, 2, ..., n$ such that $d_{ij} = 0$. If we call them $j_1, j_2, ..., j_t$ we have the following homogeneous linear system

$$\begin{aligned} d_{ij_1} &= c_{i1}a_{1j_1} + c_{i2}a_{2j_1} + ... + c_{it}a_{tj_1} = 0 \\ d_{ij_2} &= c_{i1}a_{1j_2} + c_{i2}a_{2j_2} + ... + c_{it}a_{tj_2} = 0 \\ &.......................... \\ d_{ij_t} &= c_{i1}a_{1j_t} + c_{i2}a_{2j_t} + ... + c_{it}a_{tj_t} = 0 \end{aligned}$$

with variables $c_{i1}, c_{i2}, ..., c_{it}$. The coefficient matrix of this linear system is

$$\begin{pmatrix} a_{1j_1} & a_{1j_2} & ... & a_{1j_t} \\ a_{2j_1} & a_{2j_2} & ... & a_{2j_t} \\ ... & ... & ... & ... \\ a_{tj_1} & a_{tj_2} & ... & a_{tj_t} \end{pmatrix}.$$

Since A is NSC the above matrix has a non-zero determinant; hence from Kramer's rule the trivial solution is the only solution. This contradicts the fact that $c_{it} \neq 0$. □

5.3 The Dual of Matrix Product Codes

The next theorem will give us a formula for the dual of the matrix product code.

Theorem 14. *Let* $C = (C_1, C_2, ..., C_n)A$ *as above, and let us assume that* A *is a non-singular* nxn *matrix. The dual of* C *is given by the formula*

$$C^{\perp} = (C_1^{\perp}, C_2^{\perp}, ..., C_n^{\perp})(A^{-1})^T.$$

Observation 4. In this proof I will assume that the elements of $C, C^{\perp}$ are $m \times n$ matrices and for any 2 matrices P, Q with the same size, say $t \times s$ we can define the dot product $< P, Q >$ in the same way as codewords. So

$$< P, Q >= \sum_{i,j=1}^{t,s} p_{ij}q_{ij}, \tag{1}$$

where p_{ij} and q_{ij} are respectively the $(i,j) - th$ entry of matrices P and Q.

Proof. Let $W = (C_1^{\perp}, C_2^{\perp}, ..., C_n^{\perp})(A^{-1})^T$. In order to prove that $W = C^{\perp}$ we need to show two things.

1. $dim(C^{\perp}) = dim(W)$.

2. For any $c \in C$ and $w \in W$, $< c, w >= 0$.

Let start with the first one.

1. $dim(C^{\perp}) = mn - dim(C) = mn - dim(C_1) - dim(C_2) - ... - dim(C_n)=$
   $(m - dim(C_1)) + (m - dim(C_2)) + ... + (m - dim(C_n))=$
   $dim(C_1^{\perp}) + dim(C_2^{\perp}) + ... + dim(C_n^{\perp}) = dim(W)$.

2. Let $c = (c_1, c_2, ..., c_n)A \in C$, for some $c_i \in C_i$. Also let $w = (w_1, w_2, ..., w_n)B \in W$, for some $w_i \in C_i^\perp$ and $B = (A^{-1})^T$.

   Let $R_1, R_2, ...R_n$ be the rows of A in order, also let $Q_1, Q_2, ..., Q_n$ be the rows of B in order ($Q_1^T, Q_2^T, ..., Q_n^T$ are the columns of A^{-1} in order). It is easy to check that $c = c_1R_1 + c_2R_2 + ... + c_nR_n$ and $w = w_1Q_1 + w_2Q_2 + ... + w_nQ_n$. If we show that for any $i, j = 1, 2, ..., n$, $< c_iR_i, w_jQ_j >= 0$ then $< c, w >= 0$.

   Case 1: Let $i \neq j$. If $c_i = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ ... \\ \alpha_m \end{pmatrix}$ and $w_j = \begin{pmatrix} \beta_1 \\ \beta_2 \\ ... \\ \beta_m \end{pmatrix}$ then $c_iR_i = \begin{pmatrix} \alpha_1R_i \\ \alpha_2R_i \\ ... \\ \alpha_mR_i \end{pmatrix}$ and $w_jQ_j = \begin{pmatrix} \beta_1Q_j \\ \beta_2Q_j \\ ... \\ \beta_mQ_j \end{pmatrix}$. Since $< R_i, Q_j >= (AA^{-1})(i, j) = 0$ it follows $< c_iR_i, w_jQ_j >= 0$.

   Case 2: Let $i = j$. In this case if $R_i = (\alpha_1, \alpha_2, ..., \alpha_n)$ and $Q_i = (\beta_1, \beta_2, ..., \beta_n)$ then $c_iR_i = (\alpha_1c_i, \alpha_2c_i, ..., \alpha_nc_i)$ and $w_iQ_i = (\beta_1w_i, \beta_2w_i, ..., \beta_nw_i)$. Since $c_i \in C_i$ and $w_i \in C_i^\perp$ we have $< c_i, w_i >= 0$, therefore $< c_iR_i, w_iQ_i >= 0$.

□

In the last theorem if we take A to be non-singular by columns, $(A^{-1})^T$ may not be non-singular by columns. In order to fix that, for any positive integer n we can define the square nxn matrix $J_n = \begin{pmatrix} 0 & 0 & ... & 0 & 1 \\ 0 & 0 & ... & 1 & 0 \\ ... & ... & ... & ... & ... \\ 0 & 1 & ... & 0 & 0 \\ 1 & 0 & ... & 0 & 0 \end{pmatrix}$.

We can easily check that $(C_1^\perp, C_2^\perp, ..., C_n^\perp) = (C_n^\perp, C_{n-1}^\perp, ..., C_1^\perp) \cdot J_n$, therefore the above theorem transforms to

$$((C_1, C_2, ..., C_n)A)^\perp = (C_n^\perp, C_{n-1}^\perp, ..., C_1^\perp) \cdot J_n \cdot (A^{-1})^T.$$

It turns out that the next theorem is true.

Theorem 15. *If A is a given NSC square matrix, then $J \cdot (A^{-1})^T$ is also NSC.*

Observation 5. In the following we will drop the index n from J_n for simplicity. There will be no confusion since the index n will be understood from the given data. In the above theorem the size of J will have be the same as the size of A.

Before we prove Theorem 15 we need to prove some Lemmas first.

Lemma 7. *Let $B = JA$ and $C = AJ$, where J is the above $n \times n$ matrix and A is a random nxn matrix. If α_{ij}, β_{ij} and γ_{ij} are respectively the $(i, j) - th$ entry of A, B and C, then for any $i, j = 1, 2, ..., n$, $\beta_{ij} = \alpha_{n-i+1,j}$ and $\gamma_{ij} = \alpha_{i,n+1-j}$.*

Observation 6. In other words, if $R_1, R_2, ..., R_n$ are the rows of A in order and $C_1, C_2, ..., C_n$ are the columns of A in order, then the rows of B in order would be $R_n, R_{n-1}, ..., R_1$ and the columns of C in order would be $C_n, C_{n-1}, ..., C_1$.

Proof. The proof is straightforward from the definition of matrix multiplication and the fact that the $(i, j) - th$ term of J is equals to 1 if $i + j = n + 1$ and 0 otherwise. □

Lemma 8. *Let A be a non-singular $n \times n$ matrix and π a permutation of $\{1, 2, 3, ..., n\}$. Also let $C_1, ..., C_n$ be the columns of A in order and let $R_1, R_2, ..., R_n$ be the rows of A^{-1} in order. Let us denote by B the $n \times n$ matrix such that its columns in order would be $C_{\pi(1)}, C_{\pi(2)}, ..., C_{\pi(n)}$ and B_0 the $n \times n$ matrix such that its rows in order would be $R_{\pi(1)}, R_{\pi(2)}, ..., R_{\pi(n)}$. From these conditions we can say that $B_0 = B^{-1}$.*

Proof. The proof will be done by evaluating $B_0 \cdot B$ in blocks. The blocks for B_0 will be its Rows and the blocks for B will be its columns.

$$B_0 \cdot B = \begin{pmatrix} R_{\pi(1)} \\ R_{\pi(2)} \\ ... \\ R_{\pi(n)} \end{pmatrix} \cdot \begin{pmatrix} C_{\pi(1)} & C_{\pi(2)} & ... & C_{\pi(n)} \end{pmatrix} =$$

$$\begin{pmatrix} < R_{\pi(1)}, C_{\pi(1)} > & < R_{\pi(1)}, C_{\pi(2)} > & ... & < R_{\pi(1)}, C_{\pi(n)} > \\ < R_{\pi(2)}, C_{\pi(1)} > & < R_{\pi(2)}, C_{\pi(2)} > & ... & < R_{\pi(2)}, C_{\pi(n)} > \\ ... & ... & ... & ... \\ < R_{\pi(n)}, C_{\pi(1)} > & < R_{\pi(n)}, C_{\pi(2)} > & ... & < R_{\pi(n)}, C_{\pi(n)} > \end{pmatrix}$$

Remember that C_i's are the columns of A and R_j's are the rows of A^{-1}, therefore $< R_{\pi(j)}, C_{\pi(i)} >$ is equals to 1 when $i = j$ and 0 when $i \neq j$. So $B_0 \cdot B = I$. □

Lemma 9. *The idea of this lemma is taken from the Schur's Complement of a block matrix. See [21, page 6, relations (17) (18) and (19)].*

Let $X = \begin{pmatrix} P & Q \\ R & S \end{pmatrix}$ *be a non-singular matrix of size* $(n+m) \times (n+m)$*, where* P, Q, R, S *are matrices with sizes respectively* $n \times n, n \times m, m \times n, m \times m$.

Let $X^{-1} = \begin{pmatrix} P_0 & Q_0 \\ R_0 & S_0 \end{pmatrix}$ *where the sizes of matrices* P_0, Q_0, R_0, S_0 *are respectively the same as of* P, Q, R, S. *If* P *is non-singular then* S_0 *is also non-singular.*

Observation 7. Note that if $Y = \begin{pmatrix} P' & Q' \\ R' & S' \end{pmatrix}$ is a matrix of size $(n + m) \times (n + m)$, where P', Q', R', S' are matrices with same size as respectively P, Q, R, S then it possible to multiply XY in blocks and the sizes of the blocks of XY will be the same as the sizes of the blocks of X.

Proof. Let us define $L_1 = \begin{pmatrix} I_n & P^{-1}Q \\ \mathbf{0} & I_m \end{pmatrix}$, $L_2 = \begin{pmatrix} P & \mathbf{0} \\ \mathbf{0} & -RP^{-1}Q + S \end{pmatrix}$ and $L_3 = \begin{pmatrix} I_n & \mathbf{0} \\ RP^{-1} & I_m \end{pmatrix}$

Note that matrices L_1, L_2, L_3 have the same size as X and also their blocks have identical sizes as the blocks of X.

It is easy to check by definition that L_1, L_3 are non-singular and $L_1^{-1} = \begin{pmatrix} I_n & -P^{-1}Q \\ \mathbf{0} & I_m \end{pmatrix}$, $L_3^{-1} = \begin{pmatrix} I_n & \mathbf{0} \\ -RP^{-1} & I_m \end{pmatrix}$. Now let us show that $X = L_3 L_2 L_1$.

$$\begin{aligned} L_3 \cdot L_2 \cdot L_1 &= \begin{pmatrix} I_n & \mathbf{0} \\ RP^{-1} & I_m \end{pmatrix} \begin{pmatrix} P & \mathbf{0} \\ \mathbf{0} & -RP^{-1}Q + S \end{pmatrix} \begin{pmatrix} I_n & P^{-1}Q \\ \mathbf{0} & I_m \end{pmatrix} \\ &= \begin{pmatrix} P & \mathbf{0} \\ R & -RP^{-1}Q + S \end{pmatrix} \begin{pmatrix} I_n & P^{-1}Q \\ \mathbf{0} & I_m \end{pmatrix} = \begin{pmatrix} P & Q \\ R & S \end{pmatrix} = X \end{aligned}$$

Since X, L_1, L_3 are non-singular then L_2 is non-singular. L_2 non-singular implies that $-RP^{-1}Q + S$ is also non-singular and $L_2^{-1} = \begin{pmatrix} P^{-1} & \mathbf{0} \\ \mathbf{0} & (-RP^{-1}Q + S)^{-1} \end{pmatrix}$.

From $X = L_3 L_2 L_1$ we have

$$\begin{aligned} X^{-1} = L_1^{-1} L_2^{-1} L_3^{-1} &= \begin{pmatrix} I_n & -P^{-1}Q \\ \mathbf{0} & I_m \end{pmatrix} \begin{pmatrix} P^{-1} & \mathbf{0} \\ \mathbf{0} & (-RP^{-1}Q + S)^{-1} \end{pmatrix} \begin{pmatrix} I_n & \mathbf{0} \\ -RP^{-1} & I_m \end{pmatrix} \\ &= \begin{pmatrix} P^{-1} & -P^{-1}Q(-RP^{-1}Q + S)^{-1} \\ \mathbf{0} & (-RP^{-1}Q + S)^{-1} \end{pmatrix} \begin{pmatrix} I_n & \mathbf{0} \\ -RP^{-1} & I_m \end{pmatrix} \\ &= \begin{pmatrix} P^{-1} + P^{-1}Q(-RP^{-1}Q + S)^{-1}RP^{-1} & P^{-1}Q(-RP^{-1}Q + S)^{-1} \\ -(-RP^{-1}Q + S)^{-1}RP^{-1} & (-RP^{-1}Q + S)^{-1} \end{pmatrix} \end{aligned}$$

It follows $S_0 = (-RP^{-1}Q + S)^{-1}$, so S_0 is non-singular. □

Now it is time to prove **Theorem 15**

Proof. A is a given nxn non-singular by columns (NSC) matrix. We need to prove that $D = J(A^{-1})^T$ is also NSC.

The proof will be done using the definition, but first let us denote by $\alpha_{ij}, \beta_{ij}, \delta_{ij}$ respectively the $(i, j) - th$ entry of A, $A^{-1}$and D.

Let $t \in \{1, 2, ..., n\}$ be a random integer and let $j_1, j_2, ..., j_t$ be the indices in increasing order of t random chosen columns of D. Also let M be the minor obtain from "intersecting" the first t rows of D with columns $j_1, j_2, ..., j_t$. All we need to prove is $\det(M) \neq 0$.

