ECOLE POLYTECHNIQUE FEDERAL DE LAUSANNE

Cyclic codes and Uncertainty Principle

Author:
Othmane Rih

Supervisor:
Prof Maryna Viazovska

November 10, 2021

Introduction

The emergence of Coding theory begins in 1948. Claude Shannon (1916-2001), an engineer and a brilliant mathematician, also known for roaming on his unicycle while juggling and building machines that immediately shut down as soon as they turn on, presented his most famous paper "A Mathematical Theory of Communication" where he focuses on the following problem :

Suppose you want to send a message (a bunch of O and 1) through a noisy communication channel. The channel may be a telephone line, a high frequency radio link, or a satellite communication. The noise may be human error , lightning, imperfections in equipment,etc., and may result in errors so that the message received is different from the one we sent, how can we prevent that ? or more precisely, how can we detect those errors ? How many can we detect ? And can we correct them ?

This is where Richard Hamming (1915-1998), a famous mathematician and colleague of Shannon at Bell Labs, introduced the first error correcting code in 1950, known as the Hamming(7,4)-code. This was the beginning of a new subject, known as Error-correcting codes,or ECC, that has concrete applications. Space communications would not have been possible without their use, and the fact that we can still enjoy our CDs and DVDs even though they have a little scratch is also due to ECC.

In this report, we will present a long standing problem in error-correcting theory:
For a finite alphabet (like a binary one), can we get error-correcting codes that can guarantee a fixed amount of information that will be corrected, and that for any length of the said information.

We do not pretend to solve it here, but we will give some heuristic arguments that give a positive answer, but the question is still open for now.

Here is how the report is arranged : At the start, we will see how we can reformulate the uncertainty principle for a finite cyclic group of prime order [Tao, 2005], then we will give basic notions of Coding Theory and see how the reformulated uncertainty principle can help us construct codes over $\mathbb{C}$ (see [Evra et al., 2018],[Roth, 2006],[Kelbert, 2013]). In the next section, we will try to generalize the result of Section 1 to all finite fields (see [Evra et al., 2018]), and finally, we will discuss whether the codes that answer our problem exist or not [Evra et al., 2018].

Contents

Acknowledgements

I would like to express my sincere gratitude to Pr. Maryna Viazovska for her guidance, comments and suggestions through the course of this project.

1 Uncertainty principle revisited

Before introducing notions about cyclic codes, we will reformulate the uncertainty principle for finite cyclic groups of prime order. There is actually nothing uncertain in the uncertainty principle, but this name is widely used because of its similarity with the Heisenberg's uncertainty principle in physics. All the results here can be found in [Tao, 2005].

We recall some results ([Tao, 2005] 1.Introduction) :
Let $G = \mathbb{Z}/p\mathbb{Z}$ a finite cyclic group , $f : G \to \mathbb{C}$ a complex value function.
We define here the Fourier Transform $\hat{f} : G \to \mathbb{C}$ as follow :

$$\hat{f}(\xi) = \frac{1}{|G|} \sum_{x \in G} f(x)\overline{e(x,\xi)}.$$

Here $e(x,\xi) = e^{(2\pi i x\xi)/p}$ and $|G|$ denotes the cardinality of G.

Now by setting $supp(f) = \{x \in G : f(x) \neq 0\}$, it implies that :

$$\begin{aligned} sup_{\xi \in G}|\hat{f}| &\leq \frac{\sum_{x \in G} |f(x)|}{|G|} \\ &\leq \frac{|supp(f)|^{\frac{1}{2}}}{|G|^{\frac{1}{2}}} \left(\frac{\sum_{x \in G} |f(x)|^2}{|G|} \right)^{\frac{1}{2}} \\ &\leq \frac{|supp(f)|^{\frac{1}{2}}}{|G|^{\frac{1}{2}}} \left(\sum_{\xi \in G} |\hat{f}(\xi)|^2 \right)^{\frac{1}{2}} \\ &\leq \frac{|supp(f)|^{\frac{1}{2}}}{|G|^{\frac{1}{2}}} |supp(\hat{f})|^{\frac{1}{2}} sup_{\xi \in G}|\hat{f}|. \end{aligned}$$

Hence , if f is non-zero function, we get the famous uncertainty principle

$$|supp(f)||supp(\hat{f})| \geq |G|.$$

For more theory on Fourier analysis on groups, we refer to [Terras, 1999].

In this section, we will try to improve this inequality for finite prime cyclic groups.

Theorem (1.1): ([Tao, 2005], Theorem 1.1) Let p be a prime number. If $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ is a non-zero function, then

$$|supp(f)| + |supp(\hat{f})| \geq p + 1.$$

Conversely, if A and B are two subsets of $\mathbb{Z}/p\mathbb{Z}$ such that $|A| + |B| \geq p + 1$, then there exists a non-zero function f such that $supp(f) = A$ and $supp(\hat{f}) = B$.

Now, before getting to this result, few lemmas are necessary to obtain it.

Lemma (1.2): ([Tao, 2005] , Lemma 1.2) Let p be prime, $n \in \mathbb{N}_{\geq 1}$ and let $P(z_1, \ldots, z_n)$ be a polynomial with integer coefficients. If $P(\omega_1, \ldots, \omega_n) = 0$ for $\omega_1, \ldots, \omega_n$ p^{-th} roots of unity (not necessarily distinct), then $P(1, \ldots, 1)$ is a multiple of p .

Proof. We put $\omega = e^{(i2\pi)/p}$. Then, for each $0 \leq j \leq n$, we have $\omega_j = \omega^{k_j}$ for $0 \leq k_j \leq p$ an integer. We define $Q(z)$ as the remainder of $R(z) = P(z^{k_1}, \ldots, z^{k_n})$ divided by $z^p - 1$. Hence $R(z) = (z^p - 1)F(z) + Q(z)$ for a polynomial F with integer coefficient, and Q is a polynomial with integer coefficient, of degree at most $p - 1$. So by the previous equality, we have $Q(\omega) = 0$ and $Q(1) = R(1) = P(1, \ldots, 1)$.
But the fact that $Q(\omega) = 0$ and Q is a polynomial with integer coefficient of degree at most $p - 1$, tell us directly that Q is a multiple of the cyclotomic polynomial $\Phi_p = \sum_{i=0}^{p-1} X^i$, since it is the minimal polynomial of ω in $\mathbb{Z}[X]$.
Hence $Q(1) = R(1) = P(1, \ldots, 1) = \lambda p$ for some $\lambda \in \mathbb{Z}$. □

Using this lemma, we can prove that the determinant of the Fourier matrix is non-zero.

