Chapter 1

Search for Good Linear Codes in the Class of Quasi-Cyclic and Related Codes

Nuh Aydin and Tsvetan Asamov
Department of Mathematics, Kenyon College
Gambier, OH, USA 43022
{*aydinn,asamovt*}*@kenyon.edu*

This chapter gives an introduction to algebraic coding theory and a survey of constructions of some of the well known classes of algebraic block codes such as cyclic codes, BCH codes, Reed-Solomon codes, Hamming codes, quadratic residue codes, and quasi-cyclic (QC) codes. It then describes some recent generalizations of QC codes and open problems related to them. Also discussed in this chapter are elementary bounds on the parameters of a linear code, the main problem of algebraic coding theory, and some algebraic and combinatorial methods of obtaining new codes from existing codes. It also includes a section on codes over $\mathbb{Z}_4$, integers modulo 4, due to increased attention given to these codes recently. Moreover, a recently created database of best known codes over $\mathbb{Z}_4$ is introduced.

Keywords: Code constructions, bounds on codes, cyclic codes, quasi-cyclic codes, quaternary codes, best known codes, database of codes.

1.1. Introduction and Basic Definitions

Coding theory is concerned with reliability of communication over noisy channels. Error correcting codes are used in a wide range of communication systems from deep space communication, to quality of sound in compact disks and wireless phones.

The basic principle of coding theory is to employ redundancy to recover original messages even if errors occur during the transmission. Redundancy is naturally used in human languages. It is built into natural languages in many ways.[67] One of the ways the redundancy is manifest in human languages is the fact that not every possible string of symbols is a valid word in a language. Humans as well as computers can use this fact to detect and even correct the errors in communication. For example, suppose you see the word "mistaky" in a text. An error can be detected and corrected even in the absence of surrounding context using the maximum like-

lihood principle: Among the valid words in the language, "mistake" is the closest one to the received string.

Using the same basic principles, we can formulate the basic notions of coding theory in a mathematical way.

Definition 1.1. A code C of length n over an alphabet F is a subset of $F^n = \{(a_1, a_2, \ldots, a_n) : a_i \in F, 1 \leq i \leq n\}$.

Notice the analogy with the set of valid words in a language. Codewords in F^n can be likened to valid words in the language. Not every possible string of symbols is a valid word in a language, likewise not every vector in F^n is a codeword (except for the trivial and quite useless code of $C = F^n$). Throughout this chapter, vectors will be represented by bold face letters such as $\mathbf{u} \in F^n$.

The alphabet F of a code is a finite set, the most important case being a finite field. In this case, we often consider subsets of F^n that are vector subspaces. Such codes are called *linear codes*.

Example 1.1. Let $C_1 = \{u_1 = 1200, u_2 = 0102\}$ and $C_2 = \{v_1 = 00000, v_2 = 10110, v_3 = 11001, v_4 = 01111\}$. Then C_1 is a ternary code of length 4 and C_2 is a binary code of length 5. It can easily be verified that C_1 is not a linear code, whereas C_2 is. The dimension of C_2 is 2. These two specific codes will be referred to a few times in this section.

A fundamental concept in coding theory is distance.

Definition 1.2. For two vectors $\mathbf{u} = (u_1, u_2, \ldots, u_n), \mathbf{v} = (v_1, v_2, \ldots, v_n)$ in F^n the Hamming distance between them is denoted and defined by $d(\mathbf{u}, \mathbf{v}) = |\{i : u_i \neq v_i\}|$, the number of positions in which $\mathbf{u}$ and $\mathbf{v}$ differ. (For a set A, $|A|$ denotes the number of elements in A). For a code C, we define the minimum distance of C to be $\min\{d(\mathbf{u}, \mathbf{v}) : \mathbf{u}, \mathbf{v} \in C, \mathbf{u} \neq \mathbf{v}\}$.