From Lemma 7 we have

$$M = \begin{pmatrix} \delta_{1j_1} & \delta_{1j_2} & ... & \delta_{1j_t} \\ \delta_{2j_1} & \delta_{2j_2} & ... & \delta_{2j_t} \\ ... & ... & ... & ... \\ \delta_{tj_1} & \delta_{tj_2} & ... & \delta_{tj_t} \end{pmatrix} = \begin{pmatrix} \beta_{j_1,n} & \beta_{j_2,n} & ... & \beta_{j_t,n} \\ \beta_{j_1,n-1} & \beta_{j_2,n-1} & ... & \beta_{j_t,n-1} \\ ... & ... & ... & ... \\ \beta_{j_1,n-t+1} & \beta_{j_2,n-t+1} & ... & \beta_{j_t,n-t+1} \end{pmatrix}$$

Next we put $\{k_1, k_2, ..., k_{n-t}\}$=$\{1, 2, ..., n\} - \{j_1, j_2, ..., j_t\}$ with $k_1 < k_2 < ... < k_{n-t}$ and let us define

$$A_0 = \begin{pmatrix} \alpha_{1k_1} & \alpha_{1k_2} & ... & \alpha_{1k_{n-t}} & \alpha_{1j_1} & \alpha_{1j_2} & ... & \alpha_{1j_t} \\ \alpha_{2k_1} & \alpha_{2k_2} & ... & \alpha_{2k_{n-t}} & \alpha_{2j_1} & \alpha_{2j_2} & ... & \alpha_{2j_t} \\ ... & ... & ... & ... & ... & ... & ... & ... \\ \alpha_{nk_1} & \alpha_{nk_2} & ... & \alpha_{nk_{n-t}} & \alpha_{nj_1} & \alpha_{nj_2} & ... & \alpha_{nj_t} \end{pmatrix}$$

It is easy to see that A_0 is a column permutation of A, therefore A_0 is NSC. From Lemma 8 we have

$$A_0^{-1} = \begin{pmatrix} \beta_{k_1,1} & \beta_{k_1,2} & \dots & \beta_{k_1,n} \\ \beta_{k_2,1} & \beta_{k_2,2} & \dots & \beta_{k_2,n} \\ \dots & \dots & \dots & \dots \\ \beta_{k_{n-t},1} & \beta_{k_{n-t},2} & \dots & \beta_{k_{n-t},n} \\ \beta_{j_1,1} & \beta_{j_1,2} & \dots & \beta_{j_1,n} \\ \beta_{j_2,1} & \beta_{j_2,2} & \dots & \beta_{j_2,n} \\ \dots & \dots & \dots & \dots \\ \beta_{j_t,1} & \beta_{j_t,2} & \dots & \beta_{j_t,n} \end{pmatrix}$$

Now we will apply Lemma 9 for $X = A_0$ and P the intersection of the first $n - t$ rows with $n - t$ columns of A_0. $X = A_0$ and P are non-singular because A_0 is NSC. Using the above Lemma we can say that also S_0 is non-singular, where S_0 is obtained from A_0^{-1} intersecting the last t rows with the last t columns. If we do that we obtain

$$S_0 = \begin{pmatrix} \beta_{j_1,n-t+1} & \beta_{j_1,n-t+2} & \dots & \beta_{j_1,n} \\ \beta_{j_2,n-t+1} & \beta_{j_2,n-t+2} & \dots & \beta_{j_2,n} \\ \dots & \dots & \dots & \dots \\ \beta_{j_t,n-t+1} & \beta_{j_t,n-t+2} & \dots & \beta_{j_t,n} \end{pmatrix}$$

Finally again from Lemma 7 we can say that $M = JS_0^T$, hence M is non-singular, therefore $\det(M) \neq 0$.

□

6 Quasi Cyclic Code (QCC)

Quasi Cyclic Codes is a very useful generalization of cyclic codes. Zahra Sepasdar [11] introduced some very interesting ideals/cyclic codes, defined from a given quasi-cyclic codes. She used this ideals in order to find generator polynomials for such codes.

6.1 Definition and Polynomial Representation of a Quasi Cyclic Code

Let s, l be two positive integers. If $c \in F_q^{sl}$, it can be written in the form $c = (A_0, A_1, ..., A_{l-1})$ where A_i's are codewords with length s. So $A_i = (a_{i,0}, a_{i,1}, ..., a_{i,s-1}) \in F_q^s$.

Definition 17. A linear code C of length sl over F_q is called *Quasi Cyclic Code* (QCC) of index s if and only if $(A_0, A_1, ..., A_{l-1}) \in C$ implies $(A_{l-1}, A_0, ..., A_{l-2}) \in C$.

As before we will identify codewords of a QCC with polynomials, but this time we will use two variable polynomials.

Let $F_q[x, y]$ be the set of all two variables polynomials with coefficients in a finite field F_q and let $R_{s,l}$ be the subset of $F_q[x, y]$ containing all polynomials of degree less then s with respect to x and degree less then l with respect to y. Note that the order of s and l is important here.

It is well known that $R_{s,l}$ is a vector space over the field F_q with dimension $n = ls$. Furthermore in $R_{s,l}$ we also have the multiplication modulo $(x^s - 1, y^l - 1)$. As before I will denote with $*$ this multiplication, so for any $f(x, y)$ and $g(x, y)$ in $R_{s,l}$ we have

$$f(x, y) * g(x, y) = f(x, y) \cdot g(x, y)|_{x^s=1, y^l=1}.$$

Definition 18. Let $c \in F_q^{ls}$ with $c = (A_0, A_1, ..., A_{l-1})$ and $A_i = (a_{i,0}, a_{i,1}, ..., a_{i,s-1})$ as above. We can define

1. $A_i(x) = a_{i,0} + a_{i,1}x + a_{i,2}x^2 + ...a_{i,s-1}x^{s-1} \in R_s = F[x]/ < x^s - 1 >$.
2. $c(x, y) = A_0(x) + A_1(x)y + A_2(x)y^2 + ... + A_{l-1}(x)y^{l-1} \in R_{s,l}$.
3. $\pi : F^{sl} \to R_{s,l}$ with $\pi(c) = c(x, y)$.

It is easy to check that the map π is an isomorphism of vectors spaces, but as in the case of cyclic codes $R_{s,l}$ is also a ring. Because of the isomorphism any linear code of length sl can be seen as a subspace of $R_{s,l}$.

Theorem 16. *Let* C *be a quasi cyclic code of index* s *and length* $n = sl$. *For any* $c = c(x, y) \in C$ *and any* $p(y) \in F_q[y]$, *we have* $c(x, y) * p(y) \in C$.

Proof. First let us prove for $p(y) = y$. If $c = c(x, y) \in C$ then

$$c(x, y) * y = (A_0(x) + A_1(x)y + A_2(x)y^2 + ... + A_{l-1}(x)y^{l-1}) * y$$

$$= A_0(x) * y + A_1(x) * y^2 + A_2(x) * y^3 + ... + A_{l-1}(x) * y^l$$

$$= A_{l-1}(x) + A_0(x)y + A_2(x)y^2 + ... + A_{l-2}(x)y^{l-1}$$

$$= \pi(A_{l-1}, A_0, A_1, ...A_{l-2}) \in \pi(C) \equiv C.$$

The last codeword is in C, because C is quasi cyclic.

Using the method of mathematical induction we can prove that $c(x, y) * y^k \in C$ for any positive integer k and for any $c = c(x, y) \in C$.

Finally, using the fact that C is linear we can conclude that $c(x, y) * p(y) \in C$ for any $c = c(x, y) \in C$ and any $p(y) \in F[y]$, by taking $p(y) = \alpha_0 + \alpha_1 y + \alpha_2 y^2 + ... + \alpha_r y^r$. □

6.2 The Generators of a Quasi Cyclic Code

In the following, we will try to find generators for quasi cyclic codes. Let C be a quasi cyclic code of index s and length $n = sl$, and let $f(x, y) \in C$ be any random element. We can easily verify that $f(x, y)$ can be written in the form

$$f(x, y) = f_0(y) + f_1(y)x + f_2(y)x^2 + ... + f_{s-1}(y)x^{s-1}$$

where $f_i(y) \in S_l = F[y]/ < y^l - 1 >$. In other words $f_i(y)$ are polynomials with variable y and degree strictly less then l. Let

$$I_0 = \{g_0(y) \in S_l, \text{ such that } g_0(y) + g_1(y)x + ... + g_{s-1}(y)x^{s-1} \in C \text{ for some, } \\ g_1(y), g_2(y), ..., g_{s-1}(y) \in S_l\}$$

Proposition 3. I_0 *is an ideal in* S_l.

Proof. It is easy to check that I_0 is a subspace of S_l. All we have to do now is prove that $p(y) * g_0(y) \in I_0$ for any $g_0(y) \in I_0$ and $p(y) \in F[y]$.

Since $g_0(y) \in I_0$, there exists $g(x, y) = g_0(y) + g_1(y)x + ... + g_{s-1}(y)x^{s-1} \in C$. From Theorem 16, we have $g(x, y) * p(y) \in C$, but

$$p(y)*g(x, y) = (p(y)*g_0(y))+(p(y)*g_1(y))x+(p(y)*g_2(y))x^2+...+(p(y)*g_{s-1}(y))x^{s-1}.$$

It follows $p(y) * g_0(y) \in I_0$. □

We know that S_l is a principal ideal domain. So $I_0 =< p_0^0(y) >$ and $p_0^0(y) \mid (y^l - 1)$.

Recall that $f(x, y) = f_0(y)+f_1(y)x+f_2(y)x^2+...+f_{s-1}(y)x^{s-1}$ is a random element in C so $f_0(y) \in I_0 =< p_0^0(y) >$. Therefore $f_0(y) = p_0^0(y)q_0(y)$, for some $q_0(y) \in S_l$.

Note that we don't have to use $*$ for $f_0(y)$ because $q_0(y)$ can be chosen such that $deg(p_0^0(y)q_0(y)) < l$.

Since $p_0^0(y) \in I_0$, there exists

$$p_0(x, y) = p_0^0(y) + p_1^0(y)x + p_2^0(y)x^2 + ... + p_{s-1}^0(y)x^{s-1} \in C.$$

Let $h_1(x,y) = f(x,y) - p_0(x,y) * q_0(y)$. From Theorem 16 and linearity of C we can say $h_1(x,y) \in C$. Now let's try to evaluate it.

$$h_1(x,y) = f(x,y) - p_0(x,y) * q_0(y) = (f_0(y) - p_0^0(y)q_0(y)) + (f_1(y) - q_0(y) * p_1^0(y))x +$$

$$(f_2(y) - q_0(y) * p_2^0(y))x^2 + ... + (f_{s-1}(y) - q_0(y) * p_{s-1}^0(y))x^{s-1}.$$

Since $f_0(y) = p_0^0(y)q_0(y)$ we can say that the term x^0 is missing in $h_1(x,y)$. So it can be written in the form

$$h_1(x,y) = h_1^1(y)x + h_2^1(y)x^2 + ... + h_{s-1}^1(y)x^{s-1} \in C.$$

Let us define with

$$I_1 = \{g_1(y) \in S_l, \text{ such that } g_1(y)x + ... + g_{s-1}(y)x^{s-1} \in C \text{ for some, } g_2(y), g_3(y), ..., g_{s-1}(y) \in S_l\}$$

As before, we can prove that I_1 is also an ideal in $S_l = F[y]/ < y^l - 1 >$ and $I_1 =< p_1^1(y) >$ with $p_1^1(y) \mid (y^l - 1)$. As $h_1(x,y)$ has no x^0 term, $h_1^1(y) \in I_1$, so $h_1^1(y) = p_1^1(y)q_1(y)$. Since $p_1^1(y)$ belongs to I_1 as its generator there exists

$$p_1(x,y) = p_1^1(y)x + p_2^1(y)x^2 + ... + p_{s-1}^1(y)x^{s-1} \in C.$$

Let us define $h_2(x,y) = h_1(x,y) - p_1(x,y) * q_1(y)$. As before we can say $h_2(x,y) \in C$ and of the form

$$h_2(x,y) = h_2^2(y)x^2 + h_3^2(y)x^3 + ... + h_{s-1}^2(y)x^{s-1}.$$

If we put together $h_1(x,y) = f(x,y) - p_0(x,y) * q_0(y)$ and $h_2(x,y) = h_1(x,y) - p_1(x,y) * q_1(y)$, we can find

$$f(x,y) = p_0(x,y) * q_0(y) + p_1(x,y) * q_1(y) + h_2(x,y).$$

We can keep going like this by defining ideals $I_2, I_3, ..., I_{s-1}$, and at the end we have

$$f(x,y) = p_0(x,y) * q_0(y) + p_1(x,y) * q_1(y) + ... + p_{s-1}(x,y) * q_{s-1}(y).$$

$p_i(x,y)$ are called the generators of the quasi cyclic code C, since they only depend on C and not on the choice of $f(x,y)$. The $x^0, x^1, ..., x^{i-1}$ terms are missing in each $p_i(x,y)$. We obtain the code C be multiplying those generators with polynomials in $S_l = F[y]/ < y^l - 1 >$.

7 Permuted Quasi Cyclic Codes (PQCC)

We know from the previous chapter that from any QCC of length sl and index s over some we can define s ideals/cyclic codes of length l. I was thinking if it is possible to write down any QCC as a matrix-product of the cyclic codes defined above?

It turned out that the structure of a QCC is not right to be written as a matrix-product. That is why I manipulated those code a little bit. I called this new type *Permuted Quasi Cyclic Codes* since they can be obtained from a quasi cyclic code using a permutation.

7.1 Definition Dimension and Basis

Definition 19. Let s, l be positive integers and let C be a linear code of length $s \cdot l$ over some finite field F_q. Any codeword $f \in C$ can be written in the form $f = (f_1, f_2, ..., f_s)$, where $f_i \in F_q^l$, for any $i = 1, 2, ...s$. We say C is a *Permuted Quasi Cyclic Code* of length sl and index s over F_q if and only if $f = (f_1, f_2, ..., f_s) \in C$ implies $(f_1^{[1]}, f_2^{[1]}, ..., f_s^{[1]}) \in C$.

Recall that for any element $x = (x_1, x_2, ..., x_l) \in F_q^l$, $x^{[1]} = (x_l, x_1, x_2, ..., x_{l-1})$.

It is obvious from both definitions that there exist a permutation of the set $\{1, 2, 3, ..., l \cdot s\}$ such that every quasi cyclic code becomes a permuted quasi cyclic code and viceversa. It is not easy to find a mathematical formula for this permutation that is why I will illustrate that with an example.

Example 3. Let us define the isomorphism $\delta : F_q^{12} \to F_q^{12}$ such that

$$\delta(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}, a_{12}) = (a_1, a_4, a_7, a_{10}, a_2, a_5, a_8, a_{11}, a_3, a_6, a_9, a_{12}).$$

It is easy to check that if C is a quasi cyclic code of length 12 and index 3, then $\delta(C)$ is a permuted quasi cyclic code of length 12 and index 3.
Viceversa, if C is a permuted quasi cyclic code of length 12 and index 3, then $\delta^{-1}(C)$ is a quasi cyclic code of length 12 and index 3.

In the quasi cyclic codes we had ideals $I_0, I_1, ..., I_{s-1}$. In the permuted quasi cyclic codes we will define cyclic codes $C_1, C_2, ..., C_s$ that represent respectively the ideals $I_0, I_1, ..., I_{s-1}$.

Definition 20. Let C be a PQCC of length sl and index s over F_q. Let us define the following

$$C_1 = \{a_1 \in F_q^l, \text{such that } (a_1, a_2, ..., a_s) \in C, \text{for some } a_2, a_3, ..., a_s \in F_q^l\},$$

$$C_2 = \{a_2 \in F_q^l, \text{such that } (\mathbf{0}, a_2, ..., a_s) \in C, \text{for some } a_3, a_4, ..., a_s \in F_q^l\},$$

$$C_3 = \{a_3 \in F_q^l, \text{such that } (\mathbf{0}, \mathbf{0}, a_3, ..., a_s) \in C, \text{for some } a_4, a_5, ..., a_s \in F_q^l\},$$

...

$C_s = \{a_s \in F_q^l, \text{ such that } (\mathbf{0}, \mathbf{0}, ..., \mathbf{0}, a_s) \in C\}$.

Since I couldn't come up with a nice formula for the permutation, I will prove the following theorem.

Theorem 17. *Let C be a PQCC of length sl and index s over F_q. Every $C_1, C_2, ..., C_s$ defined as above is a linear and cyclic code.*

Proof. The proof will be done for C_1 and it can be generalized for all the others.