Lemma (1.3): ([Tao, 2005], Lemma 1.3) Let p prime, $x_1, \ldots, x_n$ distinct elements of $\mathbb{Z}/p\mathbb{Z}$ and $\xi_1, \ldots, \xi_n$ also be distinct elements of $\mathbb{Z}/p\mathbb{Z}$, then the matrix $(e^{(2\pi i x_j \xi_k)/p})_{1 \leq j,k \leq n}$ has non-zero determinant.

This is a famous (not the most famous) result due to Chebotarëv. The proof presented by Terrence Tao is quite clever and does not need any very advanced knowledge except the previous lemma.

Proof. Let $\omega_j = e^{(2\pi i x_j)/p}$, we define the following polynomial $D(z_1, \ldots, z_n) = det(z_j^{\xi_k})_{1 \leq j,k \leq n}$, which is a polynomial with integer coefficients.
Now we would like to show that $D(1, \ldots, 1)$ is not multiple of p, to obtain $D(w_1, \ldots, w_n) \neq 0$.
Unfortunately, $D(1, \ldots, 1) = det(1^{\xi_k})_{1 \leq j,k \leq n} = 0$, so Lemma 1.2 is not much of use, but D clearly vanishes when $z_j = z_{j'}$ for $j \neq j'$ (two lines are the same, hence the determinant is zero). Hence, we can factor D

$$D(z_1, \ldots, z_n) = P(z_1, \ldots, z_n) \prod_{1 \leq i < j \leq n} (z_i - z_j)$$

for some polynomial P with integer coefficients. So now, it suffices to compute $P(1, \ldots, 1)$ and apply Lemma 1.2 for P.
To compute $P(1, \ldots, 1)$, we consider the following expression :

$$(z_1 \frac{d}{dz_1})^0 \ldots (z_n \frac{d}{dz_n})^{n-1} D(z_1, \ldots, z_n)|_{z_1 = \ldots = z_n = 1}. \tag{1.1}$$

The main idea here is to differentiate D repeatedly to isolate P from any factor, so $P(1, \ldots, 1)$ will not disappear when evaluating at $z_1 = \ldots = z_n = 1$.

To simplify the explanation, let see what happens if we consider the following expression : $(z_n \frac{d}{dz_n})^{n-1} D(z_1, \ldots, z_n)$.

If we analyse $z_n(d/dz_n)D(z_1, \ldots, z_n)$, There are $n - 1$ terms where P is multiplied with $n - 2$ terms of the form $z_j - z_n$ (it means a $z_j - z_n$ has disappear for $1 \leq j \leq n$) and other terms where P have been differentiated (which means there is still a $z_j - z_n$).
Again, if we consider $(z_n(d/dz_n))^2 D(z_1, \ldots, z_n)$, there are $(n - 1)(n - 2)$ terms where P is multiplied with $n - 3$ terms of the form $z_j - z_n$, and other terms where $z_j - z_n$ appears more than $n - 2$ times for $1 \leq j \leq n$.
At the end, we have $(n - 1)!$ terms where P is multiplied with no $z_j - z_n$ and other terms where there is still a $z_j - z_n$ for $1 \leq j \leq n$.

Hence, if we analyse (1.1), there are terms where P is not multiplied by any $z_i - z_j$, and other terms where a $z_i - z_j$ haven't been differentiated for $1 \leq i < j \leq n$. So those terms will disappear

when evaluating at $z_1 = z_2 = \ldots = z_n = 1$. So (1.1)$= (n-1)!(n-2)!\ldots 1!P(1,\ldots,1)$, and since $n \leq p$, $(n-1)!(n-2)!\ldots 1!$ is not a multiple of p.

Now, we will still consider (1.1), but we reformulate it :

$$(z_1\frac{d}{dz_1})^0\ldots(z_n\frac{d}{dz_n})^{n-1}D(z_1,\ldots,z_n)|_{z_1=\ldots=z_n=1} = (z_1\frac{d}{dz_1})^0\ldots(z_n\frac{d}{dz_n})^{n-1}\begin{vmatrix} z_1^{\xi_1} & \cdots & z_n^{\xi_1} \\ \vdots & \ddots & \vdots \\ z_1^{\xi_n} & \cdots & z_n^{\xi_n} \end{vmatrix}|_{z_1=\ldots=z_n=1}$$

$$= \begin{vmatrix} (z_1\frac{d}{dz_1})^0 z_1^{\xi_1} & \cdots & (z_n\frac{d}{dz_n})^{n-1} z_n^{\xi_1} \\ \vdots & \ddots & \vdots \\ (z_1\frac{d}{dz_1})^0 z_1^{\xi_n} & \cdots & (z_n\frac{d}{dz_n})^{n-1} z_n^{\xi_n} \end{vmatrix}|_{z_1=\ldots=z_n=1}$$

$$= \begin{vmatrix} z_1^{\xi_1} & \cdots & \xi_1^{n-1} z_n^{\xi_1} \\ \vdots & \ddots & \vdots \\ z_1^{\xi_n} & \cdots & \xi_n^{n-1} z_n^{\xi_n} \end{vmatrix}|_{z_1=\ldots=z_n=1}$$

$$= \begin{vmatrix} 1 & \xi_1 & \cdots & \xi_1^{n-1} \\ \vdots & \vdots & \vdots & \\ 1 & \xi_n & \cdots & \xi_n^{n-1} \end{vmatrix}.$$

Thus, we get the determinant of a Vandermonde matrix, which is equal to $\prod_{1\leq k<k'\leq n}(\xi_k - \xi'_k)$. Since the $\xi_k < p$ are distinct, the determinant is not a multiple of p. Hence $P(1,\ldots,1)$ is not a multiple of p, so $P(\omega_1,\ldots,\omega_n) \neq 0$. Hence $D(\omega_1,\ldots,\omega_n) \neq 0$.

□

From this result, we obtain immediately this corollary that will prove the theorem.

Corollary (1.4): ([Tao, 2005], Corollary 1.4) If p is prime and A,$\tilde{A}$ subsets of $\mathbb{Z}/p\mathbb{Z}$, with $|A| = |\tilde{A}|$. Then the linear transform $T : l^2(A) \to l^2(\tilde{A})$ defined as $Tf = \hat{f}_{|_{\tilde{A}}}$ is invertible.

Here $l^2(A)$ is the set of function $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ which are equal to zero outside of A.