Example 1.2. For the codes C_1 and C_2 defined above, we have $d(u_1, u_2) = 3$ and $d(v_1, v_2) = 4$. The minimum distance of both C_1 and C_2 is 3.

Exercise 1.1.1. Show that the Hamming distance defines a metric on F^n, i.e., for all $\mathbf{u}, \mathbf{v}, \mathbf{w} \in F^n$ it satisfies the following properties: i) $d(\mathbf{u}, \mathbf{v}) \geq 0$, ii) $d(\mathbf{u}, \mathbf{v}) = 0 \Leftrightarrow \mathbf{u} = \mathbf{v}$, iii) $d(\mathbf{u}, \mathbf{v}) = d(\mathbf{v}, \mathbf{u})$, iv) $d(\mathbf{u}, \mathbf{v}) \leq d(\mathbf{u}, \mathbf{w}) + d(\mathbf{w}, \mathbf{v})$.

The minimum distance of a code determines its error-detecting and correcting capabilities. We like to have codes with large minimum distances so that few changes will not turn a codeword into another. At the same time, we want a code to contain as many codewords as possible so that we can transmit many different messages. Not surprisingly, these are two conflicting goals. There are trade offs between the two objectives. This is one of the main problems in coding theory. We will address this question more carefully later in this chapter.

Definition 1.3. We say that a code C is e-error detecting, if $\mathbf{v} \in F^n$ is such that $d(\mathbf{v}, \mathbf{u}) \leq e$ for some $\mathbf{u} \in C$ then either $\mathbf{v} = \mathbf{u}$ or $\mathbf{v} \notin C$.

Intuitively, this means that a set of at most e changes on a codeword does not produce another codeword. In the example above, the single change in the word "mistake" did not lead to another valid word. Is this true for every word in English language, i.e., is the English language single error detecting? For the codes C_1 or C_2, if you take any codeword and if you introduce two errors (i.e., if you change two coordinates) you do not end up with another codeword.

Definition 1.4. We say that a code C is e-error correcting, if for all $\mathbf{v} \in F^n$ such that $d(\mathbf{v}, \mathbf{u_1}) \leq e$ and $d(\mathbf{v}, \mathbf{u_2}) \leq e$ for some $\mathbf{u_1}, \mathbf{u_2} \in C$ we have $\mathbf{u_1} = \mathbf{u_2}$.

This means that a vector in F^n cannot be within a Hamming distance e of more than one codeword. Try to verify that both C_1 and C_2 are 1-error correcting codes by taking arbitrary vectors (of appropriate length over the relevant alphabet) and checking this property.

Now we can state the precise relationship between the minimum distance of a code and its error detecting and correcting capability.

Theorem 1.1. *Let C be a code with minimum distance d. Then C is a $t = d - 1$ error-detecting code and $e = \lfloor \frac{d-1}{2} \rfloor$ error correcting code, where $\lfloor x \rfloor$ denotes the greatest integer $\leq x$.*

Exercise 1.1.2. Prove this theorem using the properties of the Hamming distance.

Determining the minimum distance of a code is an important and in general a difficult problem in coding theory. For a code of size M, there are $\binom{M}{2} = \frac{M(M-1)}{2} = O(M^2)$ distinct pairs to consider to find the minimum distance. For linear codes, we get an improvement. We first need to introduce the concept of Hamming weight.

Definition 1.5. For a vector $\mathbf{u} \in F^n$, the Hamming weight $w_H(\mathbf{u})$ of $\mathbf{u}$ is defined to be $|\{i : u_i \neq 0\}|$, the number of non-zero components of $\mathbf{u}$. For a code $C \subseteq F^n$, the minimum Hamming weight of C is $\min\{w_H(\mathbf{u}) : \mathbf{u} \in C, \mathbf{u} \neq \mathbf{0}\}$.