1. First I will prove linearity for C_1. So let $a_1, b_1 \in C_1$ and $t \in F_q$. From the definition of C_1 there exist two codewords $a, b \in C$ of the form $a = (a_1, a_2, ..., a_s)$ and $b = (b_1, b_2, ..., b_s)$. Since C is linear we have that

   $$a + tb = (a_1 + tb_1, a_2 + tb_2, ..., a_s + tb_s) \in C.$$

   From the definition of C_1 we have $a_1 + tb_1 \in C_1$, so C_1 is a linear code.

2. Now let us prove that C_1 is cyclic. If $a_1 \in C_1$ there exist $a \in C$ of the form $a = (a_1, a_2, ..., a_s)$. Since C is a PQCC we have $(a_1^{[1]}, a_2^{[1]}, ..., a_s^{[1]}) \in C$, therefore $a_1^{[1]} \in C_1$ which makes C_1 a cyclic code.

□

Observation 8. If the above linear code C of length sl is not a PQCC we can still define $C_1, ...C_s$ but they will just be linear codes of length l.

The next theorem will give us a formula for the dimension of a linear code C of length sl in terms of the dimensions of the above $C_1, C_2, ...C_s$.

Theorem 18. *Let C be a linear code of length sl over F_q and let $C_1, C_2, ..., C_s$ be the above linear codes. The dimension of C is given by*

$$\dim(C) = \dim(C_1) + \dim(C_2) + ... + \dim(C_s).$$

Proof. The proof of this formula will be done using the method of mathematical induction on s.

1. Base Step $s = 2$.

   In this case we only have C_1, C_2 as in Definition 20 and we will have to show that

   $$\dim(C) = \dim(C_1) + \dim(C_2).$$

   Let us define the linear transformation

   $$\varphi : C \to C_1, \varphi(a_1, a_2) = a_1.$$

   It is very easy to see that φ is onto and $\text{kern}(\varphi) = \{\mathbf{0}\} \times C_2$, where × is the Cartesian Product of two sets.

   So $\dim(\text{kern}(\varphi)) = \dim(C_2)$, therefore from the Rank-Nullity Theorem we have $\dim(C) = \dim(C_1) + \dim(C_2)$.

2. Next we will assume that this theorem is true for any linear code D of length $(s-1)l$.

3. Let us prove the theorem for any linear code C of length sl. We can define

   $D = \{(a_1, a_2, ..., a_{s-1}) \in F_q^{(s-1)l}$, such that $(a_1, a_2, ..., a_{s-1}, a_s) \in C$, for some

   $a_s \in F_q^l\}$.

   D satisfies following properties.

   (a) D is a linear code of length $(s-1)l$ over F_q.

   (b) $\dim(C) = \dim(D) + \dim(C_s)$.
   The proof is identical as in the case of $s = 2$. This time we will define

   $$\varphi : C \to D, \varphi(a_1, a_2, ..., a_{s-1}, a_s) = (a_1, a_2, ..., a_{s-1})$$

   and as before we will apply the Rank-Nullity Theorem.

   (c) If $D_1, D_2, ..., D_{s-1}$ are the linear codes defined from D as in Definition 20, then it is easy to check that $C_1 = D_1$, $C_2 = D_2$,...,$C_{s-1} = D_{s-1}$.

   We can assume that $\dim(D) = \dim(D_1) + ... + \dim(D_{s-1})$ since the length of D is $l(s-1)$, so

   $\dim(C) = \dim(D) + \dim(C_s) = \dim(D_1) + \dim(D_2) + ...\dim(D_{s-1}) + \dim(C_s)$, so

   $\dim(C) = \dim(C_1) + \dim(C_2) + ...\dim(C_{s-1}) + \dim(C_s)$.

□

Next we will try to find a basis for C assuming this time that C is a permuted quasi cyclic code. Recall that in this case the above $C_1, ..., C_s$ are cyclic codes.

Let g_i be the canonical generator of C_i taken as a codeword and let $k_i = \dim(C_i)$. We know from Lemma 5 and statement 5 of Proposition 2 that a basis for C_1 is the set

$$B_1 = \{g_1, g_1^{[1]}, g_1^{[2]}, ..., g_1^{[k_1-1]}\},$$

where for any positive integer m, $g_1^{[m]}$ is obtained from g_1 as in Notation 1. In the same way we can say that the basis for C_i, $i = 1, 2, ..., s$ is the set

$$B_i = \{g_i, g_i^{[1]}, g_i^{[2]}, ..., g_i^{[k_i-1]}\}.$$

Since $g_1 \in C_1$ we have that $(g_1, p_{12}, p_{13}, ..., p_{1s}) \in C$ for some $p_{1j} \in F_q^l$, $j = 2, 3, ..., s-1$. Furthermore there exists $p_{ij} \in F_q^l$, $1 \leqslant i < j \leqslant s$ such that the following codewords belong in C.

$$(\mathbf{0}, g_2, p_{23}, p_{24}, ..., p_{2s}),$$

$$(\mathbf{0}, \mathbf{0}, g_3, p_{34}, p_{35}, ..., p_{3s}),$$

$$\begin{gathered} \dots \\ (\mathbf{0},\mathbf{0},\dots,\mathbf{0},g_{s-1},p_{s-1,s}), \\ (\mathbf{0},\mathbf{0},\dots,\mathbf{0},g_s). \end{gathered}$$

.

We can claim that the following codewords form a basis for C.

$$\begin{array}{rrrr}
(g_1,p_{12},p_{13},\dots,p_{1s}), & (g_1^{[1]},p_{12}^{[1]},p_{13}^{[1]},\dots,p_{1s}^{[1]}), & \dots, & (g_1^{[k_1-1]},p_{12}^{[k_1-1]},p_{13}^{[k_1-1]},\dots,p_{1s}^{[k_1-1]}), \\
(\mathbf{0},g_2,p_{23},\dots,p_{2s}), & (\mathbf{0},g_2^{[1]},p_{23}^{[1]},\dots,p_{2s}^{[1]}), & \dots, & (\mathbf{0},g_2^{[k_2-1]},p_{23}^{[k_2-1]},\dots,p_{2s}^{[k_2-1]}), \\
(\mathbf{0},\mathbf{0},g_3,p_{34},\dots,p_{3s}), & (\mathbf{0},\mathbf{0},g_3^{[1]},p_{34}^{[1]},\dots,p_{3s}^{[1]}), & \dots, & (\mathbf{0},\mathbf{0},g_3^{[k_3-1]},p_{34}^{[k_3-1]},\dots,p_{3s}^{[k_3-1]}), \\
\dots & & \dots & \dots \\
(\mathbf{0},\mathbf{0},\dots,\mathbf{0},g_s), & (\mathbf{0},\mathbf{0},\dots,\mathbf{0},g_s^{[1]}), & \dots, & (\mathbf{0},\mathbf{0},\dots,\mathbf{0},g_s^{[k_s-1]}).
\end{array}$$

Proof. Since the number of the above codewords is $k_1+k_2+\dots+k_s = \mathrm{dim}(C)$ all we have to do is prove that all those vectors are linearly independent. This can be done by using the definition of linearly independent codewords. We can set the “famous equation“ and let $\alpha_0, \alpha_1, \dots, \alpha_{k_1-1}$ be the scalars in order of the codewords in the first row. Equalizing only the first entries on both sides of the “famous equation“ we obtain $\alpha_0 g_0 + \alpha_1 g_1 + \dots + \alpha_{k_1-1} g_{k_1-1} = \mathbf{0}$. Since B_1 above is a basis for C_1 we have $\alpha_0 = \alpha_1 = \dots = \alpha_{k_1-1} = 0$.

Next we can cut off all the first row codewords from the “famous equation“ and equalize the second entries on both sides of the same equation. After doing that all the scalars of the vectors in the second row will be zero. Repeating this procedure s times we can prove that all the scalars of “famous equation“ are zero, which implies linear independence of the above codewords. □

Next we will prove a theorem that we are going to apply later.

Theorem 19. *Let C be a PQCC of length sl and index s over some finite field. Let $(a_1, a_2, \dots, a_s)$ be a random codeword in C, with $a_i \in F_q^l$ for all $i = 1, 2, \dots s$. Also let p be a random element in F_q^l and let us define $b_i(x) = p(x) * a_i(x)$. With these conditions we can show that $(b_1, b_2, \dots, b_s) \in C$.*

Remark 1. For any element $d \in F_q^l$, $d(x)$ is the polynomial in $F[x]/ < x^l - 1 >$ that represents d using isomorphism π as in Definition 8. Meanwhile “$*$“ is the multiplication modulo $(x^l - 1)$.

Proof. If $p = (\alpha_0, \alpha_1, \dots, \alpha_{l-1}) \in F_q^l$, then $p(x) = \alpha_0 + \alpha_1 x + \dots = \alpha_{l-1} x^{l-1}$. Therefore for $i = 1, \dots, s$ we have $b_i(x) = \alpha_0 a_i(x) + \alpha_1 x * a_i(x) + \dots + \alpha_{l-1} x^{l-1} * a_i(x)$.

From statement 5 of Proposition 1 we have $b_i = \alpha_0 a_i + \alpha_1 a_i^{[1]} + \alpha_2 a_i^{[2]} + \dots + \alpha_{l-1} a_i^{[l-1]}$. So

$$(b_1, b_2, \dots, b_s) = \alpha_0 (a_1, a_2, \dots, a_s) + \alpha_1 (a_1^{[1]}, a_2^{[1]}, \dots, a_s^{[1]})$$
$$+ \alpha_2 (a_1^{[2]}, a_2^{[2]}, \dots, a_s^{[2]}) + \dots + \alpha_{l-1} (a_1^{[l-1]}, a_2^{[l-1]}, \dots, a_s^{[l-1]}).$$

Since C is PQCC and $(a_1, a_2, \dots, a_s) \in C$ we have that for any $j = 1, 2, \dots, l-1$, $(a_1^{[j]}, a_2^{[j]}, \dots, a_s^{[j]}) \in C$. Finally from the linearity of C we have $(b_1, b_2, \dots, b_s) \in C$. □

Corollary 1. *Let* C *be a PQCC of length* sl *and index* s *over some finite field and let* $C_1, C_2, ..., C_s$ *be the cyclic codes defined as above. Also for* $i = 1, 2, ..., s$ *let* g_i *be a generator of* C_i *taken as a codeword.*

If for some scalars $\beta_1, \beta_2, ..., \beta_s \in F_q$ *and for some* $i = 1, 2, .., s$ *we have* $(\beta_1 g_i, \beta_2 g_i, ..., \beta_s g_i) \in C$ *then for any* $c_i \in C_i$ *we have* $(\beta_1 c_i, \beta_2 c_i, ..., \beta_s c_i) \in C$.

7.2 Permuted Quasi Cyclic Codes as Matrix Product of Cyclic Codes

In this section I will try find a necessary and a sufficient condition so any PQCC C can be written as matrix-product of the cyclic codes $C_1, C_2, ..., C_s$ as in Definition 20.

Theorem 20. *Let* $D_1, D_2, ..., D_s$ *be cyclic codes of length* l *over some* F_q *and let* A *be an* $s \times s$ *matrix with entries in* F_q. *The linear code* C*, defined as* $C = (D_1, D_2, ..., D_s)A$ *is a PQCC of length* sl *and index* s.

Proof. Let α_{ij} be the $(i, j)th$ entry of matrix A. For any $(b_1, b_2, ..., b_s) \in C$ (where $b_j \in F_q^l$), there exists $d_i \in D_i, i = 1, 2, ..., s$ such that $(b_1, b_2, ..., b_s) = (d_1, d_2, ..., d_s)A$. So for any $j = 1, 2, ..., s$ we have

$$b_j = \alpha_{1j} d_1 + \alpha_{2j} d_2 + ... + \alpha_{sj} d_s.$$

Therefore

$$b_j^{[1]} = \alpha_{1j} d_1^{[1]} + \alpha_{2j} d_2^{[1]} + ... + \alpha_{sj} d_s^{[1]}.$$

Since this last equation is true for any $j = 1, 2, .., s$ we can say that

$$(b_1^{[1]}, b_2^{[1]}, ..., b_s^{[1]}) = (d_1^{[1]}, d_2^{[1]}, ..., d_s^{[1]})A.$$

Since D_j is cyclic and $d_j \in D_j$ we have that $d_j^{[1]} \in D_j$, for any $j = 1, 2, ..., s$. Hence

$$(b_1^{[1]}, b_2^{[1]}, ..., b_s^{[1]}) \in (D_1, D_2, ..., D_s)A = C.$$

□

In the following we will try to find conditions in which any PQCC code of index s can be written as a matrix product of those cyclic codes $C_1, C_2, ..., C_s$ as in Definition 20.

Theorem 21. *Let* C *be a PQCC of length* sl *and index* s *over some* F_q. *Let* $C_1, C_2, ..., C_s$ *be as above with* g_i *the canonical generator of* C_i. *Let us assume that for any positive integers* i, j *with* $1 \leqslant i < j \leqslant s$ *there exist scalars* α_{ij} *in* F_q *such that*

$$(g_1, \alpha_{12} g_1, \alpha_{13} g_1, ..., \alpha_{1s} g_1) \in C,$$

$$(\mathbf{0}, g_2, \alpha_{23} g_2, \alpha_{24} g_2, ..., \alpha_{2s} g_2) \in C,$$

$$(\mathbf{0}, \mathbf{0}, g_3, \alpha_{34} g_3, \alpha_{35} g_3, ..., \alpha_{3s} g_3) \in C,$$

$$...$$

$$(\mathbf{0}, \mathbf{0}, ..., g_{s-1}, \alpha_{s-1,s} g_{s-1}) \in C.$$

Under these conditions $C = (C_1, C_2, ..., C_s)A$ *where*

$$A = \begin{pmatrix} 1 & \alpha_{12} & \alpha_{13} & \alpha_{14} & ... & \alpha_{1,s-1} & \alpha_{1s} \\ 0 & 1 & \alpha_{23} & \alpha_{24} & ... & \alpha_{2,s-1} & \alpha 2s \\ 0 & 0 & 1 & \alpha_{34} & ... & \alpha_{3,s-1} & \alpha 3s \\ ... & ... & ... & ... & ... & ... & ... \\ 0 & 0 & 0 & 0 & ... & 1 & \alpha_{s-1,s} \\ 0 & 0 & 0 & 0 & ... & 0 & 1 \end{pmatrix}$$

Proof. Since $\det(A) \neq 0$ we have that

$$\dim((C_1, C_2, ..., C_s)A) = \dim(C_1) + \dim(C_2) + ... + \dim(C_s) = \dim(C),$$

therefore all we have to do is prove that $C \subseteq (C_1, C_2, ..., C_s)A$.

Let $(a_1, a_2, ..., a_s) \in C$ for some $a_i \in F_q^l$. We can define $c_1, c_2, ..., c_k$ in a recursive way as follows

$$\begin{aligned} &c_1 = a_1, \\ &c_2 = a_2 - \alpha_{12} c_1, \\ &c_3 = a_3 - \alpha_{13} c_1 - \alpha_{23} c_2, \\ &c_4 = a_4 - \alpha_{14} c_1 - \alpha_{24} c_2 - \alpha_{34} c_3, \\ &... \\ &c_s = a_s - \alpha_{1s} c_1 - \alpha_{2s} c_2 - ... - \alpha_{s-1,s} c_{s-1}. \end{aligned}$$

After solving the above equations for $a_1, a_2, ..., a_s$ in terms of $c_1, c_2, ..., c_s$ we can see that $(a_1, a_2, ..., a_s) = (c_1, c_2, ..., c_s)A$. In order to finish the proof we have to show that $c_i \in C_i$ for any $i = 1, 2, ..., s$.