Proof. Here, the coefficients of the matrix are exactly like in the previous lemma.
We have that

$$T = \begin{pmatrix} e(x_1,\xi_1) & \cdots & e(x_p,\xi_1) \\ \vdots & \ddots & \vdots \\ e(x_1,\xi_p) & \cdots & e(x_p,\xi_p) \end{pmatrix} = \begin{pmatrix} e^{\frac{2\pi i x_1\xi_1}{p}} & \cdots & e^{\frac{2\pi i x_p\xi_1}{p}} \\ \vdots & \ddots & \vdots \\ e^{\frac{2\pi i x_1\xi_p}{p}} & \cdots & e^{\frac{2\pi i x_p\xi_p}{p}} \end{pmatrix}.$$

Hence our linear transform is invertible.

□

Now, we have all the tools to finally prove the theorem.

Proof of Theorem 1.1. Suppose that we have a non-zero function f such that

$$|supp(f)| + |supp(\hat{f})| \leq p.$$

Then if we consider $supp(f) = A$, there is a set $\tilde{A}$ in $\mathbb{Z}/p\mathbb{Z}$ which is disjoint from $supp(\hat{f})$ and $|A| = |\tilde{A}|$. Hence $Tf = 0$ and $f \neq 0$, which is not possible because of Corollary 1.4.

Now we prove the converse and consider the case $|A| + |B| = p + 1$.
We choose $\tilde{A}$ in $\mathbb{Z}/p\mathbb{Z}$ such that $\tilde{A} \cap B = \{\xi\}$. Now , by Corollary 1.4, there exists $f \in l^2(A)$ such

that $\hat{f}$ is zero on $\tilde{A}\backslash\{\xi\}$ and non-zero on $\{\xi\}$. So $supp(\hat{f}) \subseteq B$ implies $|supp(\hat{f})| \leq |B|$.

$$p+1 \leq |supp(f)| + |supp(\hat{f})| \leq |supp(f)| + |B| \Rightarrow |A| + |B| \leq |supp(f)| + |B| \\ \Rightarrow |A| \leq |supp(f)|.$$

Hence $supp(f) = A$, and thus $supp(f) = B$.
Now suppose $|A| + |B| > p + 1$ and $A = A' \bigcup A''$, $B = B' \bigcup B''$, such that $|A'| + |B'| = p + 1$ and $|A''| + |B''| = p+1$. Hence we get f',f'' such that $supp(f') = A'$ and $supp(\hat{f'}) = B'$, $supp(f'') = A''$ and $supp(\hat{f''}) = B''$.

- If $supp(f') \cap supp(f'') = \emptyset$, by setting $f = f' + f''$, we have $supp(f) = A$ and $supp(\hat{f}) = B$.
- If $supp(f') \cap supp(f'') \neq \emptyset$, we consider the set $X = \{-f'(a)/f''(a) | a \in supp(f') \cap supp(f'')\}$. It is sufficient to take $\alpha \in \mathbb{C}$ such that $\alpha \neq -f'(a)/f''(a)$ for every $a \in supp(f') \cap supp(f'')$, which is always possible, since X is a finite subset of $\mathbb{C}$. Hence, by setting $f = f' + \alpha f''$, we have $supp(f) = A$ and $supp(\hat{f}) = B$.

□

Remark (1.5): ([Tao, 2005] End of page 125) One result of the theorem that we will use later is that for any polynomial
$P(z) = \sum_{j=0}^{k} c_j z^{n_j}$ such that $c_j \neq 0$ for $0 \leq j \leq k$, and $0 \leq n_0 < \ldots < n_k < p$.
We can have at most k zeros when evaluating P at the p^{-th} roots of unity. Such a polynomial is only the Fourier Transform in $\mathbb{Z}/p\mathbb{Z}$ of function whose support has cardinality $k+1$, so the support of P must contain at least $p - k$ p^{-th} roots of unity by the previous Theorem 1.1 .

2 Notions of Coding theory

In this section, we introduce notions about codes. Then, we will see how we can link cyclic codes of length n and ideals of $\mathbb{F}_l[\mathbb{Z}/n\mathbb{Z}]$. More precisely, we will describe what happens when n is prime. Also, Using the results of Section 1, we will prove the existence of good cyclic codes over the field $\mathbb{C}$.

Definition (2.1): ([Roth, 2006], 1.3 Block codes) Let F a finite alphabet, $n, M \in \mathbb{N}_{\geq 1}$, an $[n, M, d]$-code C is a subspace of F^n of cardinality M such that $\forall a \neq 0 \in C$, $d = \min_{a \in C} wt(a)$.
$wt(a)$ is called the weight of a, which is the number of non-zero components of a.
The dimension of C is defined by $k = log_{|F|}M$ and the information rate by $R = \frac{k}{n}$.

Here is some elementary examples (see [Roth, 2006], Example 1.3 and 1.4) :

- The binary repetition code $[3, 2, 3]$ is $\{000, 111\}$. The dimension is $k = log_2(2) = 1$.
- The binary parity code $[3, 4, 2]$ is $\{000, 011, 101, 110\}$. The dimension is $k = log_2(4) = 2$.

Definition (2.2): ([Roth, 2006], 2.1 Definition) Let F a finite field, $n, M \in \mathbb{N}_{\geq 1}$, an $[n, M, d]$-code C over F is linear if C is a linear subspace of F^n over F.
If k is the dimension like in the previous definition, then C is a linear $[n, k, d]$-code.

The parity code over $\mathbb{F}_2$ is a linear $[3, 2, 2]$ code, spanned by $(0, 1, 1)$ and $(1, 0, 1)$ ([Roth, 2006], Example 2.1).

Remark (2.3): In most common definitions, F is a finite field , but we can find in the the literature codes over $\mathbb{C}$ or $\mathbb{R}$, see [Mohamed et al., 2016].

Definition (2.4): ([Roth, 2006], 8.1 Definition) A linear Code C is called cyclic if it is invariant under cyclic permutation :

$$(a_0, a_1, \ldots, a_n) \in C \Leftrightarrow (a_{n-1}, a_0, \ldots, a_{n-2}) \in C.$$

The parity code over $\mathbb{F}_2$ is an example of cyclic code.

Definition (2.5): ([Evra et al., 2018], Introduction) A family of codes $C(n)$ of parameters $[n, k_n, d_n]$ is said to be asymptotically good or good if there exists a constant $c > 0$ such that :

$$\frac{k_n}{n} \geq c, \quad \frac{d_n}{n} \geq c$$

for all $n \in \mathbb{N}$.

An example of good cyclic codes are the so-called Justensen codes, which are a class of concatenated codes ([Kelbert, 2013], Definition 3.5.3).

