1. BASIC FACTS

In a general setting, we can define a code in the following way:

- A $q$-ary code $C$ is a subset of sequences of length $n$ of symbols taken from a finite set $A$ with $q$ elements, which is called the alphabet of the code. The sequences in $C$ are called its words.

- The Hamming distance between two code words $v = (v_0, v_1, \ldots, v_{n-1})$ and $w = (w_0, w_1, \ldots, w_{n-1})$ to be the number of coordinates in which they differ; i.e.
  \[ d(v, w) = |\{i \mid v_i \neq w_i, \ 0 \leq i \leq n - 1\}|. \]

- The weight or minimum distance of a $C$ is the number:
  \[ w(C) = \min\{d(v, w) \mid v, w \in C\}. \]

- If the alphabet is a finite field $\mathbb{F}_q$, with $q$ elements and code words form a linear subspace of the vector space $\mathbb{F}_q^n$, then the code is called a $q$-ary linear code.

- A linear code $C$ is called a cyclic code if for every word $v = (v_0, v_1, \ldots, v_{n-1}) \in C$, the vector $(v_{n-1}, v_0, \ldots, v_{n-2})$ obtained from $v$ by the cyclic shift of coordinates $i \mapsto i + 1$, taken modulo $n$, is also in $C$. 
The vector space $\mathbb{F}_q^n$ can be constructed in different ways. In particular, the quotient ring

$$\mathcal{R}_n = \frac{\mathbb{F}_q[X]}{\langle X^n - 1 \rangle}$$

is an $n$-dimensional vector space over $\mathbb{F}_q$ and it is easy to see that a code is cyclic if and only if it maps, under the obvious isomorphism $\psi: \mathbb{F}_q^n \to \mathcal{R}_n$ to an ideal of $\mathcal{R}_n$.

- Given an ideal $I$ of $\mathcal{R}_n$, it is clear that there is a unique monic polynomial $g \in \mathbb{F}_q[X]$, which is a divisor of $X^n - 1$, such that $I$ is generated by the class $\overline{g}$ in $\mathcal{R}_n$. We shall refer to it as the generating polynomial of $I$.

- The polynomial $h = (X^n - 1)/g$ is such that the ideal annihilated by $h$ is precisely $I$ and is called the check polynomial of $I$.

- If $\gcd(q, n) = 1$, then $\mathcal{R}_n$ is semisimple and there is an idempotent $\varepsilon \in I$, which is the identity element in $I$ such that $I = \mathcal{R}_n \varepsilon$. A polynomial $e \in \mathbb{F}_q[X]$ such that $\overline{e} = \varepsilon$ will be called an idempotent generator of $I$.

- Since $g$ and $h$ are relatively prime, there exist polynomials $r, s \in \mathbb{F}_q[X]$ such that $rg + sh = 1$. If one of the polynomials $g, e$ is known, then the other can be found according to the following formulas:

$$e = rg, \quad g = \gcd(X^n - 1, e).$$

If we denote by $A = \langle a \mid a^n = 1 \rangle$ the cyclic group of order $n$, we have that

$$\mathcal{R}_n \cong \mathbb{F}_q A.$$

In this isomorphism, the class of indeterminate $X$ maps to the generator $a$ of $A$.

Hence, cyclic codes can also be defined as the ideals of the group algebra $\mathbb{F}_q G$. 

2. SOME MINIMAL CYCLIC CODES

• Let $g$ be an element of the finite abelian group $A$. The $q$-cyclotomic class of $g$ is the set

$$C_g = \{g^j | 0 \leq j \leq t_g - 1\},$$

where $t_g$ is the smallest positive integer, such that

$$q^{t_g} \equiv 1 \pmod{o(g)},$$

and $o(g)$ denotes the order of $g$.

• If $G = \langle a \rangle$ is a cyclic group of order $n$, then an element $g \in G$ is of the form $g = a^s$ and we can define the $q$-cyclotomic class of $s$ as the set of integers

$$\Omega_s = \{s, qs, q^2s, \ldots, q^{t_s - 1}s\}$$

where $t_s$ is the smallest positive integer such that $q^{t_s} \equiv s \pmod{n}$.