The proof will be done step by step starting with $c_1 \in C_1$. Then we will show $c_2 \in C_2$, $c_3 \in C_3$ and so on until we finish with $c_s \in C_s$. The proof of each step will require the results of the previous steps.

1. Since $(a_1, a_2, ..., a_s) \in C$ then $c_1 = a_1 \in C_1$.

2. From Corollary 1 of Theorem 19 and the fact that $(g_1, \alpha_{12} g_1, \alpha_{13} g_1, ..., \alpha_{1s} g_1) \in C$ we have that $(c_1, \alpha_{12} c_1, \alpha_{13} c_1, ..., \alpha_{1s} c_1) \in C$. Since C is linear, if we subtract the last codeword from $(a_1, a_2, ..., a_s)$, the result will still be in C. Therefore we can write

$$\begin{gathered} (a_1 - c_1, a_2 - \alpha_{12} c_1, a_3 - \alpha_{13} c_1, ..., a_s - \alpha_{1s} c_1) = \\ (\mathbf{0}, c_2, a_3 - \alpha_{13} c_1, ..., a_s - \alpha_{1s} c_1) \in C. \end{gathered}$$

From the definition of C_2 we have $c_2 \in C$.

3. Again from Corollary 1 of Theorem 19 and the fact that $(\mathbf{0}, g_2, \alpha_{23}g_2, \alpha_{24}g_2, ..., \alpha_{2s}g_2) \in C$ we have $(\mathbf{0}, c_2, \alpha_{23}c_2, \alpha_{24}c_2, ..., \alpha_{2s}c_2) \in C$. But from the above step we also have that $(\mathbf{0}, c_2, a_3 - \alpha_{13}c_1, ..., a_s - \alpha_{1s}c_1) \in C$. If we do once again the difference of the last two codewords we have that

   $$(\mathbf{0}, \mathbf{0}, a_3 - \alpha_{13}c_1 - \alpha_{23}c_2, a_4 - \alpha_{14}c_1 - \alpha_{24}c_2, ..., a_s - \alpha_{1s}c_1 - \alpha_{2s}c_2) = \\ (\mathbf{0}, \mathbf{0}, c_3, a_4 - \alpha_{14}c_1 - \alpha_{24}c_2, ..., a_s - \alpha_{1s}c_1 - \alpha_{2s}c_2) \in C.$$

   So $c_3 \in C_3$.

4. Let us do it quickly for c_4 too.

   From above we have $(\mathbf{0}, \mathbf{0}, c_3, a_4 - \alpha_{14}c_1 - \alpha_{24}c_2, ..., a_s - \alpha_{1s}c_1 - \alpha_{2s}c_2) \in C$ and as above we can show that $(\mathbf{0}, \mathbf{0}, c_3, \alpha_{34}c_3, \alpha_{35}c_3, ..., \alpha_{3s}c_3) \in C$.

   If we do the difference of the last two codewords again and use the fact that $c_4 = a_4 - \alpha_{14}c_1 - \alpha_{24}c_2 - \alpha_{34}c_3$ we have $(\mathbf{0}, \mathbf{0}, \mathbf{0}, c_4, w_5, ..., w_s) \in C$, for some $w_5, ..., w_s \in F_q^l$. So $c_4 \in C_4$.

Repeating this process s times will end the proof of this theorem. □

If the index of PQCC is $s = 2$ then the hypothesis of this theorem is satisfied.

Theorem 22. *Let* C *be a PQCC of length* $2l$ *index* 2 *over some* F_q. *Let* C_1, C_2 *and* g_1, g_2 *be as above. If for some matrix* A, $C = (C_1, C_2)A$, *then* $(g_1, \alpha g_1) \in C$ *for some scalar* $\alpha \in F_q$.

Proof. Since the length of C_1, C_2 is l and the length of C is $2l$, then our matrix A has to be a 2×2 matrix. So let $A = \begin{pmatrix} \alpha_1 & \alpha_2 \\ \alpha_3 & \alpha_4 \end{pmatrix}$.

Case 1: $\alpha_1 \neq 0$.
In this case $(g_1, \frac{\alpha_2}{\alpha_1}g_1) = (\frac{1}{\alpha_1}g_1, \mathbf{0})A \in (C_1, C_2)A = C$. So we can take $\alpha = \frac{\alpha_2}{\alpha_1}$.
Case 2: $\alpha_1 = 0$, so $A = \begin{pmatrix} 0 & \alpha_2 \\ \alpha_3 & \alpha_4 \end{pmatrix}$.
Since $g_1 \in C_1$ there exist $p \in F_q^l$ such that $(g_1, p) \in C = (C_1, C_2)A$, therefore $(g_1, p) = (c_1, c_2)A$, for some $c_1 \in C_1$ and $c_2 \in C_2$. If we work the last matrix multiplication we have

$$g_1 = \alpha_3 c_2 \text{ and } p = \alpha_2 c_1 + \alpha_4 c_2.$$

From the first equality we have $g_1 \in C_2$. Since g_1 generates C_1 and C_2 is cyclic we can show that $C_1 \subseteq C_2$. It is easy to see now that also $p \in C_2$ from the second equality.

Applying the definition of C_2 we have $(\mathbf{0}, p) \in C$. Since C is linear the difference of (g_1, p) with $(\mathbf{0}, p)$ will still be in C, so $(g_1, \mathbf{0}) \in C$. In this case we can take $\alpha = 0$.

Note that if we have $C = (C_2, C_1)A$, then let B be the matrix obtained from A interchanging rows. It is easy to check that $C = (C_1, C_2)B$. □

The following Lemmas will help us understand better the structure of PQCC of index $s = 2$ that satisfy the above condition.

Since the generator of the last cyclic code C_s is not used, we can denote the generator of C_1 with g if the index of C is $s = 2$.

Lemma 10. *Let C be a PQCC of length $2l$ index 2 over some F_q. Let C_1, C_2 be as above and let g be the canonical generator of C_1 with $(g, \alpha g) \in C$ for some scalar $\alpha \in F_q$. If α is not unique the following hold:*

1. $(g, \mathbf{0}) \in C$ *(i.e $\alpha = 0$ works).*
2. $C_1 \subseteq C_2$.
3. *For any $\gamma \in F_q$, $(g, \gamma g) \in C$ (i.e any α works).*

Proof.

1. Let $(g, \alpha_1 g) \in C$ and $(g, \alpha_2 g) \in C$ with $\alpha_1 \neq \alpha_2$. With no loss of generality we can assume $\alpha_1 \neq 0$ and because C is linear we have $\frac{\alpha_2}{\alpha_1}(g, \alpha_1 g) = (\frac{\alpha_2}{\alpha_1} g, \alpha_2 g) \in C$.

   If we subtract $(\frac{\alpha_2}{\alpha_1} g, \alpha_2 g)$ from $(g, \alpha_2 g)$, the result will is still in C. Therefore $(\eta g, \mathbf{0}) \in C$, where $\eta = 1 - \frac{\alpha_2}{\alpha_1}$.

   Since $\alpha_1 \neq \alpha_2$ we have $\eta \neq 0$, so $\frac{1}{\eta}(\eta g, \mathbf{0}) = (g, \mathbf{0}) \in C$.

2. Since $(g, \alpha_1 g) \in C$ and $(g, \alpha_2 g) \in C$ for some scalars $\alpha_1 \neq \alpha_2$, from the linearity of C we have that $(\mathbf{0}, (\alpha_2 - \alpha_1)g) \in C$ for some $\alpha_1 \neq \alpha_2$.

   It follows $\frac{1}{\alpha_2 - \alpha_1}(\mathbf{0}, (\alpha_2 - \alpha_1)g) = (\mathbf{0}, g) \in C$. From the definition of C_2 we have $g \in C_2$. Since g generates C_1 and C_2 is cyclic we can show that $C_1 \subseteq C_2$.

3. From above we have that $(g, \mathbf{0}) \in C$ and $(\mathbf{0}, g) \in C$. Since C is linear, for any scalar $\gamma \in F_q$ we have

$$(g, \mathbf{0}) + \gamma(\mathbf{0}, g) = (g, \gamma g) \in C.$$

□

The following is a converse.

Lemma 11. *Let C be a PQCC of length $2l$ index 2 over some F_q. Let C_1, C_2, g be as above with $(g, \alpha g) \in C$ for some scalar $\alpha \in F_q$. If $C_1 \subseteq C_2$ then for any $\gamma \in F_q$, $(g, \gamma g) \in C$.*

Proof. Since $g \in C_1 \subseteq C_2$ we have $(\mathbf{0}, g) \in C$.

Again using the fact that C is linear, for any $\gamma \in F_q$ we have

$$\gamma(\mathbf{0}, g) + (g, \alpha g) - \alpha(\mathbf{0}, g) = (g, \gamma g) \in C.$$

□

Lemma 12. *Let* D_1, D_2 *be two cyclic codes of length* l *over some* F_q *and let* α *be any scalar in* F_q. *Also let* $A = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$ *and* $C = (D_1, D_2)A$. *From Theorem 20 we know that* C *is a PQCC of index* 2 *and length* $2l$. *So let* C_1, C_2 *be the usual cyclic codes defined from* C *and let* g *be the canonical generator of* C_1. *Under these conditions we have.*

1. $D_1 = C_1$ *and* $D_2 = C_2$.

2. $(g, \alpha g) \in C$.

Proof. 1. From what is given it is easy to check that

$$C = \{(d_1, \alpha d_1 + d_2), d_1 \in D_1, d_2 \in D_2\}.$$

It is obvious that $D_1 = C_1$.

In order to prove $D_2 = C_2$ let $c_2 \in C_2$, so $(\mathbf{0}, c_2) \in C$. Since $(\mathbf{0}, c_2) \in C$ there exist $d_1 \in D_1$ and $d_2 \in D_2$ such that $(\mathbf{0}, c_2) = (d_1, \alpha d_1 + d_2)$. It follows $c_2 = d_2 \in D_2$, hence $C_2 \subseteq D_2$.

For the other inclusion let $d_2 \in D_2$ and $d_1 = \mathbf{0} \in D_1$. It follows that $(d_1, \alpha d_1 + d_2) = (\mathbf{0}, d_2) \in C$, therefore $d_2 \in C_2$.

2. We can easily check that $(g, \alpha g) = (g, \mathbf{0})A \in (C_1, C_2)A = (D_1, D_2)A = C$.

□

The last Lemma can be generalized as follows.

Lemma 13. *Let* $D_1, D_2, ..., D_s$ *be cyclic codes of length* l *over some* F_q. *Let* C *be the PQCC of index* s *and length* sl *defined as* $C = (D_1, D_2, ..., D_s)A$, *where* A *is a given* $s \times s$ *matrix of the form*

$$A = \begin{pmatrix} 1 & \alpha_{12} & \alpha_{13} & \alpha_{14} & ... & \alpha_{1,s-1} & \alpha_{1s} \\ 0 & 1 & \alpha_{23} & \alpha_{24} & ... & \alpha_{2,s-1} & \alpha 2s \\ 0 & 0 & 1 & \alpha_{34} & ... & \alpha_{3,s-1} & \alpha 3s \\ ... & ... & ... & ... & ... & ... & ... \\ 0 & 0 & 0 & 0 & ... & 1 & \alpha_{s-1,s} \\ 0 & 0 & 0 & 0 & ... & 0 & 1 \end{pmatrix}$$

Under these conditions we have.

1. $C_1 = D_1, C_2 = D_2, ..., C_s = D_s$, *where* $C_1, ..., C_s$ *are cyclic codes obtained from* C *as in Definition 20.*

2. *The below codewords are all in* C.

$$(g_1, \alpha_{12}g_1, \alpha_{13}g_1, ..., \alpha_{1s}g_1),$$

$$(\mathbf{0}, g_2, \alpha_{23}g_2, \alpha_{24}g_2, ..., \alpha_{2s}g_2),$$

$$(\mathbf{0}, \mathbf{0}, g_3, \alpha_{34}g_3, \alpha_{35}g_3, ..., \alpha_{3s}g_3),$$

$$\dots$$

$$(\mathbf{0}, \mathbf{0}..., \mathbf{0}, g_{s-1}, \alpha_{s-1,s}),$$

$$(\mathbf{0}, \mathbf{0}..., \mathbf{0}, g_s).$$

where $g_1, g_2, ..., g_s$ *are respectively the canonical generators of* $C_1, C_2, ..., C_s$.

Now it is time to generalize at a certain point Theorem 21.

Theorem 23. *Let* C *be a PQCC of length* sl, *index* s *over some finite field* F_q. *Also let* $C_1, C_2, ..., C_s$ *be the cyclic of length* l *as described above. If* $C = (C_1, C_2, ..., C_s)A$ *where* A *is an* $s \times s$ *matrix with all Principal Minors non zero, then there exist* α_{ij} *with* $2 \leqslant i < j \leqslant s$ *such that the following codewords*

$$(g_1, \alpha_{12}g_1, \alpha_{13}g_1, ..., \alpha_{1s}g_1),$$

$$(\mathbf{0}, g_2, \alpha_{23}g_2, \alpha_{24}g_2, ..., \alpha_{2s}g_2),$$

$$(\mathbf{0}, \mathbf{0}, g_3, \alpha_{34}g_3, \alpha_{35}g_3, ..., \alpha_{3s}g_3),$$

$$\dots$$

$$(\mathbf{0}, \mathbf{0}, ..., g_{s-1}, \alpha_{s-1,s}g_{s-1}),$$

belong in C. *Here* g_i *is the canonical generator of* C_i *taken as a codeword.*

Observation 9. Let M be an $n \times n$ matrix. For any $i = 1, 2, ..., n$, the *Principal Minor* of order i is the determinant of the matrix obtained from M intersecting the first i rows with the first i columns.

Proof. The proof will be done using the method of mathematical induction on the index s.

1. If s=2 this theorem is true thanks to Theorem 22.
2. Let us assume that this theorem holds for any PQCC of index $s - 1$.
3. Now we can prove the theorem for the above C.

   Let β_{ij} be the $(i, j) - th$ entry of A. Since all the principal minors of A are non-zero then $\beta_{11} \neq 0$. It is easy to check that

   $$(g_1, \frac{\beta_{21}}{\beta_{11}}g_1, \frac{\beta_{31}}{\beta_{11}}g_1, ..., \frac{\beta_{s1}}{\beta_{11}}g_1) = (\frac{1}{\beta_{11}}g_1, \mathbf{0}, ..., \mathbf{0})A \in (C_1, C_2, ..., C_s)A = C.$$

   So if we take $\alpha_{1,j} = \frac{\beta_{1j}}{\beta_{11}}$ for any $j = 2, 3, ..., s$ we have that

   $$(g_1, \alpha_{12}g_1, \alpha_{13}g_1, ..., \alpha_{1s}g_1) \in C.$$

   In order to prove that the other codewords also belong in C, first let us define

$D = \{(p_2, p_3, ..., p_s) \in F_q^{l(s-1)}, \text{ such that } (\mathbf{0}, p_2, ..., p_s) \in C\}.$

It is easy to check that D is PQCC of length $l(s-1)$ and index $s-1$. Also it is very easy to check that $D_1 = C_2, D_2 = C_3, ..., D_{s-1} = C_s$, where $D_1, ..., D_{s-1}$ are the cyclic codes obtained from D as in Definition 20.