To make our work on cyclic code easier, we will see how we can assimilate cyclic codes over a field F, to ideals in the ring $F[X]/(X^n-1)$.

Proposition (2.6): ([Evra et al., 2018] Proposition 2.5) Let $n \geq 1$ and F a field, we consider the isomorphism between F^n and $R = F[X]/(X^n-1)$ defined by :

$$\phi : (a_0, \ldots, a_{n-1}) \to \sum_{i=0}^{n-1} a_i X^i.$$

C is cyclic code over F if and only if $\phi(C)$ is an ideal of R.

Proof. Suppose C is a cyclic code, therefore C is a subspace of the vector space F^n, which means C is a subgroup. Thus $\phi(C)$ is a subgroup under addition in R.
Now let $c = (c_1, \ldots, c_n) \in C$, therefore $x\phi(c) = c_{n-1} + xc_o + x^2c_1 + \ldots + x^{n-1}c_{n-2} \in \phi(C)$ since $(c_{n-1}, c_0, \ldots, c_{n-2}) \in C$.
In general , $x^i\phi(c) = c_{n-i} + c_{n-i+1}x + \ldots + c_{n-1}x^{i-1} + c_0x^i + \ldots + c_{i-1}x^{n-1} \in \phi(C)$, for $1 \leq i \leq n$.
Let $a(x) = \sum_{i=0}^{n-1} a_i x^i \in R$, thus $a(x)\phi(c) = \sum_{i=0}^{n-1} a_i x^i \phi(c) \in \phi(C)$, therefore $\phi(C)$ is an ideal.

Conversely, suppose I is an ideal in R, hence I is a subgroup of R, thus $\phi^{-1}(I) = C$ is a subspace of F^n.
Let $c(x) = \sum_{i=0}^{n-1} c_i x^i \in I$, then $x^i c(x) \in I$ for $0 \leq i < n$ since I is an ideal, but this says that all the cyclic shifts of $c(x)$ are in I. Hence $\phi^{-1}(I) = C$ is a cyclic code.

□

Now , to describe the ideals of R, we consider the case where $n = p$ is prime.

Proposition (2.7): ([Evra et al., 2018] Proposition 2.6) Suppose p prime, F a field such that $p \neq char(F)$, Then :

1. The ring $R = F[X]/(X^p-1)$ is a direct sum of finite extensions of F.
2. If $x^p - 1$ splits in linear factors, R is isomorphic to F^n as ring.
3. Assume $F = \mathbb{F}_l$, a finite field of order l, $r = ord_p(l)$ (the order of l as an element of the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^* = \mathbb{F}_p^*$), then

   $$R = \mathbb{F}_l[X]/(X^p-1) = \mathbb{F}_l \oplus (\mathbb{F}_{l^r})^s$$

   for $s = (p-1)/r$.

Proof. 1. Since $p \neq char(F)$, we have that $X^p - 1$ is separable in $F[X]$. Hence it factors as a product of distinct irreducible polynomials $X^p - 1 = \prod_{i=0}^{s} g_i$. In particular, $g_0 = X - 1$. Thus, from the Chinese remainder theorem

$$R \cong \bigoplus_{i=0}^{s} F[X]/(g_i).$$

Since g_i is irreducible, each $F[X]/(g_i)$ is a field extension of F of degree $deg(g_i)$.

2. We have $X^p - 1 = \prod_{i=1}^{p}(X - \mu_i)$. But since $F[X]/(X - \mu_i) \cong F$ for each $1 \leq i \leq p$, we have

$$R \cong \bigoplus_{i=1}^{p} F[X]/(X - \mu_i) \cong F^p.$$

.

3. We know that $\mathbb{F}_p^*$ is a cyclic htr group of order $p-1$, so the order r of l modulo p divides $p-1$, hence $sr = p-1$ is an integer.
We know that $l^r \equiv 1[p]$ and $\mathbb{F}_{l^r}^*$ is a cyclic group of order $l^r - 1$. But since p divides $l^r - 1$, there exists an element of order p in $\mathbb{F}_{l^r}$. So $\mathbb{F}_{l^r}$ contains all the p-th roots of unity. Hence $\mathbb{F}_{l^r}$ is the splitting field of $X^p - 1$. So for each root of unity μ, $\mathbb{F}_l[\mu]$ is equal to $\mathbb{F}_{l^r}$, and since the degree of the extension is r, the irreducible factors of $X^p - 1$ are of degree r, except $X - 1$. Hence :
$$R = \mathbb{F}_l \oplus (\mathbb{F}_{l^r})^s.$$

□

Now we can describe the ideals of R, since in each case R is just a finite direct sum of fields. Suppose we are in case 2, then an ideal I of R is a finite product of ideals : $I = I_1 \oplus I_2 \ldots \oplus I_p$, where $I_j = 0$ or $I_j = F$ for $1 \leq j \leq p$.

We would like now to compute the dimensions of our cyclic codes.

Lemma (2.8): ([Evra et al., 2018] Lemma 2.8) Let p prime,F a field, f a polynomial in $F[X]$ and I_f the ideal generated by the image of f in $R = F[X]/(X^p - 1)$ and $g = gcd(f, X^p - 1)$. Then :

1. $I_f = I_g$.
2. dim(I_f)=dim(I_g)=$p - deg(g)$.

Proof. 1. We have that g divides f in $F[X]$ and since $F[X]$ is a principal ideal domain, there exists h_1,h_2 in $F[X]$ such that $g = h_1 f + h_2(X^p - 1)$. So f divides g in R, hence $I_f = I_g$ in R.

2. by the previous equality in 1, we have dim(I_g)=$deg((X^p - 1)/g) = p - deg(g)$.

□

Remark (2.9): We denote $Z(f) = deg(gcd(f, X^p - 1))$ for any polynomial in $F[X]$ and prime p. As we have seen, if F has characteristic different from p, then $X^p - 1$ is a separable polynomial. So $Z(f)$ is therefore the number of p-th roots of unity ξ, in an algebraic closure of F, such that $f(\xi) = 0$.

Using the results of the previous section, we prove the existence of good cyclic codes over the field $\mathbb{C}$.