Codes of length $n = p^m$, when $q$ has order $\varphi(p^m)$ modulo $p^m$.

Let $p$ be a prime not dividing $q = |\mathbb{F}_q|$. Let $G = \langle a \rangle$ be a cyclic group of order $n$. Since $\mathbb{F}_qG$ is semisimple, to determine all the ideals of $\mathbb{F}_qG$ it suffices to describe the minimal ones; i.e., it suffices to find the set of primitive idempotents.

Given a cyclotomic class $C_i$ in $G$, we set

$$\overline{C_i} = \sum_{g \in C_i} g \in \mathbb{F}_qG.$$

**Lemma** Let $p$ and $q$ be as above and assume that $q$ has order $\varphi(p^m)$ modulo $p^m$. Then, $G$ contains $m + 1$ cyclotomic classes given by

$$C_i = \{a^{p_i-1}, a^{p_i-1}q, \ldots, a^{p_i-1}q^{\varphi(p^m-1)}\}, \quad 1 \leq i \leq m + 1.$$

**Theorem (Pruthi and Arora, 1997)** Under the conditions above, the group algebra $\mathbb{F}_qG$ has $m + 1$ primitive idempotents given by

$$e_0 = \frac{1}{p^m} \sum_{i=1}^{m+1} \overline{C_i},$$
\[ e_i = \frac{1}{p^{n-i+1}} [(p - 1)(1 + C_{i+1} + \cdots + C_m) - C_i], \]

\[ 1 \leq i \leq m. \]

In 1999 they gave similar results for codes of length \( 2p^m \).

Now:

\[
e_i(X) = \frac{1}{p^{n-i}} \sum_{j=0}^{p^{n-i}-1} X^{jp^i} - \frac{1}{p^{n-i-1}} \sum_{j=0}^{p^{n-i+1}-1} X^{jp^{i-1}}
\]

\[
= \frac{1}{p^{n-i-1}} \left[ p \sum_{j=0}^{p^{n-i}-1} X^{jp^i} - \sum_{j=0}^{p^{n-i+1}-1} X^{jp^{i-1}} \right]
\]

\[
= \frac{1}{p^{n-i-1}} \left[ (p - 1) \left( \sum_{j=0}^{p^{n-i}-1} X^{jp^i} \right) - \left( \sum_{j=1}^{p^{n-i}-1} X^{jp^i} \right) \right]
\]

\[
= \frac{1}{p^{n-i-1}} \left( p - \sum_{j=0}^{(p-1)p^{i-1}} X^{jp^{i-1}} \right) \left( \sum_{j=0}^{p^{n-i}-1} X^{jp^i} \right)
\]

Also:

\[
X^{p^n} - 1 = (X^{p^i} - 1) \sum_{j=0}^{p^{n-i}-1} X^{jp^i}
\]

\[
= (X^{p^{i-1}} - 1) \left( \sum_{j=0}^{(p-1)p^{i-1}} X^{jp^{i-1}} \right) \left( \sum_{j=0}^{p^{n-i}-1} X^{jp^i} \right)
\]
We can compute:

\[ g_i(X) = \gcd(X^{p^n} - 1, e_i(X)) \]
\[ = ((X^{p^{i-1}} - 1) \left( \sum_{j=0}^{p^{i-1}-1} X^{jp^j} \right)). \]

So:

\[ \dim(I_i) = p^n - \deg(g_i(X)) = p^n - p^i(p^{n-i} - 1) \]
\[ = p^i - p^{i-1} = \varphi(p^i). \]

3. AN APPROACH VIA GROUP ALGEBRAS

Let \( G \) be a cyclic group of order \( 2p^n \), \( p \) an odd prime. Write \( G = C \times A \) where \( A \) is the \( p \)-Sylow subgroup of \( G \) and \( C = \{1, t\} \) is its \( 2 \)-Sylow subgroup. Then, we have that

\[ FG \cong F(C \times A) \cong (FC)A \cong (FCe_1 \oplus FCe_2)A. \]

Since the two primitive idempotents of \( FC \) are

\[ e_1 = \frac{(1 + t)}{2} \quad \text{and} \quad e_2 = \frac{(1 - t)}{2} \]

we immediately have the following.