For the code C_1 both codewords have weight 2, for C_2 the weights are 0,3,3,4. Note that the Hamming distance and the Hamming weight are related by $d(\mathbf{u}, \mathbf{v}) = w_H(\mathbf{u} - \mathbf{v})$ if the alphabet is an additive group. For linear codes, the minimum distance is the same as the minimum weight.

Lemma 1.1. *Let C be a linear code. Then the minimum distance of C is equal to the minimum weight of C.*

Exercise 1.1.3. Show that the minimum distance of C_2 is the same as the minimum weight of C_2, but that is not the case for C_1. Then, prove this lemma.

Therefore, to compute the minimum distance of a linear code of size M, in the worst case one needs to consider $M - 1 = O(M)$ vectors, instead of $O(M^2)$ vectors.

We also note that the dimension of a linear code determines its size.

Exercise 1.1.4. Let C be a linear code of dimension k over a finite field of order q. Show that $|C| = q^k$.

For a linear code, the most important parameters are the length, the dimension and the minimum distance. If a linear code C over $\mathbb{F}_q$, the finite field with q elements, has the values n, k and d for the length, the dimension and the minimum distance respectively, it is referred to as an $[n, k, d]_q$-code. In the case of a non-linear code, we use the notation $(n, M, d)_q$ where M is the size of the code. So, we say that C_1 is a $(4, 2, 3)_3$-code and C_2 is a $[5, 2, 3]_2$-code.

Let C be an $[n, k, d]_q$ linear code. Since C is a vector subspace of $\mathbb{F}_q^n$, every basis of C has k elements. A $k' \times n$, $(k' \geq k)$, matrix G whose row space is equal to C is called a *generator matrix* for C. A generator matrix of the form $G = (I_k|A)$, where I_k denotes the $k \times k$ identity matrix, is said to be in the standard form. For the code C_2 a generator matrix is $G_2 = \begin{pmatrix} 1\,0\,1\,1\,0 \\ 1\,1\,0\,0\,1 \end{pmatrix}$. After some elementary row operations it can be put into the standard form: $G_2 = \begin{pmatrix} 1\,0\,1\,1\,0 \\ 0\,1\,1\,1\,1 \end{pmatrix}$.

The inner product of two codewords $\mathbf{u}$ and $\mathbf{v}$ in $V := \mathbb{F}_q^n$ is defined in the usual

way

$$\langle \mathbf{u}, \mathbf{v} \rangle := \sum_{i=1}^{n} v_i u_i.$$

The *dual* or *orthogonal code* $C^{\perp}$ of an $[n,k]_q$ linear code C is defined by

$$C^{\perp} := \{\mathbf{v} \in V \ : \langle \mathbf{u}, \mathbf{v} \rangle = 0 \text{ for all } \mathbf{u} \in C\}.$$

It is easily verified that $C^{\perp}$ is a vector space of V of dimension $n-k$, i.e., an $[n, n-k]_q$ code. Let C be an $[n,k,d]_q$ code and let $G = (I_k|A)$ be a generator matrix of C. Let $H = (-A^T|I_{n-k})$, where superscript T stands for the transpose, then

$$GH^T = (I_k|A)\begin{pmatrix} -A \\ I_{n-k} \end{pmatrix} = -A + A = 0.$$

Thus, the rows of H are orthogonal to the rows of G, and since $rank(H) = n-k$, H is a generator matrix for $C^{\perp}$. The matrix H is a *parity check matrix* for C. More generally, a parity check matrix for a linear code C is a matrix whose row space is $C^{\perp}$, equivalently, a matrix whose null space is C. A linear code C is determined by either a generator matrix or a parity check matrix. For C_2, a parity check matrix is $H_2 = \begin{pmatrix} 1\,1\,1\,0\,0 \\ 1\,1\,0\,1\,0 \\ 0\,1\,0\,0\,1 \end{pmatrix}$. The parity check matrix of a linear code has the following important property:

Lemma 1.2. *Let C be a code with a parity check matrix H such that any set of $d-1$ columns of H is linearly independent and there is a set of d columns of H that is linearly dependent. Then, the minimum distance of C is d.*

Exercise 1.1.5. Prove this lemma and use it to verify that the minimum distance of C_2 is 3.