Theorem (2.10): ([Evra et al., 2018] Theorem 3.3) Let p a prime, $f(X) = \sum_{i=0}^{p-1} a_i X^i \in \mathbb{C}[X]$. Let $wt(f) = |\{i | a_i \neq 0\}|$ and $Z(f) = |\{\mu \in \mu_p(\mathbb{C}) | f(\mu) = 0\}|$ i.e the number of $p-$th roots of unity which are also roots of f. Then :
$$wt(f) - Z(f) \geq 1.$$

Proof. Like in Remark 1.5, f can be seen has the Fourier transform of a function $g \in \mathbb{C}^{\mathbb{Z}/p\mathbb{Z}}$. Hence, if we see $f \in \mathbb{C}^{\mathbb{Z}/p\mathbb{Z}}$, we have that $|supp(g)| = wt(f)$ and $|supp(f)| = p - Z(f)$, and so :
$$|supp(g)| + |supp(f)| \geq p + 1 \Rightarrow wt(f) - Z(f) \geq 1.$$

□

Remark (2.11): We have equality for the cyclotomic polynomial $f = 1 + X \ldots + X^{p-1}$, where $wt(f) = p$ and $Z(f) = p - 1$.

Now we can use Lemma 2.8 to reformulate Theorem 2.10 : if $f \in \mathbb{C}[X]$ such that $deg(f) < p$, then f can be seen as en element of $R = F[X]/(X^p - 1)$. Thus, by Lemma 2.8, the dimension of I_f satisfies
$$dim(I_f) = p - Z(f)$$
where $Z(f) = deg(gcd(f, X^p - 1))$.

We get therefore the following theorem :

Theorem (2.12): ([Evra et al., 2018] Theorem 3.5) For all $f \in \mathbb{C}[X]$ such that $deg(f) < p$, f can be considered as an element of $R = F[X]/(X^p - 1)$. Therefore

$$wt(f) + dim(I_f) \geq p + 1$$

where I_f is the ideal generated by f in R.

Now we can finally construct our good family of cyclic codes :

Corollary (2.13): ([Evra et al., 2018] Corollary 3.6) There exists a good family of cyclic codes over $\mathbb{C}$.

Proof. Let $\xi = e^{(i2\pi)/p} \in \mathbb{C}$ and $f(X) = \prod_{i=1}^{(p-1)/2} (X - \xi^i)$. Since f divides $X^p - 1$, we have $dim(I_f) = p - deg(f) = (p+1)/2$ by Lemma 2.8.
Let $h \neq 0$ an element of I_f, then $dim(I_h) \leq dim(I_f)$. Hence

$$wt(h) \geq p + 1 - dim(I_h) \geq p + 1 - dim(I_f) \geq \frac{p+1}{2}$$

by Theorem 2.12.
So the Ideal $C_p = I_f$ is a $[p, (p-1)/2, (p+1)/2]_{\mathbb{C}}$-cyclic code, and the family $\{C_p\}_{p\,prime}$ is a good family of cyclic codes □

3 Generalisation of The Uncertainty principle

We saw how the uncertainty principle can help us build good cyclic codes over $\mathbb{C}$, it will make sense to see if we can try to generalise the same pattern for any field. Unfortunately, as we will see, the uncertainty principle does not hold over all fields, but maybe we can find a weaker version that still hold.
(A little digression, we cannot resist to mention the result of Roy Meshulam [Meshulam, 2006] as an improvement of Terrence Tao results [Tao, 2005] for finite abelian groups)

Definition (3.1): ([Evra et al., 2018] Definition 4.1) Let F be a field, p a prime number and $R = F[X]/(X^p - 1)$. For $f \in R$, represented by a polynomial of degree $< p$, we denote by I_f the ideal generated by f in R, and we denote

$$\mu_{F,p}(f) = wt(f) + dim(I_f).$$

We define the invariant

$$\mu_{F,p} = min\{\mu_{F,p}(f) | 0 \neq f \in R\}.$$

Some simple remarks ([Evra et al., 2018] Section 4) :

1. for $f = 1 + X + \cdots + X^{p-1}$, we have $wt(f) = p$ and $dim(I_f) = 1$. Hence $\mu_{F,p} \leq p+1$ for any field F and prime p.
2. Like we have seen in section 2, $\mu_{\mathbb{C},p} = p + 1$ for any prime p

We can now reformulate the uncertainty principle as follows :

Definition (3.2): ([Evra et al., 2018] Definition 4.2) A field F is said to satisfy the uncertainty principle if, for any prime number p, we have $\mu_{F,p} > p$ or equivalently $\mu_{F,p} = p + 1$.

Now the question that we want to answer is : Are there fields that satisfy Definition 3.2 ?
Here are some results about finite fields that approach Definition 3.2 :

Proposition (3.3): ([Evra et al., 2018] Proposition 4.3) Let $F = \mathbb{F}_l$ a finite field of prime order and l is a primitive root modulo p i.e $ord_p(l) = p - 1$. Then $\mu_{F,p} = p + 1$.

Proof. Let $r = ord_p(l) = p - 1$. By Proposition 2.7, there are $s = (p-1)/r$ irreducible polynomials of degree r that divides $\Phi_p = 1 + X \cdots + X^{p-1}$. But since $s = 1$ and $r = p - 1$, Φ_p is irreducible in $\mathbb{F}_l[X]$. So for every polynomial $f \in \mathbb{F}_l[X]$ of degree less then p, the gcd of f and $X^p - 1$ can only be 1, $X - 1$ or Φ_p. Therefore, the dimension $dim(I_f) = p - deg(gcd(f, X^p - 1))$ is equal to p, $p - 1$ or 1, respectively (by Lemma 2.8).

1. If $dim(I_f) = p$, then $wt(f) \geq 1$ ($f \neq 0$) and $\mu_{\mathbb{F}_l,p}(f) \geq p + 1$.

2. If $dim(I_f) = p-1$, we get $X-1 = gcd(f, X^p-1)$ and $X-1$ divides f. So $f = (X-1)f_2$ such that $wt(f_2) \geq 1$, therefore $f_2 = c + Xf_3$ with $c \neq 0$. So $f = c(X-1) + X(X-1)f_3$ and thus $wt(f) = wt(c(X-1) + X(X-1)f_3) \geq wt(c(X-1)) = 2$. Hence $\mu_{\mathbb{F}_l,p}(f) \geq p-1+2 = p+1$.

3. Suppose $dim(I_f) = 1$, then $gcd(f, X^p-1) = \Phi_p$, and $f = c\Phi_p$ for some $c \neq 0$ since $deg(f) < p$. So $wt(f) = p$ which means $\mu_{\mathbb{F}_l,p}(f) = p+1$.

□

Other examples of fields that approach our definition :

Proposition (3.4): ([Evra et al., 2018] Proposition 4.4) if F is a field of characteristic p prime, then $\mu_{F,p} = p+1$.