Now it is time to write down D as a matrix product so we can use step 2.

Let us take random $(p_2, p_3, ..., p_s) \in D$, so $(\mathbf{0}, p_2, p_3, ..., p_s) \in C = (C_1, C_2, ..., C_s)A$. Therefore there exists $c_i \in C_i$ such that

$$(\mathbf{0}, p_2, p_3, ..., p_s) = (c_1, c_2, ..., c_s) \cdot \begin{pmatrix} \beta_{11} & \beta_{12} & ... & \beta_{1s} \\ \beta_{21} & \beta_{22} & ... & \beta_{2s} \\ ... & ... & ... & ... \\ \beta_{s1} & \beta_{s2} & ... & \beta_{ss} \end{pmatrix}.$$

So we can write

$$\begin{aligned} \mathbf{0} &= \beta_{11}c_1 + \beta_{21}c_2 + ... + \beta_{s1}c_s, \\ p_2 &= \beta_{12}c_1 + \beta_{22}c_2 + ... + \beta_{s2}c_s, \\ p_3 &= \beta_{13}c_1 + \beta_{23}c_2 + ... + \beta_{s3}c_s, \\ &... \\ p_s &= \beta_{1s}c_1 + \beta_{2s}c_2 + ... + \beta_{ss}c_s. \end{aligned}$$

Since $\beta_{11} \neq 0$ we can solve for c_1 on equation 1 and substitute it to the other equations. If we do that we have

$$\begin{aligned} p_2 &= \eta_{11}c_2 + \eta_{12}c_3 + ... + \eta_{1,s-1}c_s, \\ p_3 &= \eta_{21}c_2 + \eta_{22}c_3 + ... + \eta_{2,s-1}c_s, \\ &... \\ p_s &= \eta_{s-1,1}c_2 + \eta_{s-1,2}c_3 + ... + \eta_{s-1,s-1}c_s. \end{aligned}$$

where $\eta_{ij} = -\frac{\beta_{i+1,1}}{\beta_{11}} \cdot \beta_{1,j+1} + \beta_{i+1,j+1}$, for any $i, j = 1, 2, .., s-1$.

Let us denote by B the $s-1 \times s-1$ matrix such that its $(i,j)-th$ entry is $\eta_{i,j}$. It is easy to check from above that $(p_2, p_3, ..., p_s) = (c_2, c_3, ..., c_s)B$, hence

$$D \subseteq (C_2, ..., C_s)B = (D_1, ..., D_{s-1})B.$$

Since $\dim(D) = \dim(D_1) + ... + \dim(D_{s-1}) \geqslant \dim((D_1, ..., D_{s-1})B)$ we have that

$$D = (D_1, ..., D_{s-1})B.$$

In order to apply step 2, we will have to prove that B has all its principal minors non-zero.

Since $\beta_{11} \neq 0$ we can apply Gauss elimination process on matrix A until all the entries below β_{11} become 0. If we do that we obtain

$$A \backsim \begin{pmatrix} \beta_{11} & \beta_{12} & \beta_{13} & \dots & \beta_{1s} \\ 0 & \eta_{11} & \eta_{12} & \dots & \eta_{1,s-1} \\ 0 & \eta_{21} & \eta_{22} & \dots & \eta_{2,s-1} \\ \dots & \dots & \dots & \dots & \\ 0 & \eta_{s-1,1} & \eta_{s-1,2} & \dots & \eta_{s-1,s-1} \end{pmatrix}.$$

It is easy to see now that also B has all its principal minors non-zero.

Since D is PQQC of index $s-1$ we can assume that this theorem is true for D. Recall that for any $t = 2, 3, ..., s$, g_t is the generator of $C_t = D_{t-1}$, therefore for any $i, j = 2, 3, .., s-1$ with $i < j$ there exist scalars $\alpha_{i,j} \in F_q$ such that

$$(g_2, \alpha_{23} g_2, \alpha_{24} g_2, ..., \alpha_{2s} g_2) \in D,$$

$$(\mathbf{0}, g_3, \alpha_{34} g_3, \alpha_{35} g_3, ..., \alpha_{3s} g_3) \in D,$$

$$\dots$$

$$(\mathbf{0}, \mathbf{0}, ..., g_{s-1}, \alpha_{s-1,s} g_{s-1}) \in D.$$

The above relations and the definition of D end the proof of this theorem, since we also have $(g_1, \alpha_{12} g_1, \alpha_{13} g_1, ..., \alpha_{1s} g_1) \in C$.

□

Theorem 24. *Let* $D_1, ..., D_s$ *be linear code of length* l *over some* F_q *and* A *an* $s \times s$ *matrix with all its principal minors non-zero.*

Let $C = (D_1, D_2, ..., D_s)A$ *be the linear code of length* sl. *If* $D_1 \supseteq D_2 \supseteq ... \supseteq D_s$, *then* $C_1 = D_1, C_2 = D_2, ..., C_s = D_s$, *where* $C_1, C_2, ..., C_s$ *are the linear codes of length* l *obtained from* C *as in Definition 20.*

In order to prove this theorem we need to prove a Lemma first.

Lemma 14. *Let* $D_1, D_2, ..., D_s$ *be linear codes such that* $D_i \subseteq D_1$, *for any* $i = 2, 3, ..., s$. *Also let* A *be a random* $s \times s$ *matrix with rows in order* $R_1, R_2, ..., R_s$ *and* $\alpha_2, \alpha_3, ..., \alpha_s$ *be random scalars.*

If B *is the* $s \times s$ *matrix with rows in order* $R_1, \alpha_2 R_1 + R_2, \alpha_3 R_1 + R_3, ..., \alpha_s R_1 + R_s$, *then* $(D_1, D_2, ..., D_s)A = (D_1, D_2, ..., D_s)B$.

Proof. Let $d = (d_1, d_2, ..., d_s)A \in (D_1, D_2, ..., D_s)A$. So $d = d_1R_1 + d_2R_2 + ... + d_sR_s$. It is easy to check that

$$d = d_1'R_1 + d_2(\alpha_2R_1 + R_2) + d_3(\alpha_3R_1 + R_3) + ... + (\alpha_sR_1 + R_s)$$

where $d_1' = d_1 - \alpha_2d_2 - ... - \alpha_sd_s \in D_1$. That is why $d \in (D_1, D_2, ..., D_s)B$, so

$$(D_1, D_2, ..., D_s)A \subseteq (D_1, D_2, ..., D_s)B.$$

In the same way we can show the other inclusion too. □

Now it is time to prove **Theorem 24**

Proof. The proof again will be done by induction on s.

1. For $s = 2$ we have $C = (D_1, D_2)A$, where $A = \begin{pmatrix} \alpha_1 & \alpha_2 \\ \alpha_3 & \alpha_4 \end{pmatrix}$ with $\alpha_1 \neq 0$, $\det(A) \neq 0$ and $D_1 \supseteq D_2$. From the above Lemma we can choose A such that $\alpha_3 = 0$, hence $\alpha_4 \neq 0$.

   Let us show first that $D_1 = C_1$.

   If $d_1 \in D_1$ we have that $(d_1, \mathbf{0})A \in (D_1, D_2)A = C$, hence $(\alpha_1d_1, \alpha_2d_1) \in C$, therefore $\alpha_1d_1 \in C_1$. Since $\alpha_1 \neq 0$ we have $d_1 \in C_1$.

   If $c_1 \in C_1$ then there exists $f_2 \in F_q^l$ such that $(c_1, f_2) \in C = (D_1, D_2)A$. Therefore there exist $d_1 \in D_1$, $d_2 \in D_2 \subseteq D_1$ such that $(c_1, f_2) = (d_1, d_2)A = (\alpha_1d_1, \alpha_2d_1 + \alpha_4d_2)$. It follows $c_1 = \alpha_1d_1 \in D_1$.

   Now it is time to show $D_2 = C_2$.

   If $d_2 \in D_2$ we have $(\mathbf{0}, d_2)A \in (D_1, D_2)A = C$, which implies that $(\mathbf{0}, \alpha_4d_2) \in C$. By definition $d_2 \in C_2$ because $\alpha_4 \neq 0$.

   If $c_2 \in C_2$ then $(\mathbf{0}, c_2) \in C = (D_1, D_2)A$, hence there exist $d_1 \in D_1$ and $d_2 \in D_2$ such that $(\mathbf{0}, c_2) = (d_1, d_2)A$. Working out the last matrix multiplication we get $\mathbf{0} = \alpha_1d_1$, which implies $d_1 = \mathbf{0}$ and $c_2 = \alpha_2d_1 + \alpha_4d_2 = \alpha_4d_2 \in D_2$.

2. Let us assume that this theorem is true for any linear code with length $(s - 1)l$.

3. Now we can prove the theorem for our linear code C.

   So we have $C = (D_1, D_2, ..., D_s)A$, where $D_1 \supseteq D_2 \supseteq ... \supseteq D_s$ and A is $s \times s$ matrix with all principal minors non-zero. From the above Lemma we can choose A to be of the form $A = \begin{pmatrix} \alpha_{11} & b \\ \mathbf{0} & B \end{pmatrix}$ where α_{11} is a non-zero scalar, $\mathbf{0}$ is a column matrix of length $s - 1$ with all the entries 0, b is some row matrix with length $s - 1$ and B is an $(s - 1 \times s - 1)$ matrix with all principal minors non-zero.

   As before we can define

$$F = \{(p_2, p_3, ..., p_s) \in F_q^{l(s-1)}, \text{ such that } (\mathbf{0}, p_2, ..., p_s) \in C\}.$$

F is a linear code of length $(s-1)l$ and if $F_1, ..., F_{s-1}$ are the linear codes obtained from F as in Definition 20 we have $F_1 = C_2$, $F_2 = C_3$,...,$F_{s-1} = C_s$.

From the structure of the matrix A, the fact that $C = (D_1, D_2, ..., D_s)A$ and the fact that $\alpha_{11} \neq 0$ we can show easily that $C_1 = D_1$.

Now let $(p_2, ..., p_s) \in F$, it follows $(\mathbf{0}, p_2, ..., p_s) \in C = (D_1, D_2, ..., D_s)A$. So for any $i = 1, 2, ..., s$, there exists $d_i \in D_i$ such that

$$(\mathbf{0}, p_2, ..., p_s) = (d_1, d_2, ..., d_s)A.$$

Note that we can multiply $(d_1, d_2, ..., d_s)A$ in blocks such that the blocks in A would be $\alpha_{11}, b, \mathbf{0}, B$ as above and the blocks of $(d_1, d_2, ..., d_s)$ would be d_1 and $(d_2, d_3, ..., d_s)$. If we do that we have

$$(\mathbf{0}, (p_2, p_3, ..., p_s)) = (\alpha_{11} d_1, d_1 b_1 + (d_2, d_3, ..., d_s)B).$$

Therefore $d_1 = \mathbf{0}$ and $(p_2, p_3, ..., p_s) = d_1 b_1 + (d_2, d_3, ..., d_s)B = (d_2, d_3, ..., d_s)B$. Since $(p_2, p_3, ..., p_s)$ was random in F we can say that

$$F \subseteq (D_2, ..., D_s)B$$

.

In order to prove the other inclusion, first we apply Theorem 18. So

$\dim(C) = \dim(C_1) + \dim(C_2) + ... + \dim(C_s) = \dim(C_1) + \dim(F_1) + ... + \dim(F_{s-1})$,

$\dim(C) = \dim(C_1) + \dim(F) = \dim(D_1) + \dim(F)$.

Since the matrices A and B are non-singular we also have

$\dim((D_2, D_3, ..., D_s)B) = \dim(D_2) + \dim(D_3) + ... + \dim(D_s) = \dim(C) - \dim(D_1)$, $\dim((D_2, D_3, ..., D_s)B) = \dim(D_1) + \dim(F) - \dim(D_1) = \dim(F)$.

It follows $F = (D_2, D_3, ..., D_s)B$, so we can assume that the theorem holds for F. For any $i = 2, 3, ..., s$ we have $D_i = F_{i-1} = C_i$. This ends the proof since also $C_1 = D_1$.

□

7.3 The Dual of a Permuted Quasi Cyclic Code

Recall that if C is a linear code of length sl we can still define linear codes $C_1, C_2, ..., C_s$ of length l as in Definition 20. We also know that $C^\perp$ is a linear code of length sl, so also for $C^\perp$ we can define linear codes of length l as in Definition 20. Let us call them $(C^\perp)_1, (C^\perp)_2, ..., (C^\perp)_s$.

A question arises. Is there a connection between $(C^\perp)_1, (C^\perp)_2, ..., (C^\perp)_s$ and $C_1, C_2, ..., C_s$?

The answer in general is no, however there is a connection between $(C^\perp)_1, (C^\perp)_2, ..., (C^\perp)_s$ and some other codes defined from C in a similar way as $C_1, C_2, ..., C_s$.

Definition 21. Let C be a linear code of length sl over F_q. Let us define the following:

$C^0_1 = \{a_s \in F^l_q, \text{ such that } (a_1, a_2, ..., a_s) \in C, \text{ for some } a_1, a_2, ..., a_{s-1} \in F^l_q\}$,

$C^0_2 = \{a_{s-1} \in F^l_q, \text{ such that } (a_1, ...a_{s-2}, a_{s-1}, \mathbf{0}) \in C, \text{ for some } a_1, ..., a_{s-2} \in F^l_q\}$,

$C^0_3 = \{a_3 \in F^l_q, \text{ such that } (a_1, ..., a_{s-3}, a_{s-2}, \mathbf{0}, \mathbf{0}) \in C, \text{ for some } a_1, ..., a_{s-3} \in F^l_q\}$,

...

$C^0_s = \{a_1 \in F^l_q, \text{ such that } (a_1, \mathbf{0}, \mathbf{0}, ..., \mathbf{0}) \in C\}$.

Observation 10. As in Theorems 17 and 18 we can show that:

1. C^0_i's are linear codes of length l for any $i = 1, 2, ..., s$.
2. They are cyclic codes if C is PQCC of index s.
3. $\dim(C) = \dim(C^0_1) + \dim(C^0_2) + ... + \dim(C^0_s)$

Theorem 25. *Let C a linear code of length sl over some F_q. Let $C^\perp$ be its dual and let $(C^\perp)_1, (C^\perp)_2, ..., (C^\perp)_s$ and $C^0_1, C^0_2, ..., C^0_s$ be the linear codes of length l as above. Under these condition we have:*

$$(C^\perp)_1 = (C^0_s)^\perp,\ (C^\perp)_2 = (C^0_{s-1})^\perp,\ ...,\ (C^\perp)_{s-1} = (C^0_2)^\perp \text{ and } (C^\perp)_s = (C^0_1)^\perp.$$

Proof. The proof will be done using the method of mathematical induction on s.

1. Base step $s = 2$.

   In this case we only have C^0_1, C^0_2 and $(C^\perp)_1, (C^\perp)_2$. Let us now show that $(C^\perp)_2 = (C^0_1)^\perp$ and $(C^\perp)_1 = (C^0_2)^\perp$ by starting with the first equality.

   If $s \in (C^\perp)_2$ we have $(\mathbf{0}, s) \in C^\perp$. For any $b_2 \in C^0_1$ there exists $b_1 \in F^l_q$ such that $(b_1, b_2) \in C$. Therefore we have

   $$0 =< (\mathbf{0}, s), (b_1, b_2) >=< \mathbf{0}, b_1 > + < s, b_2 >=< s, b_2 > .$$

   Since the last equality is true for any $b_2 \in C^0_1$ we have $s \in (C^0_1)^\perp$.