The *Hamming weight enumerator*, $W_C^H(x,y)$, of a linear code C of length n is defined as

$$W_C^H(x,y) = \sum_{\boldsymbol{u} \in C} x^{n-w(\boldsymbol{u})} y^{w(\boldsymbol{u})} = \sum_{i=0}^{n} A_i x^{n-i} y^i$$

where $A_i = |\{\mathbf{u} \in C : w(\mathbf{u}) = i\}|$, the number of codewords in C with weight equal to i. The weight enumerator of the code C_2 is $W = x^5 + 2x^2y^3 + xy^4$.

One of the classical theorems of coding theory is MacWilliam's identity which relates the weight enumerators of a code and its dual.

Theorem 1.2. [53] *The relationship between the Hamming weight enumerators of a q-ary linear code C and its dual $C^\perp$ is given by*

$$W^H_{C^\perp}(x,y) = \frac{1}{|C|} W^H_C(x+(q-1)y, x-y).$$

Definition 1.6. The map that sends $W^H_C(x,y)$ to $\frac{1}{|C|}W^H_C(x+(q-1)y,x-y)$ is called the *MacWilliams transform.*

The MacWilliams transform of the weight enumerator W of C_2 is $x^5+2x^3y^2+4x^2y^3+xy^4$. Therefore, the minimum distance of $C_2^\perp$ is 2 and it is a $[5,3,2]_2$-code. Note that the sum of the coefficients of the weight enumerator is the total number of codewords.

Definition 1.7. A linear code C is called *self-orthogonal* if $C \subseteq C^\perp$ and *self-dual* if $C = C^\perp$. A code C (not necessarily linear) is called *formally self-dual* if its Hamming weight enumerator coincides with its MacWilliams transform.

It is clear that a self-dual code is also formally self-dual. Another important notion in coding theory is equivalence of codes.

Definition 1.8.[53] Let C_1 and C_2 be codes of length n over $\mathbb{F}_q$. We say that C_1 and C_2 are *equivalent* if there are n permutations $\pi_0, \pi_1, \ldots, \pi_{n-1}$ of $\mathbb{F}_q$ and a permutation σ of n coordinate positions such that

$$\text{If} \quad (c_0,\ldots,c_{n-1}) \in C_1 \quad \text{then} \quad \sigma\big(\pi_0(c_0),\ldots,\pi_{n-1}(c_{n-1})\big) \in C_2.$$

For linear codes only those π_i's which are the compositions of a scalar multiplication with a field automorphism are allowed. The scalar multiple may vary for each coordinate, but the field automorphism must be the same.

There are some important special cases: when all π_i's are identity permutations, we say that C_1 and C_2 are *permutation equivalent* and when each π_i is a multiplication by a non-zero scalar, C_1 and C_2 are said to be *scalar multiple equivalent* or *monomially equivalent*. For prime fields such as $\mathbb{Z}_p$, integers modulo a prime p (also denoted by $\mathbb{F}_p$ or $GF(p)$), there are no non-trivial field automorphisms. Equivalent (linear) codes have the same weight enumerator, in particular they have the same minimum distance.