Proof. By Lemma 2.8, we need to show that for any $0 \neq f \in R = F[X]/(X^p-1)$, we have

$$wt(f) > p - dim(I_f) = deg(gcd(f, X^p-1)).$$

Since F has characteristic p, we have $X^p - 1 = (X-1)^p$, so there is $0 \leq m \leq p$ such that $gcd(f, X^p-1) = (X-1)^m$. So we need to prove that $wt(f) > m$.
We do it by induction on $deg(f) < p$.

- For $deg(f) = 0$, we have $f = c \neq 0$ and if $(X-1)^m$ divides f, then $m = 0$ and thus $wt(f) = 1 > 0$.
- Now suppose $deg(f) > 0$ and that the property is valid for all polynomials of degree $< deg(f)$:
  - If $f(0) = 0$, then $(X-1)^m$ divides $f(X)/X = g(X)$, but since $deg(g) < deg(f)$ and $wt(f) = wt(g)$, we have $wt(f) = wt(g) > m$.
  - If $f(0) \neq 0$:
    - Suppose $m = 0$, then $f = c + Xf_2$ for $c \neq 0$ and $f_2 \in R$. Hence $wt(f) \geq wt(c) = 1 > 0$.
    - Suppose $m > 1$, thus $f = (X-1)^m f_1$ for $f_1 \in R$. Therefore, $f' = (X-1)^{m-1} f_1 + (X-1)^m f_1'$, so $(X-1)^{m-1}$ divides f', which means $wt(f') > m-1$ by induction. But since $f(0) \neq 0$, it means that $wt(f) = wt(f') + 1$, and therefore $wt(f) > m$.

□

We gave fields that are close to our definition, but still, that is not what we are looking for. So maybe the answer to our question is negative. Actually, Borello and Solé proved under some conjecture that no finite field satisfies the uncertainty principle ([Borello and Solé, 2021] Corollary 3.1).

So the only field that we know that satisfies Definition 3.2 is $\mathbb{C}$. Thus, maybe we can come up with a result for fields of characteristic 0.

Theorem (3.5): ([Evra et al., 2018] Theorem 4.6) For every field of characteristic 0 and for every prime p, we have $\mu_{F,p} = p+1$.

To prove this, we will need the following lemma :

Lemma (3.6): ([Evra et al., 2018] Lemma 4.5) Let p prime, and F a field of characteristic 0 and $f = \sum_{i=0}^{p-1} a_i X^i$ a non-zero element of $R = F[X]/(X^p-1)$. Then for every prime q, there exists a field E of characteristic q and a polynomial $\tilde{f} \in E[X]/(X^p-1)$ such that $wt(\tilde{f}) < wt(f)$ and $dim_E(I_{\tilde{f}}) < dim_F(I_f)$.

Proof of Theorem 3.5. By Lemma 3.6, for $q = p$, we have $\mu_{E,p}(\tilde{f}) \leq \mu_{F,p}(f)$. Thus, since E has characteristic p, $\mu_{F,p}(f) \geq \mu_{E,p}(\tilde{f}) > p$ by Proposition 3.4. Therefore, the inequality is true for all non-zero f and the result follows. □

Since it seems rather difficult to find finite fields that actually correspond to Definition 3.2, it would be reasonable to weaken our definition :

Definition (3.7): Let δ a real number such that $0 < \delta \leq 1$, we say that F satisfy the δ-uncertainty principle for a prime p if

$$\mu_{F,p} > \delta p.$$

Some examples :

- We consider the field $F = \mathbb{F}_2$ and $p = 3$. This satisfies Proposition 3.4, hence $\mu_{\mathbb{F}_2,3} = 4 > \delta 3$ for any $0 < \delta \leq 1$
- ([Evra et al., 2018] Example 5.2) Actually we can come up with a class of examples : Suppose Artin's Conjecture is true (This was proved by Hooley [Hooley, 1967] under the Generalized Riemann Hypothesis), then for any prime l, there exists an infinite set of primes P such that l is a primitive root in $\mathbb{F}_p^*$ for all $p \in P$. Thus, by Proposition 3.3, $\mu_{\mathbb{F}_l,p} = p + 1 > \delta p$ for any prime $p \in P$.

Remark (3.8): ([Evra et al., 2018] Example 5.2) Even though we came up with finite fields that satisfy the uncertainty principle for an infinite set of primes, this example does not lead to good cyclic codes. Suppose a proper ideal $I_p \subset \mathbb{F}_l[X]/(X^p - 1)$, if we refer to the proof of Proposition 3.3, I_p is generated either by $X - 1$ or Φ_p.
In the first case, we get $dim(I_p) = p - deg(X - 1) = p - 1$ and

$$wt(h) \geq p + 1 - dim(I_h) \geq p + 1 - dim(I_f) = wt(f) = 2$$

for any $h \in I_f$. Hence, the distance of I_p is 2.
In the second case, $dim(I_p) = p - deg(\Phi_p) = 1$ and

$$wt(h) \geq p + 1 - dim(I_h) \geq p + 1 - dim(I_f) = wt(f) = p$$

for any $h \in I_f$. Hence, the distance of I_p is p.
So as $p \to \infty$, one of the inequalities of Definition 2.5 fails in both cases.

It seems that our new definition is not sufficient to guarantee good cyclic codes, but maybe by adding more irreducible factors to $X^p - 1$, which means adding a new condition on $ord_p(l)$, we can hope for a better outcome.

Definition (3.9): ([Evra et al., 2018] Definition 5.3) Let δ, ϵ real numbers, such that $0 < \epsilon < \delta \leq 1$. We say that the field $\mathbb{F}_l$ satisfy the ϵ-δ uncertainty principle if there exists an infinite set of primes P such that :

1. $\mu_{F,p} > \delta p$
2. $ord_p(l) < \epsilon p$.

If a finite field $\mathbb{F}_l$ satisfy our definition, it implies directly the existence of good cyclic codes.

Theorem (3.10): ([Evra et al., 2018] Theorem 5.4) Let $\mathbb{F}_l$ a finite field of order l that satisfy the ϵ-δ uncertainty principle for δ,ϵ reals numbers. Then there exists a family of good cyclic codes over $\mathbb{F}_l$.