In order to prove the other inclusion let $s \in (C_1^0)^\perp$. For any $(b_1, b_2) \in C$ we have $b_2 \in C_1^0$, therefore $< s, b_2 >= 0$. So

$$< (\mathbf{0}, s), (b_1, b_2) >=< \mathbf{0}, b_1 > + < s, b_2 >= 0 + 0 = 0.$$

Since the last equality is true for any $(b_1, b_2) \in C$ we can say that $(0, s) \in C^\perp$, hence $s \in (C^\perp)_2$.

Now it is time to prove $(C^\perp)_1 = (C_2^0)^\perp$. First we will show that $(C^\perp)_1 \subseteq (C_2^0)^\perp$ and then $\dim[(C^\perp)_1] = \dim[(C_2^0)^\perp]$.

If $s \in (C^\perp)_1$, there exist $p \in F_q^l$ such that $(s, p) \in C^\perp$. Since for any $c_1 \in C_2^0$ we have $(c_1, \mathbf{0}) \in C$ we can write

$$0 =< (s, p), (c_1, \mathbf{0}) >=< s, c_1 > + < p, \mathbf{0} >=< s, c_1 > .$$

Since the above is true for any $c_1 \in C_2^0$ we have $s \in (C_2^0)^\perp$.

We also have to prove that the dimensions of $(C_2^0)^\perp$ and $(C^\perp)_1$ are the same.

$$\dim[(C^\perp)_1] = \dim[C^\perp] - \dim[(C^\perp)_2] = (2n - \dim[C]) - \dim[(C_1^0)^\perp],$$

$$\dim[(C^\perp)_1] = (2n - \dim[C]) - (n - \dim[C_1^0]) = n - (\dim[C] - \dim[C_1^0]),$$

$$\dim[(C^\perp)_1] = n - \dim[C_2^0] = \dim[(C_2^0)^\perp].$$

2. Let us assume that this theorem is true for any linear code W with length $l(s - 1)$.

3. Now we can show the theorem for our linear code C. First we can define the following sets

   $P = \{(a_1, ..., a_{s-1}) \in F_q^{l(s-1)}, \text{ such that } (a_1, ..., a_{s-1}, a_s) \in C^\perp, \text{ for some } a_s \in F_q^l\}$.

   $B = \{(b_1, ..., b_{s-1}) \in F_q^{l(s-1)}, \text{such that } (b_1, ..., b_{s-1}, \mathbf{0}) \in C\}$.

   The following statements are true

   (a) P, B are linear codes of length $s(l - 1)$ over F_q.

   (b) $\dim[C^\perp] = \dim[P] + \dim[(C^\perp)_s]$ and $\dim[C] = \dim[C_1^0] + \dim[B]$.

   The proof of the first one can be done by defining the linear transformation

$$\eta : C^\perp \to P, \eta(a_1, ..., a_{s-1}, a_s) = (a_1, ..., a_{s-1})$$

   and applying the rank-nullity theorem.

   For the second one we can still apply the same theorem on the linear transformation

$$\nu : C \to C_1^0, \nu(b_1, b_2, ..., b_s) = b_s.$$

(c) $P = B^{\perp}$ and $(C^{\perp})_s = (C_1^0)^{\perp}$.
The proof of this one can be done in an identical way as in the case of $s = 2$.

(d) $P_1 = (C^{\perp})_1, P_2 = (C^{\perp})_2,...,P_{s-1} = (C^{\perp})_{s-1}$ and $B_1^0 = C_2^0, B_2^0 = C_3^0,...,B_{s-1}^0 = C_s^0$. These are obvious from the definitions.

Finally let us define $W = P^{\perp} = B$. Since the length of W is $l(s-1)$ this theorem is true for W, so

$$(W^{\perp})_1 = (W_{s-1}^0)^{\perp}, (W^{\perp})_2 = (W_{s-2}^0)^{\perp}, ..., (W^{\perp})_{s-1} = (W_1^0)^{\perp} .$$

Therefore

$$(C^{\perp})_1 = P_1 = (W^{\perp})_1 = (W_{s-1}^0)^{\perp} = (B_{s-1}^0)^{\perp} = (C_s^0)^{\perp}.$$

In the same way, using W we can show that

$$(C^{\perp})_2 = (C_{s-1}^0)^{\perp}, ..., (C^{\perp})_{s-1} = (C_2^0)^{\perp}.$$

This ends the proof of the theorem since from part b) we also have $(C^{\perp})_s = (C_1^0)^{\perp}$.

□

If we pose some strong condition on C we can write down $(C^{\perp})_1, ..., (C^{\perp})_s$ in terms of $C_1, ..., C_s$, but before we have the following Lemma.

Lemma 15. *If C is a PQCC with length sl, index s over some F_q, then $C^{\perp}$ is also PQCC with the same length and index over the same F_q.*

Proof. The proof is the same way as in the theorem of the dual of a cyclic code. □

Theorem 26. *Let C be a PQCC of length $2l$, index $s = 2$ over some F_q and g be the canonical generator of the cyclic code C_1 as in Definition 20.*

Also let us assume that for some $\alpha \in F_q$ we have $(g, \alpha g) \in C$. Under these conditions we have:

1. *If $\alpha = 0$ then $(C^{\perp})_1 = C_1^{\perp}$ and $(C^{\perp})_2 = C_2^{\perp}$.*

2. *If $\alpha \neq 0$ then $(C^{\perp})_1 = C_1^{\perp} + C_2^{\perp}$ and $(C^{\perp})_2 = C_1^{\perp} \bigcap C_2^{\perp}$.*

Proof. The condition $(g, \alpha g) \in C$ implies that $C = (C_1, C_2)A$ where

$$A = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}.$$

1. When $\alpha = 0$ we have that $C = C_1 \times C_2$, where × represents the Cartisian product of two sets. It is easy to show $C^{\perp} = C_1^{\perp} \times C_2^{\perp}$, hence $(C^{\perp})_1 = C_1^{\perp}$ and $(C^{\perp})_2 = C_2^{\perp}$.

2. In the case of $\alpha \neq 0$, we can apply the theorem of the dual of matrix product code, so $C^{\perp} = (C_1^{\perp}, C_2^{\perp})(A^{-1})^T$. But

$$(A^{-1})^T = \begin{pmatrix} 1 & 0 \\ -\alpha & 1 \end{pmatrix},$$

therefore $C^{\perp} = \{(d_1 - \alpha d_2, d_2), d_1 \in C_1^{\perp}, d_2 \in C_2^{\perp}\}$.

Since $\alpha \neq 0$ it follows that $(C^{\perp})_1 = C_1^{\perp} + C_2^{\perp}$.

In order to prove $(C^{\perp})_2 = C_1^{\perp} \bigcap C_2^{\perp}$ let start with $s \in (C^{\perp})_2$, equivalent with $(\mathbf{0}, s) \in C^{\perp}$. So there exist $d_1 \in C_1^{\perp}, d_2 \in C_2^{\perp}$ such that $d_1 - \alpha d_2 = \mathbf{0}$ and $d_2 = s$. It follows $s = d_2 = \frac{1}{\alpha} d_1$, so $s \in C_1^{\perp} \bigcap C_2^{\perp}$.

In order to prove the other inclusion let $s \in C_1^{\perp} \bigcap C_2^{\perp}$. If we set $d_1 = \alpha s \in C_1^{\perp}$ and $d_2 = s \in C_2^{\perp}$ then $(d_1 - \alpha d_2, d_2) = (\mathbf{0}, s) \in C^{\perp}$. Therefore $s \in (C^{\perp})_2$.

□

After this theorem a question arises. If C is a PQCC of index 2 such that $(g, \alpha g) \in C$ for some $\alpha \in F_q$ and g as above, then is this condition also true for $C^{\perp}$?

Theorem 27. *Let C be a PQCC of length $2l$, index $s = 2$ over some F_q and let g be the generator of the cyclic code C_1 as above.*

Also let us assume that there exists $\alpha \in F_q$ such that $(g, \alpha g) \in C$. If s is the generator of $(C^{\perp})_1$ then

$(s, \beta s) \in C^{\perp}$ *for some* $\beta \in F_q$ *if and only if* $(g, \mathbf{0}) \in C$ *or* $C_2 \subseteq C_1$.

Proof. 1. Let us prove this ($\Leftarrow$) direction first.

If $(g, \mathbf{0}) \in C$ then $(g, 0g) \in C$, therefore with no loss of generality we can assume that $\alpha = 0$. It follows $C = (C_1, C_2)I_2 = C_1 \times C_2$, hence $C^{\perp} = C_1^{\perp} \times C_2^{\perp}$, so $(C^{\perp})_1 = C_1^{\perp}$. If we take $\beta = 0$ then

$$(s, \beta s) = (s, \mathbf{0}) \in C_1^{\perp} \times C_2^{\perp} = C^{\perp}.$$

If $C_2 \subseteq C_1$ we may assume that $\alpha \neq 0$. In this case we will show that $\beta = -\frac{1}{\alpha}$ works just fine.

From the above theorem and the fact that $C_2 \subseteq C_1$ we have $s \in (C^{\perp})_1 = C_1^{\perp} + C_2^{\perp} = C_2^{\perp}$.

Since $(g, \alpha g) \in C$, we have $C = (C_1, C_2)\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$ from Theorem 21.

Therefore for any $(a_1, a_2) \in C$, there exists $c_1 \in C_1, c_2 \in C_2$ such that $a_1 = c_1$ and $a_2 = \alpha c_1 + c_2$. So we can write

$$< (s, \beta s), (a_1, a_2) >=< s, a_1 > +\beta < s, a_2 >=< s, c_1 > +\beta < s, \alpha c_1 + c_2 >,$$
$$< (s, \beta s), (a_1, a_2) >=< s, c_1 > +\beta\alpha < s, c_1 > +\beta < s, c_2 > .$$

Since $\beta = -\frac{1}{\alpha}$ we have $< s, c_1 > +\beta\alpha < s, c_1 >= 0$, furthermore since $s \in C_2^{\perp}$ and $c_2 \in C_2$ we also have $< s, c_2 >= 0$.

So for any $(a_1, a_2) \in C$, $< (s, \beta s), (a_1, a_2) >= 0$. It follows $(s, \beta s) \in C^{\perp}$.

2. Now let us prove the other $(\Rightarrow)$ direction.

   In this case it is given that there exists $\beta \in \mathbb{F}_q$ such that $(s, \beta s) \in C^{\perp}$.

   We have to show either $C_2 \subseteq C_1$ or $(g, \mathbf{0}) \in C$.

   Case 1: $\beta \neq 0$. In this case I will show that $C_2 \subseteq C_1$.

   Let $c_2 \in C_2$ and $f_1 \in C_1^{\perp}$ be a random codewords. From the above theorem we can say that $C_1^{\perp} \subseteq (C^{\perp})_1$, hence $f_1 \in (C^{\perp})_1$.

   Since s is the generator of $(C^{\perp})_1$ and $(s, \beta s) \in C^{\perp}$ we have that $(f_1, \beta f_1) \in C^{\perp}$, from Corollary 1 of Theorem 19. Note that $(\mathbf{0}, c_2) \in C$ since $c_2 \in C_2$, therefore we can write
   $$0 =< (f_1, \beta f_1), (\mathbf{0}, c_2) >= \beta < f_1, c_2 > .$$

   Since $\beta \neq 0$, we have that for any $f_1 \in C_1^{\perp}$, $< f_1, c_2 >= 0$ which is equivalent with $c_2 \in (C_1^{\perp})^{\perp} = C_1$.

   Case 2: $\beta = 0$, so $(s, \mathbf{0}) \in C^{\perp}$. In this case we will show that $(g, \mathbf{0}) \in C$.

   As in the previous theorem we can show that

   $$C^{\perp} = \{(d_1 - \alpha d_2, d_2), d_1 \in C_1^{\perp}, d_2 \in C_2^{\perp}\}.$$

   Therefore there exist $d_1 \in C_1^{\perp}, d_2 \in C_2^{\perp}$ such that $d_2 = \mathbf{0}$ and $s = d_1 - \alpha d_2 = d_1$, so $s \in C_1^{\perp}$.

   Because s is also the generator of $(C^{\perp})_1$ and $C_1^{\perp}$ is a cyclic code we have that $(C^{\perp})_1 \subseteq C_1^{\perp}$.

   If $\alpha = 0$ there is nothing to prove.

   If $\alpha \neq 0$, from Theorem 26 we have that $C_1^{\perp} + C_2^{\perp} = (C^{\perp})_1 \subseteq C_1^{\perp}$, therefore $C_2^{\perp} \subseteq C_1^{\perp}$ which implies $C_1 \subseteq C_2$.

   Note that this is not what we want to prove, however from Lemma 11 we have that for any $\gamma \in \mathbb{F}_q$, $(g, \gamma g) \in C$. If we choose $\gamma = 0$ then $(g, \mathbf{0}) \in C$.

□

We can generalize this theorem even more determining whether or not the above β is unique.

Corollary 2. *With all the notations of Theorem 27 we have*

1. *If α is unique then:(Note that in this case $C_1 \nsubseteq C_2$)*
   (a) *If $\alpha = 0$ and $C_2 \nsubseteq C_1$ then $\beta = 0$ is unique.*
   (b) *If $\alpha = 0$ and $C_2 \subseteq C_1$ then for any $\beta \in F_q$ we have $(s, \beta s) \in C^\perp$.*
   (c) *If $\alpha \neq 0$ and $C_2 \nsubseteq C_1$ then there is no $\beta \in F_q$ such that $(s, \beta s) \in C^\perp$.*
   (d) *If $\alpha \neq 0$ and $C_2 \subseteq C_1$ then $\beta = -\frac{1}{\alpha}$ is the only scalar in F_q such that $(s, \beta s) \in C^\perp$.*
2. *If α is NOT unique then: (Note that in this case $C_1 \subseteq C_2$ and for any $\alpha \in F_q$, $(g, \alpha g) \in C^\perp$)*
   (a) *If $C_2 \nsubseteq C_1$ then $\beta = 0$ is unique.*
   (b) *If $C_2 \subseteq C_1$ then for any $\beta \in F_q$ we have $(s, \beta s) \in C^\perp$.*

Proof. 1. Let start the proof by assuming α is unique

   (a) Let $\alpha = 0$ and $C_2 \nsubseteq C_1$.
   We know from Theorem 27 that if $\alpha = 0$ then $\beta = 0$ works. If we use case 1 of Theorem 26 we also have that $(C^\perp)_1 = C_1^\perp$ and $(C^\perp)_2 = C_2^\perp$.
   If we assume by contradiction then β is not unique then we can apply Lemma 10 on $C^\perp$. It follows $C_1^\perp \subseteq C_2^\perp$, i.e. $C_2 \subseteq C_1$, which is a contradiction.
   (b) Let $\alpha = 0$ and $C_2 \subseteq C_1$.
   As in part a) we have $\beta = 0$ works, $(C^\perp)_1 = C_1^\perp$ and $(C^\perp)_2 = C_2^\perp$. Since $C_2 \subseteq C_1$ implies $C_1^\perp \subseteq C_2^\perp$ we can apply Lemma 11 on $C^\perp$, therefore for any $\beta \in F_q$ we have $(s, \beta s) \in C^\perp$.
   (c) This case is obvious from Theorem 27. Note that since $\alpha \neq 0$ and α unique we have that $(g, \mathbf{0}) \notin C^\perp$.
   (d) From theorem 27 we know that if $\alpha \neq 0$ and $C_2 \subseteq C_1$ then $\beta = -\frac{1}{\alpha}$ works. If we assume by contradiction that β is not unique we can apply Lemma 10 on $C^\perp$. It follows that for any β including $\beta = 0$ we have $(s, \beta s) \in C^\perp$. But again from theorem 27 if $\beta = 0$ works then $\alpha = 0$ works too. This contradicts the fact that α is unique.