**Theorem (Arora and Pruthi, 1999)** Let \( F \) be a field with \( q \) elements and \( G \) a cyclic group of order \( 2p^n \), \( p \) an odd prime, such that \( o(q) = \varphi(p^n) \) in \( U(\mathbb{Z}_{2^m}) \). If \( e_i, \ 0 \leq i \leq n \), denote the primitive idempotents of \( FA \) then, the primitive idempotents of \( FG \) are

\[ \frac{(1 + t)}{2} \cdot e_i \quad \text{and} \quad \frac{(1 - t)}{2} \cdot e_i, \ 0 \leq i \leq n. \]
In the case of a cyclic group of order $p^n$, the lattice of subgroups is a chain:

$$G = A_0 \supset A_1 \supset \cdots \supset A_n = \{1\}.$$  

In this case, the elements

$$e_0 = \hat{A} \quad \text{and} \quad e_i = \hat{A}_i - \hat{A}_{i-1}, \quad 1 \leq i \leq n,$$

form a set of orthogonal idempotents such that

$$e_0 + e_1 + \cdots + e_n = 1.$$  

With the additional hypothesis that $q$ has order $\varphi(p^n)$ modulo $p^n$, it can be shown that these idempotents coincide with those obtained by Arora and Pruthi.

It is then natural to ask when is it possible to compute the primitive idempotents as done above; i.e., directly from the subgroup structure of $G$, without reference to the cyclotomic classes.

### 3.1 Semisimple group algebras with minimum number of simple components

In the case of finite group algebras of abelian groups, there is a direct way to determine the number of simple components.

Let $F$ be a finite field, with $|F| = q$ elements, and let $A$ be a finite abelian group such that $(q, |A|) = 1$.

If $\{e_1, \ldots, e_r\}$ is the set of primitive idempotents of $FA$, we have that

$$FA = \bigoplus_{i=1}^r (FA)e_i \simeq \bigoplus_{i=1}^r F_i,$$

where $F_i \simeq (FA)e_i$, $1 \leq i \leq r$ are fields which are finite extensions of $F$. Set

$$A = \bigoplus_{i=1}^r Fe_i.$$
Notice that \( F \epsilon_i \simeq F \) as fields in a natural way and that the number \( r \) of simple components is also the dimension of \( A \) as a vector space over \( F \).

**Theorem** Let \( F \) be a finite field, with \(|F| = q\), and let \( A \) be a finite abelian group. such that \((q, |A|) = 1\). Then, the number of simple components of \( FA \) is equal to the number of \( q \)-cyclotomic classes of \( A \).

Notice that, if \( h \) is an element in a cyclotomic class \( C_g \), then \( h = g^q \) for some \( j \). As \((q, o(g)) = 1\), it follows that \( \langle g \rangle = \langle h \rangle \). Hence, each \( q \)-cyclotomic class \( C_g \) is a subset of the set \( G_g \) of all generators of the cyclic group \( \langle g \rangle \). So, it is clear that the number of cyclic subgroups of \( A \) is a lower bound for the number of simple components and that this bound is attained if and only if \( S_g = G_g \), for all \( g \in A \).

For positive integers \( r \) and \( m \), we shall denote by \( r \in \mathbb{Z}_m \) the image of \( r \) in the ring of integer modulo \( m \). Then,

\[ G_g = \{ g^r \mid (r, o(g)) = 1 \} = \{ g^r \mid \bar{r} \in U(\mathbb{Z}_{o(g)}) \} \]

**Theorem** Let \( F \) be a finite field with \(|F| = q\), and let \( A \) be a finite abelian group, of exponent \( e \), such that \((q, |A|) = 1\). Then \( S_g = G_g \), for all \( g \in A \) if and only if \( U(\mathbb{Z}_e) \) is a cyclic group generated by \( \bar{q} \in \mathbb{Z}_e \).