1.1.1. *Main Problem of Coding Theory*

One of the central problems of algebraic coding theory is to determine the best possible values of the parameters of a code, and to explicitly construct codes with those parameters. There is an online table[33] of best known linear codes over the finite fields of size ≤ 9. Additionally, there is a table of best known (non-linear) binary codes.[50]

To formulate the main problem for linear codes, we can first choose the alphabet size q, then fix two of the parameters and ask for the optimal value of the other. For example, fixing n and k, we ask for the largest value of d. This value is denoted by $d_q(n,k)$. Similarly, we can fix n and d, and try to maximize k, or the size of the code. The maximum size of such a code is denoted by $A_q(n,d)$. Or, fix k and d, and try to minimize n. This minimum value is denoted by $n_q(k,d)$. There are numerous bounds on the parameters of a code. We review some of the most elementary bounds in the next section. Others can be found in standard books in coding theory such as.[53] The problem of determining the values $n_q(k,d)$ (or $d_q(n,k)$) have been a central problem in coding theory. Many papers in the literature deal with this problem. In general, the optimal values are not determined except for small values of k, or when $n-k$ is small. A printed (but not up to date) table is available in[17] with online and up to date version at.[33] Among others, some of the cases where the problem is solved are $n_2(k,d), k \leq 8$ in,[14] $d_3(n,k), k \leq 6$ (not all cases determined) in,[15] $n_4(5,d)$ for many cases in,[16] some cases of $n_2(9,d)$ in,[27] and many cases of $n_5(k,d)$ for $k = 3,4$ in.[13,44] A survey on the subject can be found in.[41]

There are various algebraic methods to construct codes with good parameters. In the following sections we will describe some of these methods. We first review some necessary abstract algebra in section 3, then introduce some of the well-known constructions in section 4. There are also many ways to combine existing codes to produce new codes. Some of these methods are described in the next section. In section 5, we pay special attention to the class of quasi-cyclic and related codes which have proven to be promising towards a solution to the main problem of the coding theory. Section 6 focuses on the computationally difficult problem of determining the minimum distance of a code. We devote a section (section 7) to the codes over $\mathbb{Z}_4$, the integers modulo 4 due to increased attention to those codes in recent years. The section also introduces a recently created database of best known codes over $\mathbb{Z}_4$. We list some open problems in the area of quasi-cyclic and

related codes in section 8.

1.2. Some Elementary Constructions and Elementary Bounds on Codes

1.2.1. *Some Elementary Constructions*

Extending a Code

Given a code C, there are many ways of obtaining longer codes by adding coordinates to C. The most common way to extend a linear code is by adding an overall parity check. If C is an $[n, k, d]_q$-code, the extended code $\hat{C}$ is defined by

$$\hat{C} = \{(c_0, c_1, \ldots, c_{n-1}, c_n) : (c_0, c_1, \ldots, c_{n-1}) \in C, \sum_{k=0}^{n} c_k = 0\}$$

and it is an $[n+1, k, \hat{d}]$-code where $\hat{d} = d$ or $d+1$.

Puncturing a Code

Puncturing a code is opposite of extending where one fixed coordinate position is deleted from all codewords. If C is an $(n, M, d)_q$-code with $d \geq 2$, then the code C^* obtained by puncturing C once has parameters $(n-1, M, \quad d^*)$ where $d^* = d$ or $d-1$. If C is a linear code with parameters $[n, k, d]_q$ then C^* has parameters $[n-1, k, d^*]_q$, $d^* = d$ or $d-1$.

Shortening a Code

Let C be an $[n, k, d]_q$-code. Fix a position i and let C_i be the set of all codewords that have 0 at position i. Then C_i is a subcode of C. If we delete the coordinate i from the set of vectors in C_i then the resulting code is called a shortened code of C. The parameters of the shortened code are $[n-1, k-1, d]_q$.

Direct Sum

Given two linear codes C_1, C_2 over F_q with parameters $[n_i, k_i, d_i]$, $i = 1, 2$, then their direct sum is the code given by $C_1 \oplus C_2 = \{(\mathbf{u}, \mathbf{v}) : \mathbf{u} \in C_1, \mathbf{v} \in C_2\}$, $((\mathbf{u}, \mathbf{v})$ denotes the concatenation of the vectors $\mathbf{u}$ and $\mathbf{v})$. Then the parameters of the direct sum code are $[n_1 + n_2, k_1 + k_2, \min\{d_1, d_2\}]$. Moreover, if G_i and H_i are generator and parity check matrices of C_i respectively, then a generator matrix of $C_1 \oplus C_2$ is $\begin{pmatrix} G_1 & 0 \\ 0 & G_2 \end{pmatrix}$ and a parity check matrix is $\begin{pmatrix} H_1 & 0 \\ 0 & H_2 \end{pmatrix}$.