Proof. For each prime $p \in P$ like in Definition 3.9, let $I_p \subset \mathbb{F}_l[X]/(X^p - 1)$ a non-zero ideal and $r = ord_p(l) \geq 1$. By Proposition 2.7, $dim(I_p) \in A = \{1, r, r + 1, \ldots, sr, sr + 1\}$ where $s = (p-1)/r$. We take I_p such that $dim(I_p) = max\{a \in A | a \leq \epsilon p\}$.Then either $dim(I_p) = jr$ or $dim(I_p) = ir + 1$ for $0 \leq i \leq s$ and $0 < j \leq s$. Now, we show that $\epsilon p/2 < dim(I_p) \leq \epsilon p$:

- If $dim(I_p) = jr$ for $0 < j \leq s$, then

$$jr \leq \epsilon p < jr + 1 \Rightarrow \frac{jr}{2} \leq \frac{\epsilon p}{2} < \frac{jr+1}{2} \leq jr.$$

  So $\epsilon p/2 < dim(I_p) \leq \epsilon p$.

- Suppose $dim(I_p) = ir + 1$:
  - If $i = 0$, then $dim(I_p) = 1 \leq \epsilon p < r$ by our choice of I_p, which is not possible since $r = ord_p(l) < \epsilon p$. So we must have $dim(I_p) = r < \epsilon p < r + 1$. However, since $r = 1$, it means $\epsilon p/2 < 1 = dim(I_p)$.
  - if $i \geq 1$, then

$$ir + 1 \leq \epsilon p < (i+1)r \Rightarrow \frac{ir+1}{2} \leq \frac{\epsilon p}{2} < \frac{(i+1)r}{2} < ir + 1.$$

    We used the fact that

$$ir + 1 - \frac{(i+1)r}{2} = r\frac{(i-1)}{2} + 1 > 0.$$

    So $\epsilon p/2 < dim(I_p)$.

  In conclusion, we have that $\epsilon p/2 < dim(I_p) \leq \epsilon p$ by our choice of I_p.

  For every element $h \in I_p$, we have $I_h \subset I_p$ and hence $dim(I_h) \leq dim(I_p)$. Therefore, we get :

$$wt(h) > \delta p - dim(I_h) \geq \delta p - dim(I_p) \geq (\delta - \epsilon)p.$$

The cyclic code I_p has length p, distance greater than $(\delta - \epsilon)p$ and dimension greater than $\epsilon p/2$. Hence by Definition 2.5, the sequence $(I_p)_{p \in P}$ is an infinite sequence of good cyclic codes over $\mathbb{F}_l$. □

Actually, the fact that a finite field satisfy the ϵ-δ uncertainty principle give us more information about δ :

Proposition (3.11): ([Borello and Solé, 2021] Proposition 4.1) If $\mathbb{F}_q$ satisfies the ϵ-δ uncertainty principle, then $\delta < \frac{q-1}{q}$.

4 Existence of Good Cyclic codes

In this chapter, we give some heuristic arguments that show the existence of good cyclic codes over $\mathbb{F}_2$, the most common field in coding theory. All heuristic arguments are from section 6 of [Evra et al., 2018]

The problem we are interested in can be formulated as follows : Is there a family of good cyclic codes for any finite field ? At first, most evidences indicate the nonexistence of good cyclic codes. The first result in that sense was stated by Berman in 1967 for a particular class of cyclic codes :

Theorem (4.1): ([Berman, 1970] Theorem 2.1) Let $p_1, \dots, p_s$ be fixed prime numbers, and C_t a family of $[n_t, k_t, d_t]_F$ cyclic codes over the finite field F of characteristic $p \neq p_i$ for $1 \leq i \leq s$. Every cyclic code of C_t has length $n_t = p_1^{\alpha_1} \dots p_s^{\alpha_s}$ for $\alpha_i \in \mathbb{N}_{\geq 1}$ and $1 \leq i \leq s$. If $(k_t/n) > 0$ for all t, there exists a constant C such that $d_t \leq C$ for all t.

In particular, this is not a family of good cyclic codes even though $(k_t/n) > 0$ for all t since $d_t/n \leq C/n \underset{n \longrightarrow \infty}{\longrightarrow} 0$.

Another important result shown by Lin and Weldon is that long BCH codes are not good cyclic codes.

Definition (4.2): ([Lint, 1992] Definition 6.6.1) A cyclic code of length n over $\mathbb{F}_q$ is called a BCH code of designed distance δ if its generator $g(x)$ is the least common multiple of the minimal polynomials of $\beta^l, \beta^{l+1}, \dots, \beta^{l+\delta-2}$ for some l, where β is a primitive n-root of unity.
Usually $l = 1$ (called a narrow-sense BCH code). If $n = q^m - 1$, i.e β is a primitive element of $\mathbb{F}_{q^m}$, the BCH code is called primitive.

The terminology "designed distance" is explained by the following theorem.

Theorem (4.3): ([Lint, 1992] Theorem 6.6.2) The minimum distance of a BCH code with the designed distance d is at least d.

In step 2 of [Lin and Weldon, 1967], the information rate approaches 0 as the length's code increases. Hence BCH codes are not a family of good cyclic codes.

Since it is difficult to come up with results for all finite fields, we describe some heuristic arguments that all point in the direction of the existence of families of good cyclic codes over $\mathbb{F}_2$.

Lemma (4.4): ([Evra et al., 2018] Lemma 6.1) Let δ a fixed real number with $0 < \delta < 1/2$. Let S_δ be the set of polynomials f in $\mathbb{F}_2[X]/(X^p - 1)$ with $wt(f) \leq \delta p$. Then we have $|S_\delta| = 2^{pH'(\delta)+o(p)}$ where $H'(\delta) = H(\delta)/log(2)$ and $H(\delta) = -\delta log(\delta) - (1-\delta)log(1-\delta)$.

Proof. We know that the number of polynomials such that $wt(f) = \lfloor \delta p \rfloor$ is $p!/\{\lfloor \delta p \rfloor !(p - \lfloor \delta p \rfloor)!\}$. Hence

$$\binom{p}{\lfloor \delta p \rfloor} \leq |S_\delta| = \sum_{i=0}^{n=\lfloor \delta p \rfloor} \binom{p}{i} \leq p \binom{p}{\lfloor \delta p \rfloor}.$$

Since $\lfloor \delta p \rfloor \leq \lfloor p/2 \rfloor$, it implies that

$$\binom{p}{i} \leq \binom{p}{\lfloor \delta p \rfloor} \leq \binom{p}{\lfloor \frac{p}{2} \rfloor}$$

for $0 \leq i \leq \lfloor \delta p \rfloor$.