2. When α is not unique we know form Lemma 10 that for any $\alpha \in F_q$, $(g, \alpha g) \in C$. Here, with no loss of generality we can take $\alpha = 0$, so the proof of sub-cases a) and b) of this case can be done in an identical way as sub-cases a) and b) of case 1.

□

Generalizing Theorem 26 it is not easy at all, however we have the following theorem.

Theorem 28. *Let C be a linear code with length sl and let $C_1, C_2, ..., C_s$ be the linear codes of length l as in Definition 20. If $C_1 \supseteq C_2 \supseteq ... \supseteq C_s$ and for some non singular by columns matrix A we have $C = (C_1, C_2, ..., C_s)A$, then $(C^\perp)_1 = C_s^\perp$, $(C^\perp)_2 = C_{s-1}^\perp$,...,$(C^\perp)_s = C_1^\perp$.*

Proof. From the structure of matrix J_s and Theorem 14 we have

$$C^{\perp} = (C_1^{\perp}, C_2^{\perp}, ..., C_s^{\perp})(A^{-1})^T = (C_s^{\perp}, C_{s-1}^{\perp}, ..., C_1^{\perp})J_s(A^{-1})^T.$$

Theorem 15 allows us to say that that $J(A^{-1})^T$ is non-singular by columns matrix, therefore all its principal minors are non-zero. Finally if we apply Theorem 24 we get exactly what we wanted to prove. □

8 Multi Cyclic Codes (MCC)

Let q be a prime power and let m be a positive integer. Let us consider the quotient ring

$$R = F_q[x_1, x_2, ..., x_m]/ < x_1^{q-1} - 1, x_2^{q-1} - 1, ..., x_m^{q-1} - 1 > .$$

The elements of this quotient ring will be of the form $\Sigma c x_1^{\alpha_1} x_2^{\alpha_2} ... x_m^{\alpha_m}$, where $\alpha_j = 0, 1, 2, ..., q-2$ for $j = 1, 2, ..., m$. It is obvious that the number of terms, including those with a zero coefficient in every element of that quotient ring is $(q-1)^m$.

For some order of the set $\{(\alpha_1, \alpha_2, ..., \alpha_m), \alpha_j \in F_q, j = 1, 2, .., m\} = F_q^m$ we can very easily define an isomorhism of vector spaces $\pi : R \to F_q^{(q-1)^m}$, such that any element of the quotient ring is mapped to the codeword build from the coefficients of every $x_1^{\alpha_1} x_2^{\alpha_2} ... x_m^{\alpha_m}$ term taken in order defined before.

Example 4. If $q = 3$ and $m = 2$ every element of $F_3[x_1, x_2]/ < x_1^2 - 1, x_2^2 - 1 >$ can be written as $k_0 + k_1 x_1 + k_2 x_2 + k_3 x_1 x_2$. Therefore we can define

$$\pi : F_3[x_1, x_2]/ < x_1^2 - 1, x_2^2 - 1 >: \to F_3^4$$

such that $\pi(k_0 + k_1 x_1 + k_2 x_2 + k_3 x_1 x_2) = (k_0, k_1, k_2, k_3)$.

Definition 22. A linear code C of length $(q-1)^m$ over F_q is said to be a *Multi Cyclic Code* (MCC) if and only if $\pi^{-1}(C)$ is an ideal of $F_q[x_1, x_2, ..., x_m]/ < x_1^{q-1} - 1, x_2^{q-1} - 1, ..., x_m^{q-1} - 1 >$.

Since π is an ismorphism in the following we can identify C with $\pi^{-1}(C)$ with no confusion.

8.1 Multi Cyclic Code of length 4 over F_3

In this Chapter we find all multi cyclic codes when $q = 3$ and $m = 2$. We call them *Multi Cyclic Code of length 4 over* F_3. Since these type of codes will be the only multi cyclic code I will work with, sometimes I will just call them multi cyclic codes.

First I will find all the above MCC that are generated by only one polynomial.

Theorem 29. *Let* F_3^4 *and* $F_3[x_1, x_2]/ < x_1^2 - 1, x_2^2 - 1 >$ *be as above and let* $C =< k_0 + k_1 x_1 + k_2 x_2 + k_3 x_1 x_2 >$ *be a random MCC generated by only one polynomial. Let* δ *be a permutation of the set* $\{0, 1, 2, 3\}$ *and let* $C_\delta =< k_{\delta(0)} + k_{\delta(1)} x_1 + k_{\delta(2)} x_2 + k_{\delta(3)} x_1 x_2 >$. *Under theses conditions we have*

$$(c_0, c_1, c_2, c_3) \in C \iff (c_{\delta(0)}, c_{\delta(1)}, c_{\delta(2)}, c_{\delta(3)}) \in C_\delta.$$

In other words this theorem tells us that the linear code obtained from some permutation of the coefficients k_0, k_1, k_2, k_3 can also be obtained by applying the same permutation on all the codewords of C.

Proof. The proof of this theorem will be done in several steps.

Step 1 consists of finding the generator matrix of C. If $p = p(x_1, x_2) \in C$ then $p(x_1, x_2) = (k_0 + k_1x_1 + k_2x_2 + k_3x_1x_2)(a_0 + a_1x_1 + a_2x_2 + a_3x_1x_2)$ for some $a_i \in F_3$, $i = 0, 1, 2, 3$. If we work out this multiplication $mod(x_1^2 - 1, x^2 - 1)$ we have

$p(x_1, x_2) = (k_0a_0 + k_1a_1 + k_2a_2 + k_3a_3) + (k_0a_1 + k_1a_0 + k_2a_3 + k_3a_2)x_1 + (k_0a_2 + k_1a_3 + k_2a_0 + k_3a_1)x_2 + (k_0a_3 + k_1a_2 + k_2a_1 + k_3a_0)x_1x_2$. If

$A_0 = (k_0a_0 + k_1a_1 + k_2a_2 + k_3a_3)$,
$A_1 = (k_0a_1 + k_1a_0 + k_2a_3 + k_3a_2)$,
$A_2 = (k_0a_3 + k_1a_2 + k_2a_1 + k_3a_0)$,
$A_3 = (k_0a_3 + k_1a_2 + k_2a_1 + k_3a_0)$

we have that $p = (A_0, A_1, A_2, A_3) = (a_0, a_1, a_2, a_3)M_C$ where,

$$M_C = \begin{pmatrix} k_0 & k_1 & k_2 & k_3 \\ k_1 & k_0 & k_3 & k_2 \\ k_2 & k_3 & k_0 & k_1 \\ k_3 & k_2 & k_1 & k_0 \end{pmatrix}$$

So, $C = \{(a_0, a_1, a_2, a_3)M_C,\ a_i \in F_3, i = 0, 1, 2, 3\}$.

In other word, any element in C is a linear combination of the rows of M_C. However we can not claim that M_C is a generator matrix for C, because its rows may not be linearly independent. In order to find the generator matrix we can find the Reduced Row Echelon Form (RREF) of M_C and only take the rows with pivots.

Step 2: In this step we will recall some some properties of the permutation matrix.

Definition 23. Let θ be some permutation of the set $\{0, 1, 2, ..., n - 1\}$, where n is a fixed positive integer. Also let $e_0 = (1, 0, 0..., 0)^T, e_1 = (0, 1, 0, ..., 0)^T, ..., e_{n-1} = (0, 0, ..., 0, 1)^T$ be column matrices with n rows.

The permutation matrix of the permutation θ, denoted by P_θ, is the $n \times n$ matrix such that its columns in order are $e_{\theta(0)}, e_{\theta(1)}, ..., e_{\theta(n-1)}$.

Proposition 4. *The following properties are true for the permutation matrix.*

1. *Let F be a field (not necessary finite) and let θ be as above. For any $(x_0, x_1, ..., x_{n-1}) \in F^n$ we have $(x_{\theta(0)}, x_{\theta(1)}, ..., x_{\theta(n-1)}) = (x_0, x_1, ..., x_{n-1})P_\theta$.*

2. *Let α, β be two permutations of the set $\{0, 1, 2, ..., n - 1\}$. If $\beta\alpha$ is their composition then $P_{\beta\alpha} = P_\alpha \cdot P_\beta$.*

3. *Let A be an nxn matrix with rows in order $R_0, R_1, ..., R_{n-1}$ and let θ be as above.*

   If B is the $n \times n$ matrix such that its rows in order are $R_{\theta(0)}, R_{\theta(1)}, ..., R_{\theta(n-1)}$, then we can show that $B = P_\theta^T \cdot A$.

4. *For any permutation θ we have $P_\theta^T = P_\theta^{-1} = P_{\theta^{-1}}$.*

Proof. 1. The first property is a simple matrix multiplication.

2. Thanks to the above property, for any row vector $(x_0, x_1, ..., x_{n-1})$ with real entries we have

$$(x_0, x_1, ..., x_{n-1})P_\alpha P_\beta = (x_{\alpha(0)}, x_{\alpha(1)}, ..., x_{\alpha(n-1)})P_\beta =$$

$$(x_{\beta(\alpha(0))}, x_{\beta(\alpha(1))}, ..., x_{\beta(\alpha(n-1))}) = (x_0, x_1, ..., x_{n-1})P_{\beta\alpha}.$$

The last equality is equivalent to

$$(P_{\beta\alpha} - P_\alpha \cdot P_\beta)^T \cdot \begin{pmatrix} x_1 \\ x_2 \\ ... \\ x_n \end{pmatrix} = \mathbf{0}.$$

It follows $\mathrm{Null}(P_{\beta\alpha} - P_\alpha \cdot P_\beta)^T = \mathbf{R^n}$, therefore from rank-nullity theorem we have $\mathrm{rank}(P_{\beta\alpha} - P_\alpha \cdot P_\beta)^T = n - n = 0$. Hence $P_{\beta\alpha} = P_\alpha \cdot P_\beta$.

3. This property can be proved by multiplying $P_\theta^T \cdot A$ in blocks. The blocks of P_θ^T would be its entries and the blocks of A would be its rows.

4. It is easy to see that any permutation matrix is an orthonormal matrix, hence $P_\theta^T = P_\theta^{-1}$.

From property 2 we can say that $P_\theta \cdot P_{\theta^{-1}} = P_{\theta^{-1}\theta} = P_{id} = I_n$. Therefore we also have $P_\theta^{-1} = P_{\theta^{-1}}$.

□

Step 3: In this step I will analyze the rows of the matrix M_C defined in step 1.

Let R_0, R_1, R_2, R_3 be the rows of M_C in order and let p_1, p_2, p_3 be the following permutations

$$p_1 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \end{pmatrix}, p_2 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \end{pmatrix}, p_3 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 2 & 1 & 0 \end{pmatrix}.$$

It is obvious that R_1, R_2, R_3 are obtained from R_0 applying respectively the permutations p_1, p_2, p_3. Therefore if we denote with P_1, P_2, P_3 respectively the permutation matrix of p_1, p_2, p_3 we have $R_1 = R_0P_1$, $R_2 = R_0P_2$, $R_3 = R_0P_3$.

Step 4: In this step I will recall a very important property of S_4.

Let S_4 be the set of all permutations of the set $\{0, 1, 2, 3\}$. We know that S_4 is a group under the usual operation of composition.

Since $p_1^2 = p_2^2 = p_3^2 = id$ and for any $i, j, k \in \{1, 2, 3\}$ pairwise distinct $p_ip_j = p_jp_i = p_k$ we can conclude that the set $G = \{id, p_1, p_2, p_3\}$ is a subgroup of S_4.

We can also check that G is a *normal subgroup* of S_4. If we apply the property of normal subgroups for the permutation $\delta \in S_4$ of this theorem we have $p_1\delta = \delta p_{\gamma_1}$, $p_2\delta = \delta p_{\gamma_2}$ and $p_3\delta = \delta p_{\gamma_3}$. It is easy to check that

$$\gamma = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & \gamma_1 & \gamma_2 & \gamma_3 \end{pmatrix}$$

is a permutation in S_4.

Step 5: In this step we will find a relation between M_C and M_{C_δ}, where M_{C_δ} is the matrix obtained from C_δ, in the same way as M_C is obtained from C.

If for C_δ we do the same work we did for C in step 1 we have that

$$M_{C_\delta} = \begin{pmatrix} k_{\delta(0)} & k_{\delta(1)} & k_{\delta(2)} & k_{\delta(3)} \\ k_{\delta(1)} & k_{\delta(0)} & k_{\delta(3)} & k_{\delta(2)} \\ k_{\delta(2)} & k_{\delta(3)} & k_{\delta(0)} & k_{\delta(1)} \\ k_{\delta(3)} & k_{\delta(2)} & k_{\delta(1)} & k_{\delta(0)} \end{pmatrix}$$

Let us define with R_0', R_1', R_2', R_3' the rows of M_{C_δ} in order. As above it is easy to check that

$$R_0' = R_0 P_\delta,$$

$$R_1' = R_0' P_1 = R_0 P_\delta P_1 = R_0 P_{\gamma_1} P_\delta = R_{\gamma_1} P_\delta,$$

$$R_2' = R_0' P_2 = R_0 P_\delta P_2 = R_0 P_{\gamma_2} P_\delta = R_{\gamma_2} P_\delta,$$

$$R_3' = R_0' P_3 = R_0 P_\delta P_3 = R_0 P_{\gamma_3} P_\delta = R_{\gamma_3} P_\delta.$$

Note that the first relation is true from property 1 of the permutation matrix and the others are true for the relations we have in step 3, step 4 and property 3 of the permutation matrix. Now it is time to evaluate $P_\gamma^{-1} M_C P_\delta$.

$$P_\gamma^{-1} M_C P_\delta = P_\gamma^T M_C P_\delta = P_\gamma^T \cdot \begin{pmatrix} R_0 \\ R_1 \\ R_2 \\ R_3 \end{pmatrix} \cdot P_\delta.$$

From property 3 of the permutation matrix we have that

$$P_\gamma^T \cdot \begin{pmatrix} R_0 \\ R_1 \\ R_2 \\ R_3 \end{pmatrix} = \begin{pmatrix} R_0 \\ R_{\gamma_1} \\ R_{\gamma_2} \\ R_{\gamma_3} \end{pmatrix},$$

therefore

$$P_\gamma^{-1} M_C P_\delta = \begin{pmatrix} R_0 \\ R_{\gamma_1} \\ R_{\gamma_2} \\ R_{\gamma_3} \end{pmatrix} P_\delta = \begin{pmatrix} R_0' \\ R_1' \\ R_2' \\ R_3' \end{pmatrix} = M_{C_\delta}.$$

So $M_C P_\delta = P_\gamma M_{C\delta}$.

Step 6 Finally it is time to prove the theorem.