The $(\mathbf{u}|\mathbf{u}+\mathbf{v})$ *construction)*

Another way to combine two linear codes C_1, C_2 of the same length over the same field $\mathbb{F}_q$ to obtain a new code of double length is through the $(\mathbf{u}|\mathbf{u}+\mathbf{v})$ construction which is defined as $C_3 = \{(\mathbf{u}, \mathbf{u}+\mathbf{v}) : \mathbf{u} \in C_1, \mathbf{v} \in C_2\}$. It is not hard to show that the parameters of C_3 are $[2n, k_1+k_2, \min\{2d_1, d_2\}]$, where the parameters of C_i are $[n, k_i, d_i]$. It is also not difficult to show that the generator and parity check matrices of C_3 are $\begin{pmatrix} G_1 & G_1 \\ 0 & G_2 \end{pmatrix}$ and $\begin{pmatrix} H_1 & 0 \\ -H_2 & H_2 \end{pmatrix}$ respectively.

The $(\mathbf{u}|\mathbf{u}+\mathbf{av}|\mathbf{u}+\mathbf{v}+\mathbf{w})$ *construction)*

Given three codes $C_1[n_1, k_1, d_1]$, $C_2[n_2, k_2, d_2], C_3[n_3, k_3, d_3]$ over the same field $\mathbb{F}_q$, and $a \in \mathbb{F}_q$ we can generate a new code of the form $C_4 = \{(\mathbf{u}, \mathbf{u}+\mathbf{av}, \mathbf{u}+\mathbf{v}+\mathbf{w}) : \mathbf{u} \in C_1, \mathbf{v} \in C_2, \mathbf{w} \in C_3\}$. When $a = -1$, the parameters of C_4 are $[n + \max\{n_1, n_2\} + \max\{n_1, n_2, n_3\}, k_1 + k_2 + k_3, \min\{3d_1, 2d_2, d_3\}]$. Moreover, C_4 has a generator matrix of the form $\begin{pmatrix} G_1 & G_1 & G_1 \\ 0 & aG_2 & G_2 \\ 0 & 0 & G_3 \end{pmatrix}$.

Construction X

Once again, consider three codes $C_1[n_1, k_1, d_1]$, $C_2[n_2, k_2, d_2]$, $C_3[n_3, k_3, d_3]$ over a field $\mathbb{F}_q$. If $k_1 = k_2 + k_3$ and C_2 is a subcode of C_1, implying $n_1 = n_2$ and $k_1 \geq k_2$, then we can split C_2 into a union of cosets of C_1 and append a different word from C_3 to each of the cosets. Thus we end up with a code with parameters $[n_1 + n_3, k_1, d \geq \min\{d_2, d_1 + d_3\}]$ and a generator matrix given by $\begin{pmatrix} G_{12} & G_3 \\ G_2 & 0 \end{pmatrix}$. Here G_2 and G_3 are the generator matrices of respectively C_2 and C_3, while G_{12} is such that G_{12} and G_2 together generate C_1.