Hence by Stirling formula we have that :

$$\begin{aligned}
\binom{p}{\lfloor \delta p \rfloor} \sim \binom{p}{\delta p} &\sim \frac{1}{\sqrt{2\pi}} \sqrt{\frac{p}{\delta p(p-\delta p)}} \frac{p^p}{\delta p^{\delta p}(p-\delta p)^{p-\delta p}} \\
&\sim \frac{1}{\sqrt{2\pi}} \sqrt{\frac{p}{\delta p(p-\delta p)}} e^{p(-\delta log(\delta)-(1-\delta)log(1-\delta))} \\
&\sim \frac{1}{\sqrt{2\pi}} \sqrt{\frac{1}{\delta p(1-\delta)}} e^{pH(\delta)} \\
&\sim e^{pH(\delta)+o(p)} \qquad since \quad log(\frac{1}{\sqrt{p}}) = o(p) \\
&\sim 2^{pH'(\delta)+o(p)}.
\end{aligned}$$

Since $p\binom{p}{\delta p} \sim 2^{pH'(\delta)+o(p)}$, we have $|S_\delta| = 2^{pH'(\delta)+o(p)}$. □

Now we would like to control $ord_p(2)$ for an infinite set of primes, so that we get ideals of large dimensions.

Lemma (4.5): ([Evra et al., 2018] Lemma 6.2) For any ϵ with $0 < \epsilon < 1$, there exist infinitely many primes p such that $ord_p(2) < \epsilon p$.

The interest of having $r = ord_p(2)$ "small" compared with p is to let the ring $R = \mathbb{F}_2[X]/(X^p-1)$ contains many ideals. In particular, by looking for ideals of dimension $ir \approx \xi p$ for $0 < \xi < 1$, we have, by Proposition 2.7, approximately $\binom{s}{i}$ ideals of dimension ξp where $s = (p-1)/r$. Therefore $i \approx \xi p/r \approx \xi s$. So, as in Lemma 4.4, this number grows exponentially with s.

Now we fix some real number η with $0 < \eta < 1$. Let p a prime such that there exists an ideal I_p in $R = \mathbb{F}_2[X]/(X^p - 1)$ with $dim(I_p) \sim \eta p$. Let $\delta > 0$ be another parameter. We assume that the probability for an element of I_p to be in the set S_δ of Lemma 4.4 is approximately the same as the probability for a general element of R. The expected cardinality of the intersection $S_\delta \cap I_p$ should be about

$$\frac{|S_\delta||I_p|}{|R|} \simeq 2^{pH'(\delta)+dim(I_p)-p+o(1)} = 2^{p(H'(\delta)-(1-\eta))+o(1)}.$$

If δ and η are chosen so that $1 - \eta > H'(\delta)$, then our expectation is smaller than one. So the probability that $S_\delta \cap I_p \neq \emptyset$ is

$$\mathbb{P}(S_\delta \cap I_p \neq \emptyset) \leq 2^{p(H'(\delta)-(1-\eta))+o(1)} < 1.$$

Now we consider the events $\{E_p\}_{p \in P}$ such that $\mathbb{P}(E_p) = \mathbb{P}(S_\delta \cap I_p \neq \emptyset)$ and P is the set of primes that satisfy Lemma 4.5 for η.

Hence

$$\sum_{p \in P} \mathbb{P}(E_p) \leq \sum_{p \in P} 2^{p(H'(\delta)-(1-\eta))+o(1)} \leq \sum_{n \in \mathbb{N}_{\geq 1}} 2^{n(H'(\delta)-(1-\eta))+o(1)} < \infty.$$

So, by the Borel-Cantelli lemma, if we select ideals I_p of $dim(I_p) \sim \eta p$ for all primes where it's possible (an infinite set by Lemma 4.5), we may expect that $\mathbb{P}(E_p) = \mathbb{P}(S_\delta \cap I_p \neq \emptyset) = 1$ for finitely

many $p \in P$. Also, since $H'(\delta) \to 0$ as $\delta \to 0$, we can always find a δ such that $1 - \eta > H'(\delta)$ for a fixed η. Moreover, the number of ideals I_p grows exponentially with $s = p/ord_p(2)$, so we only need to find one ideal that doesn't intersect S_δ to obtain our good cyclic code with information rate η.

Conclusion: The previous argument gives us an infinite set of primes P' such that for $p \in P'$, we have $\dim(I_p)/p \approx \eta$, and, for every non-zero element $h \in I_p$, we have $wt(h) > \delta p$. So $wt(h)/p > \delta$ since $S_\delta \cap I_p = \emptyset$. So the $[p, \eta p, \delta p]$-code over $\mathbb{F}_2$ for $p \in P'$ is a good family of cyclic codes.
Hence, we get heuristically the existence of good cyclic codes over $\mathbb{F}_2$.

Bibliography

[Berman, 1970] Berman, S. D. (1970). Semisimple cyclic and abelian codes. ii. *Cybernetics*, 3(3):17–23.

[Borello and Solé, 2021] Borello, M. and Solé, P. (2021). The uncertainty principle over finite fields. https://arxiv.org/pdf/2007.04159.pdf.

[Evra et al., 2018] Evra, S., Kowalski, E., and Lubotzky, A. (2018). Good cyclic codes and the uncertainty principle. *L'Enseignement Mathématique*, 63(3):305–332.

[Hooley, 1967] Hooley, C. (1967). On Artin's conjecture. *J. Reine Angew. Math*, 1967(225):209–220.

[Kelbert, 2013] Kelbert, M. M. (2013 - 2013). *Information theory and coding by example*. Cambridge University Press, Cambridge, England ;.

[Lin and Weldon, 1967] Lin, S. and Weldon, E. (1967). Long BCH codes are bad. *Information and Control*, 11(4):445–451.

[Lint, 1992] Lint, J. v. (1992). *Introduction to Coding Theory*. Graduate Texts in Mathematics, 86. Springer Berlin Heidelberg, Berlin, Heidelberg, 2nd ed. 1992. edition.

[Meshulam, 2006] Meshulam, R. (2006). An uncertainty inequality for finite abelian groups. *European Journal of Combinatorics*, 27(1):63–67.

[Mohamed et al., 2016] Mohamed, M. H., Puchinger, S., and Bossert, M. (2016). Guruswami-Sudan List Decoding for Complex Reed-Solomon Codes. *CoRR*, abs/1611.07811.

[Roth, 2006] Roth, R. (2006). *Introduction to Coding Theory*. Cambridge University Press.

[Tao, 2005] Tao, T. (2005). An uncertainty principle for cyclic groups of prime order. *Mathematical Research Letters*, 12(1):121–127.

[Terras, 1999] Terras, A. (1999). *Fourier Analysis on Finite Groups and Applications*. London Mathematical Society student texts. Cambridge University Press, Cambridge.