Let us prove this (⇒) direction first. We need to show that if $(c_0, c_1, c_2, c_3) \in C$ then $(c_{\delta(0)}, c_{\delta(1)}, c_{\delta(2)}, c_{\delta(3)}) \in C_\delta$. From step 1 and 2 we can write

$$(c_{\delta(0)}, c_{\delta(1)}, c_{\delta(2)}, c_{\delta(3)}) = (c_0, c_1, c_2, c_3)P_\delta = (a_0, a_1, a_2, a_3)M_C P_\delta,$$

for some a_0, a_1, a_2, a_3 in F_3. From step 5 we have

$$(c_{\delta(0)}, c_{\delta(1)}, c_{\delta(2)}, c_{\delta(3)}) = (a_0, a_1, a_2, a_3)P_\gamma M_{C_\delta} = (b_0, b_1, b_2, b_3)M_{C_\delta} \in C_\delta,$$

where $(b_0, b_1, b_2, b_3) = (a_0, a_1, a_2, a_3)P_\gamma$.

Let us prove now the other direction (⇐). We need to show that if $(c_{\delta(0)}, c_{\delta(1)}, c_{\delta(2)}, c_{\delta(3)}) \in C_\delta$ then $(c_0, c_1, c_2, c_3) \in C$. Using the above properties for θ^{-1} we have

$$(c_0, c_1, c_2, c_3) = (c_{\delta(0)}, c_{\delta(1)}, c_{\delta(2)}, c_{\delta(3)})P_\delta^{-1} = (a_0, a_1, a_2, a_3)M_{C_\delta} P_\delta^{-1},$$

for some scalars a_0, a_1, a_2, a_3 in F_3.

From step 5 we can say that $M_{C_\delta} P_\delta^{-1} = P_\gamma^{-1} M_C$, so finally we have

$$(c_0, c_1, c_2, c_3) = (a_0, a_1, a_2, a_3)P_\gamma^{-1} M_C = (b_0, b_1, b_2, b_3)M_C \in C,$$

where $(b_0, b_1, b_2, b_3) = (a_0, a_1, a_2, a_3)P_\gamma^{-1}$.

□

Thanks to this theorem and the fact that we are working on F_3 the only multi cyclic codes of length 4 over F_3 generated by one polynomial are the following codes and their permutations.

1. $C_0 =< 1 >$.
2. $C_1 =< 1 + x_1 >$.
3. $C_2 =< 2 + x_1 >$.
4. $C_3 =< 1 + x_1 + x_2 >$.
5. $C_4 =< 2 + x_1 + x_2 >$.
6. $C_5 =< 1 + x_1 + x_2 + x_1x_2 >$.
7. $C_6 =< 2 + x_1 + x_2 + x_1x_2 >$.
8. $C_7 =< 2 + 2x_1 + x_2 + x_1x_2 >$.

Proposition 5. *We can show that.*

1. $C_0 = F_3^4$.

2. $C_1 = \{(a, a, b, b), a \in F_3, b \in F_3\}$.

3. $C_2 = \{(a, 2a, b, 2b), a \in F_3, b \in F_3\}$.

4. $C_3 = \{(a, b, c, 2a + 2b + 2c), a \in F_3, b \in F_3, c \in F_3\}$.

5. $C_4 = \{(a, b, c, 2a + b + c), a \in F_3, b \in F_3, c \in F_3\}$.

6. $C_5 = \{(a, a, a, a), a \in F_3\}$.

7. $C_6 = F_3^4$.

8. $C_7 = \{(a, a, 2a, 2a), a \in F_3\}$.

Proof. We will do the proof for C_4 and for the other we can apply the same idea.

Let $M_{C_4} = \begin{pmatrix} 2 & 1 & 1 & 0 \\ 1 & 2 & 0 & 1 \\ 1 & 0 & 2 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix}$ be the matrix as described in step 1 of the previous theorem. The rows with pivots of the reduced raw echelon form of M_{C_4} will give us the basis for C_4. Since we are working on F_3 we can find

$$M_{C_4} \sim \begin{pmatrix} 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

hence the first three rows of the last matrix will form a basis for C_4. It follows
$C_4 = \{a(1, 0, 0, 2) + b(0, 1, 0, 1) + c(0, 0, 1, 1), a, b, c \in F_3\}$,
$C_4 = \{(a, b, c, 2a + b + c), a, b, c \in F_3\}$.

□

Next we will show that $F_3[x]/ < x_1^2 - 1, x_2^2 - 1 >$ is principal ideal domain (all its ideals are generated by one element), but before we will find all MCC of length 4 over F_3 generated by only one polynomial.

From the above theorem, all we have to do is find all the permutations of $C_0, C_1, ..., C_7$.

1. It is easy to see that if we permute $C_0 = C_6 = F_3^4$ and C_5 we do not obtain any thing new.

2. Also if we permute C_3 we do not obtain new linear codes. Recall that $(a, b, c, d) \in C_3$ if and only if $d = 2a + 2b + 2c$. Since we are working in F_3 the last equality is equivalent to $a = 2b + 2c + 2d$ which is equivalent to $b = 2a + 2c + 2d$ which is equivalent to $c = 2a + 2b + 2d$.

3. It is easy to check that if we permute C_1 we obtain the following linear codes
$C_1' = \{(a, b, a, b), a \in F_3, b \in F_3\}$ and $C_1'' = \{(a, b, b, a), a \in F_3, b \in F_3\}$.

4. If we permute C_2 we obtain
$C_2' = \{(a, b, 2a, b), a \in F_3, b \in F_3\}$ and $C_2'' = \{(a, b, 2b, 2a), a \in F_3, b \in F_3\}$.

5. If we permute C_7 we have
$C_7' = \{(a, 2a, a, 2a), a \in F_3\}$ and $C_7'' = \{(a, 2a, 2a, a), a \in F_3\}$.

6. Finally if we permute C_4 we will have
$C_4' = \{(a, b, c, a + 2b + c), a \in F_3, b \in F_3, c \in F_3\}$ and
$C_4'' = \{(a, b, c, a + b + 2c), a \in F_3, b \in F_3, c \in F_3\}$
The reason we have no others is the following:
$(a, b, c, d) \in C_4$ is equivalent to $d = 2a + b + c$, which is equivalent to $a = b+c+2d$, which is equivalent to $b = a+d+2c$, which is equivalent to $c = a+d+2b$.
Codes C_4' and C_4'' cover all the other possibilities.

So

$$\Delta = \{\mathbf{0}, F_3^4, C_1, C_1', C_1'', C_2, C_2', C_2'', C_3, C_5, C_4, C_4', C_4'', C_7, C_7', C_7''\}$$

is the set of all MCC with length 4 over F_3 generated by only one polynomial.

We can check that Δ is closed under the addition of vector spaces. As an example lets see what we get if we do $C_1 + C_1'$.

It is easy to see that a basis for C_1 is $B_1 = \{(1, 1, 0, 0), (0, 0, 1, 1)\}$ and a basis for C_1' is $B_1' = \{(1, 0, 1, 0), (0, 1, 0, 1)\}$.

In order to find a basis for $C_1 + C_1'$ first we build the matrix

$$M = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

and apply the reduced raw echelon form on it. If we do that we have

$$M \sim \begin{pmatrix} 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

The first 3 rows of the above matrix will give us a basis for $C_1 + C_1'$. So we have
$C_1 + C_1'$=$\{a(1, 0, 0, 2) + b(0, 1, 0, 1) + c(0, 0, 1, 1), a, b, c \in F_3^4\}$,
$C_1 + C_1' = \{(a, b, c, 2a + b + c), a, b, c \in F_3\}$=$C_4$.

Theorem 30. $F_3[x]/ < x_1^2 - 1, x_2^2 - 1 >$ *is a principal ideal domain.*

Proof. Let $I \subset F_3[x]/ < x_1^2 - 1, x_2^2 - 1 >$ be a random ideal. Since we are working on F_3, I is generated by finite polynomials of $F_3[x]/ < x_1^2 - 1, x_2^2 - 1 >$.

So we have $I =< p_1, p_2, ..., p_s >=< p_1 > + < p_2 > +...+ < p_s >$.

Since $p_i \in F_3[x]/ < x_1^2 - 1, x_2^2 - 1 >$ we have $< p_i >\in \Delta$ for any $i = 1, 2, 3..., s$. Because Δ is closed under the addition of vector spaces we have $I \in \Delta$. □

We can conclude that Δ contains all the multi cyclic codes of length 4 over F_3.

8.2 Matrix Product Structure and the Dual of MCC of length 4 over F_3

It turns out that all the linear codes $C_0, C_1, ..., C_7$ defined above, can be written as matrix product of cyclic code of length 2 over F_3. Let $V = \{(a, a), a \in F_3\}$ and let $W = \{(a, 2a), a \in F_3\}$. Since we are working in F_3, the above V and W are cyclic codes.

Proposition 6. *We can show that*

1. $C_0 = C_6 = F_3^4 = (F_3^2, F_3^2) \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

2. $C_1 = (V, V) \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

3. $C_2 = (W, W) \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

4. $C_3 = (F_3^2, W) \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$.

5. $C_4 = (F_3^2, V) \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}$.

6. $C_5 = (V, \mathbf{0}) \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

7. $C_7 = (V, \mathbf{0}) \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}$.

Proof. The proof once again will be done for C_4 and the same idea can be applied for the others.

Since

$$\text{dim}((F_3^2, V) \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix})\text{=2+1=3=} \dim C_4$$

all we have to do is prove that $(F_3^2, V)\begin{pmatrix}1 & 1\\ 0 & 2\end{pmatrix} \subseteq C_4$.

Let $(c_1, c_2, c_3, c_4) \in (F_3^2, V)\begin{pmatrix}1 & 1\\ 0 & 2\end{pmatrix}$. From the definition of matrix product there exists $(a, b) \in F_3^2$ and $(c, c) \in V$ such that

$$\begin{pmatrix}c_1 & c_3\\ c_2 & c_4\end{pmatrix} = \begin{pmatrix}a & c\\ b & c\end{pmatrix}\begin{pmatrix}1 & 1\\ 0 & 2\end{pmatrix}.$$

So we can write $c_1 = a$, $c_2 = b$, $c_3 = a + 2c$, $c_4 = b + 2c$.

Recall that $(c_1, c_2, c_3, c_4) \in C_4$ if and only if $c_4 = 2c_1 + c_2 + c_3$, but $2c_1 + c_2 + c_3 = 2a + b + a + 2c = 3a + b + 2c = 0 + b + 2c = c_4$. □

It turns out that the dual of a MCC of length 4 over F_3 is still a MMC of the same length over the same F_3. We can show that

1. $(\mathbf{0})^\perp = F_3^4$.
2. $C_1^\perp = C_2$.
3. $(C'_1)^\perp = C'_2$.
4. $(C''_1)^\perp = C''_2$.
5. $C_3^\perp = C_5$.
6. $C_4^\perp = C''_7$.
7. $(C'_4)^\perp = C'_7$.
8. $(C''_4)^\perp = C_7$.

Example 5. As an example i will prove that $C_4^\perp = C''_7$.

Proof. Since $\dim(C_4) + \dim(C''_7) = 3 + 1 = 4 = \dim(F_3^4)$, it is enough to show that for any $x \in C_4$ and $y \in C''_7$, $< x, y >= 0$. Since $x = (a, b, c, 2a + b + c)$ and $y = (d, 2d, 2d, d)$ for some $a, b, c, d \in F_3$ we have $< x, y >= ad + 2bd + 2dc + 2ad + bd + dc = 3(ad + bd + cd) = 0$. □

References

[1] Lidl, Rudolf; Niederreiter, Harald *Finite fields. With a foreword by P. M. Cohn. Second edition.* Encyclopedia of Mathematics and its Applications, 20. Cambridge University Press, Cambridge, 1997. xiv+755 pp. ISBN: 0-521-39231-4

[2] Mullen, Gary L.; Mummert, Carl (2007),*Finite Fields and Applications I, Student Mathematical Library* (AMS), ISBN 978-0-8218-4418-2

[3] Aydin, Nuh; Halilovi, Ajdin *A generalization of quasi-twisted codes: multi-twisted codes.* Finite Fields Appl. 45 (2017), 96106. 94B15 (94B60 94B65)

[4] Huffman, W. Cary; Pless, Vera *Fundamentals of error-correcting codes. Cambridge University Press, Cambridge, 2003. xviii+646 pp. ISBN: 0-521-78280-5 (Reviewer: H. F. Mattson Jr.) 94Bxx (94-01)*

[5] *Blahut, Richard E. (2003). Algebraic Codes for Data Transmission (2nd ed.) , Cambridge University Press, ISBN 0-521-55374-1*

[6] *MacWilliams, F. J.; Sloane, N. J. A. (1977), The Theory of Error-Correcting Codes , New York: North-Holland Publishing, ISBN 0-444-85011-2*

[7] *Liu, Yang; Li, Ruihu; Lv, Liangdong; Ma, Yuena A class of constacyclic BCH codes and new quantum codes. Quantum Inf. Process. 16 (2017), no. 3, Art. 66, 16 pp. (Reviewer: Rong Pan) 81P70*

[8] *Fan, Yun; Liu, Hualu Quasi-cyclic codes of index 1 1/2. IEEE Trans. Inform. Theory 62 (2016), no. 11, 63426347. (Reviewer: Anuradha Sharma) 94B15*

[9] *Cem Guneri, San Ling and Buket Ozkaya. Quasi-Cyclic Codes. arXiv:2007.16029v1*

[10] *Martianus Frederic Ezerman, San Ling, Buket Ozkaya, and Patrick Sole Good Stabilizer Codes from Quasi-Cyclic Codes over* $\mathbb{F}_4$ *and* $\mathbb{F}_9$ *arXiv:1906.04964v1*

[11] *Zahra, Sepasdar Generator Polynomials And Generator Matrix For Quasi Cyclic Codes arXiv:1704.08815v1*

[12] *Roy Joshua, G.V. Ravindra FAMILIES OF QUANTUM STABILIZER AND SUBSYSTEM CODES FROM ALGEBRO-GEOMETRIC TORIC CODES*

[13] *Tim Blackmore, Graham H. Norton Matrix-Product Codes over* $\mathbb{F}_q$. *AAECC 12, 477-500 (2001)*

[14] *Bram van Asch Matrix-product codes over finite chain rings. AAECC (2008) 19:3949 DOI 10.1007/s00200-008-0063-3.*

[15] *Ferdinand Blomqvist, Oliver W. Gnilke, and Marcus Greferath. On Decoding of Generalized Concatenated Codes and Matrix-Product Codes. arXiv:2004.03538v1*

[16] D.Zeindler Permutation matrices and the moments of their characteristic polynomials. arXiv:0910.5069v2

[17] Kerber, Adalbert (1971)), Representations of permutation groups. I, Lecture Notes in Mathematics, Vol. 240, 240, Berlin, New York : Springer-Verlag, doi:10.1007/BFb0067943, ISBN 978-3-540-05693-5, MR 0325752

[18] Robinson, Derek J. S. (1996) A Course in the Theory of Groups. Graduate Texts in Mathematics. 80 (2nd ed.) Springer-Verlag. ISBN 978-1-4612-6443-9. Zbl 0836.20001

[19] Hall, Marshall (1999). The Theory of Groups. Providence: Chelsea Publishing. ISBN 978-0-8218-1967-8

[20] Zhang, Fuzhen (2005). The Schur Complement and Its Aplications. Springer. doi:10.1007/b105056. ISBN 0-387-24271-6.

[21] Stefano Nardeana, Massimiliano Ferronatob, Ahmad S. Abushaikhaa. A novel block non-symmetric preconditioner for mixed-hybrid finite-element-based flow simulations. arXiv:2009.13916v1 [math.NA] 29 Sep 2020.