1.2.2. *Some Bounds on Codes*

There are many bounds on the parameters of a code. Here, we give two most elementary bounds: the singleton bound that is related to MDS codes and the sphere packing bound that is related to perfect codes. More bounds can be found in books on the subject such as.[9,42,53,64,74]

Theorem 1.3. *(The Singleton Bound)* $A_q(n, d) \leq q^{n-d+1}$

Proof. Let C be a q-ary (n, M, d)-code. If we remove the last (or any) $d-1$ coordinate positions from each codeword in C, the resulting M words are still

distinct. Since those have length $n-d+1$, we have $M \leq q^{n-d+1}$ □

The Singleton bound implies that any $[n,k,d]_q$ code must satisfy $q^k \leq q^{n-d+1}$ or equivalently $d \leq n-k+1$. A linear code for which the equality holds in this bound is called a *maximum distance separable code*, or *MDS code*. It is known that the dual of an MDS code is also MDS. So is a shortening. MDS codes are known to exist for small lengths. In fact for any prime power q and any dimension k, $1 \leq k \leq q+1$, there exists a $[q+1,k,q-k+1]_q$ MDS code (hence for any smaller length). It is conjectured that no longer non-trivial MDS codes exist except for $n = q+2$ for q even and $k=3$ or $k=q-1$.[53] The conjecture has been proven in some cases, but the general case is still open. See[77] as an example of a case for which the conjecture is proven.

Theorem 1.4. *(The Sphere Packing Bound or the Hamming Bound)*

$$A_q(n,d) \leq \frac{q^n}{\sum_{j=0}^{t}\binom{n}{j}(q-1)^j}, \text{ where } \quad t = \lfloor \frac{d-1}{2} \rfloor.$$

The proof of this bound is based on the observation that the "spheres" of radius t around codewords are disjoint.

An $(n,M,2t+1)_q$-code C is said to be *perfect* (or *t-perfect*) if the balls $B_t(\mathbf{c}) = \{\mathbf{x} \in F^n : d(\mathbf{x},\mathbf{c}) \leq t\}$ of radius t around codewords are disjoint and cover the space F^n (here F is the alphabet of size q for the code, it is not necessarily a field), i.e.,

$$\bigcup_{\mathbf{c}\in C} B_t(\mathbf{c}) = F^n.$$

For perfect codes the equality holds in the sphere packing bound. Perfect codes are rather rare. There has been intensive search to classify all perfect codes or to discover new ones. After much effort, the classification of all perfect codes is nearly complete. The result on the classification of all perfect codes can be found in[42] (page 49) or with more details in[74] (Chapter 7).

1.3. Some Background in Abstract Algebra

In algebraic coding theory finite fields and polynomials over finite fields are very important. In this section, we review some of the basic facts about these objects. Due to space considerations, we skip background information on such topics as rings, ideals, and Euclidean domains. For more details, the reader is referred to the books such as.[30,48,64,65] Most of the definitions, theorems, and examples in

this section (and its sub-sections) can be found in[48,64] as well as the proofs of the theorems.

1.3.1. *Polynomials*

A fundamental theorem about polynomials over fields is the following theorem known as the *division algorithm*.

Theorem 1.5. *The polynomial ring $F[x]$ over a field F is a Euclidean domain with $\sigma(p(x)) = \deg(p(x))$, with the well known division algorithm of polynomials: Given $f, g \in F[x]$ with $g \neq 0$, there exist unique polynomials $q, r \in F[x]$ such that $f = q \cdot g + r$, where $r = 0$ or $\deg(r) < deg(g)$. Thus $F[x]$ is a principal ideal domain, and hence a unique factorization domain.*

Example 1.3. Let $f(x) = 3x^4 + x^3 + 2x^2 + 1 \in \mathbb{Z}_5[x], g(x) = x^2 + 4x + 2 \in \mathbb{Z}_5[x]$. Then $f = q \cdot g + r$ with $q(x) = 3x^2 + 4x, r(x) = 2x + 1$ and $\deg(r) < \deg(g)$.

Definition 1.9. Given two polynomials $f, g \in F[x]$, $g \neq 0$ we say that g *divides* f (also denoted by $g|f$) if there exists a polynomial $p \in F[x]$ such that $f = p \cdot g$. This is equivalent to saying that the remainder in the division algorithm is 0 when f is divided by g.