As an easy consequence, we have the following.

**Corollary** Let \( F \) be a finite field with \(|F| = q\), and let \( A \) be a finite abelian group, of exponent \( e \). Then \( G_g = S_g \) for all \( g \in G \) if and only if one of the following holds:

(i) \( e = 2 \) and \( q \) is odd.
(ii) \( e = 4 \) and \( q \equiv 3 \pmod{4} \).
(iii) \( e = p^n \) and \( o(q) = \varphi(p^n) \) in \( U(\mathbb{Z}_{p^n}) \).
(iv) \( e = 2p^n \) and \( o(q) = \varphi(p^n) \) in \( U(\mathbb{Z}_{2p^n}) \).

### 3.2 Minimal Abelian Codes

We wish to extend the construction of primitive idempotents to the case of a finite abelian group \( A \). To be able to do so \( A \) must be either a \( p \)-group or a group of exponent \( e = 2p^n \). We shall first consider the
case of $p$-groups.

Let $A$ be an abelian $p$-group. For each subgroup $H$ of $A$ such that $A/H \neq \{1\}$ is cyclic we shall construct an idempotent of $FA$. We remark that, since $A/H$ is a cyclic group of $p^m$-power order, there exists a unique subgroup $H^*$ of $A$ containing $H$, such that $|H^*/H| = p$. We define $e_H = \hat{H} - \hat{H}^*$. Clearly $e_H \neq 0$ and we have the following.

**Lemma** The elements $e_H$, defined as above together with $e_A = \hat{A}$ form a set of pairwise orthogonal idempotents of $FA$ whose sum is equal to 1.

**Theorem** Let $p$ be an odd prime and let $A$ be an abelian $p$-group of exponent $p^r$. Then, the set of idempotents above is the set of primitive idempotents of $FA$ if and only if one of the following holds:

(i) $p^r = 2$, and $q$ is odd.
(ii) $p^r = 4$ and $q \equiv 3 \pmod{4}$.
(iii) $p$ is an odd prime and $\phi(q) = \Phi(p^n)$ in $U(\mathbb{Z}_{p^n})$.

Also, we have the following.

**Theorem** Let $p$ be an odd prime and let $A$ be an abelian group of exponent $2p^r$. Write $A = E \times B$, where $E$ is an elementary abelian $2$-group and $B$ a $p$-group. Then the primitive idempotents of $FA$ are products of the form $e.f$, where $e$ is a primitive idempotent of $FE$ and $f$ a primitive idempotent of $FB$.

Writing $E = \langle a_1 \rangle \times \cdots \times \langle a_n \rangle$, a product of cyclic groups of order 2, then the primitive idempotents of $FE$ are all products of the form $e = e_1e_2\cdots e_n$, where

$$e_i = \frac{1 + a_i}{2} \quad \text{or} \quad e_i = \frac{1 - a_i}{2}, \quad 1 \leq i \leq n.$$

It should be noted that these are the only cases where primitive idempotents of finite abelian group algebras can be computed in this way.

### 3.3 Dimensions of minimal abelian codes
We shall compute dimensions in the case of cyclic $p$-groups. Given an idempotent of the form $e_i = \hat{A}_i - \hat{A}_{i-1}$, we wish to determine the dimension of

$$I_i = FA \cdot e_i.$$ 

Notice that $\hat{A}_i = \hat{A}_{i-1} + e_H$, that all the three elements are idempotents and that $\hat{A}_{i-1}e_i = 0$. Thus

$$(FA)\hat{A}_i = (FA)\hat{A}_{i-1} \oplus (FA)e_i.$$ 

Hence

$$\dim_F((FA)e_i) = \dim_F((FA)\hat{A}_i) - \dim_F(FA)\hat{A}_{i-1}.$$ 

If $H$ is a normal subgroup of a group $G$, we have that

$$FG \cdot \hat{H} \cong F[G/H].$$ 

so

$$\dim_F((FA)e_i) = \dim_F(F[A/A_i]) - \dim_F(F[A/A_{i-1}]) = p^i - p^{i-1} = \varphi(p^i).$$

4. DIHEDRAL CODES

Let $D_n = \langle a, b \mid a^n = b^2 = 1, bab = a^{-1} \rangle$ be the dihedral group of order $2n$, let $\mathbb{F}_q$ be a field with $q$ elements and assume that $\text{char}(\mathbb{F}_q)$ does not divide $2n$. We wish to determine the values of $n$ for which the set of primitive central idempotents can be obtained in a natural way, as before. The results in this section are due to F.S. Dutra.

First, we remark that it can be shown that the number of simple components of $\mathbb{F}_q D_n$ is greater than or equal to the number of simple components of the rational group algebra $\mathbb{Q}D_n$. 
Theorem. The number of simple components of $\mathbb{F}_qD_n$ and $\mathbb{Q}D_n$ are equal if and only if one of the following conditions holds:

(i) $n = 2$ or $4$ and $q$ is odd.

(ii) $n = 2^m$, with $m \geq 3$ and $q$ is congruent to either 3 or 5, modulo 8.

(iii) $n = p^m$ with $p$ an odd prime and the class $\bar{q}$ is a generator of the group $\mathcal{U}(\mathbb{Z}_{p^m})$.

(iv) $n = p^m$ with $p$ an odd prime, the class $\bar{q}$ is a generator of the group $\mathcal{U}^2(\mathbb{Z}_{p^m}) = \{x^2 \mid x \in \mathcal{U}(\mathbb{Z}_{p^m})\}$ and $-1$ is not a square modulo $p^m$.

(v) $n = 2p^m$ with $p$ an odd prime and the class $\bar{q}$ is a generator of the group $\mathcal{U}(\mathbb{Z}_{2p^m})$.

(vi) $n = 2p^m$ with $p$ an odd prime, the class $\bar{q}$ is a generator of the group $\mathcal{U}^2(\mathbb{Z}_{p^m}) = \{x^2 \mid x \in \mathcal{U}(\mathbb{Z}_{2p^m})\}$ and $-1$ is not a square modulo $2p^m$.

(vii) $n = 4p^m$ with $p$ an odd prime and either $q$ or $-q$ has order $\varphi(p^m)$ modulo $4p^m$.

(viii) $n = p_1^{m_1}p_2^{m_2}$ with $p_1, p_2$ odd primes, $(\varphi(p_1^{m_1}), \varphi(p_2^{m_2})) = 2$ and either $q$ or $-q$ has order $\varphi(p_1^{m_1})\varphi(p_2^{m_2})/2$ modulo $p_1^{m_1}p_2^{m_2}$.

(ix) $n = 2p_1^{m_1}p_2^{m_2}$ with $p_1, p_2$ odd primes, $(\varphi(p_1^{m_1}), \varphi(p_2^{m_2})) = 2$ and either $q$ or $-q$ has order $\varphi(p_1^{m_1})\varphi(p_2^{m_2})/2$ modulo $p_1^{m_1}p_2^{m_2}$.

Denote $A = \langle a \rangle$ and let $\{e_m\}_{m \mid n}$ be the set of idempotents of $FA$. Then all these are also primitive central idempotents of $FD_n$, except for

$$e_1 = \frac{1}{n} \sum_{i=0}^{n-1} a^i = \hat{A}.$$

and, if $n$ is even, setting $A^2 = \langle a^2 \rangle$, also for

$$e_2 = \hat{A}^2 - \hat{A}.$$

When $n$ is odd, the idempotent $e_1$ splits into:

$$e_{11} = \frac{1+b}{2} e_1 \quad \text{and} \quad e_{12} = \frac{1-b}{2} e_1$$

and, when $n$ is even, both $e_1$ and $e_2$ split into:
e_{11} = \frac{1 + b}{2} e_1, \quad e_{12} = \frac{1 - b}{2} e_1

e_{21} = \frac{1 + b}{2} e_2 \quad \text{and} \quad e_{22} = \frac{1 - b}{2} e_2

REFERENCES