Definition 1.10. A non-zero, non-constant polynomial $f \in F[x]$ is said to be *irreducible* over F if whenever $f = p \cdot q$ for some polynomials $p, q \in F[x]$ then either p or q is a constant polynomial.

Irreducible polynomials are very important in finite field theory.

Definition 1.11. A polynomial d is called a *greatest common divisor* of polynomials f and g if
i) $d|f$ and $d|g$
ii) whenever $p|f$ and $p|g$, $p|d$ as well

A greatest common divisor is unique up to a constant multiple. If f, g are either integers or polynomials, the notation (f, g) is commonly used to denote their greatest common divisor. Thus the notation $(f, g) = 1$ means f and g are relatively prime, where f and g could be either integers or polynomials.

An element $a \in F$ is called a *root* (or a *zero*) of a polynomial $f \in F[x]$ if $f(a) = 0$. It is well known (follows from Theorem 1.5) that an element $a \in F$ is a root of a

polynomial $f \in F[x]$ if and only if $(x-a)|f(x)$. For polynomials of degree 2 or 3 existence of roots is equivalent to reducibility. This result again follows from the division algorithm.

Lemma 1.3. *A polynomial of degree 2 or 3 over a field F is irreducible in $F[x]$ if and only if it has no roots in F.*

Exercise 1.3.1. Prove this lemma, and give an example to show that it is not true for polynomials of higher degrees.

If $(x-a)^k|f(x)$ for $k > 1$ then a is called a *multiple root* of f. The largest integer r such that $(x-a)^r|f(x)$ but $(x-a)^{r+1} \not| f(x)$ is called the multiplicity of a. If $r = 1$ then a is called a *simple root*. The notion of *derivative*, defined purely algebraically, is useful for determining multiplicity of roots. The derivative of a polynomial $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in F[x]$ is defined by $f'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1} \in F[x]$. Then, it is not difficult to show that the usual laws of derivatives hold in polynomial rings. We can also use derivatives to detect multiple roots.

Proposition 1.1. *An element $a \in F$ is a multiple root of $f(x) \in F[x]$ if and only if it is a root of both $f(x)$ and $f'(x)$.*

1.3.2. *Field Extensions*

In working with polynomials over fields, we often need to consider larger fields to find the roots. Therefore, a discussion of field extensions is needed. If a field F contains a subset K that happens to be a field by itself with the induced operations, then K is called a *subfield* of F, and F is called an *extension* (*field*) of K. If $K \neq F$, then K is a *proper subfield* of F.

If K is a subfield of a finite field $\mathbb{F}_p$ with p elements where p is a prime, then K must contain 0 and 1 and, by closure under addition, all the other elements of $\mathbb{F}_p$. Therefore, $K = \mathbb{F}_p$ and $\mathbb{F}_p$ contains no proper subfields. A field containing no proper subfields is called a *prime field*. Any finite field of order p, p prime, is a prime field. Another example of a prime field is the field $\mathbb{Q}$ of rational numbers, which has characteristic 0. It turns out that these are the only prime fields. Any field F contains a prime field that is isomorphic to either $\mathbb{F}_p$ or $\mathbb{Q}$ depending on whether the characteristic of F is a prime p or 0.

A common way of obtaining extension fields is by *adjoining* a set of elements S to a given field K from a larger field F that contains K. The smallest field that contains both K and S is denoted by $K(S)$. For a finite set $S = \{\alpha_1, \ldots, \alpha_n\}$ the notation $K(\alpha_1, \ldots, \alpha_n)$ is common. If $S = \{\alpha\}$ is a singleton set then $E = K(\alpha)$ is called a *simple extension* of K and α is called a *generating element* of E over K.

Elements of a larger field that are roots of (non-zero) polynomials over subfields have a special place in field theory. For fields $K \subseteq F$ and $\alpha \in F$, if there exist $a_i \in K$, $0 \leq i \leq n$, not all equal to 0, such that $a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$ then α is said to be *algebraic* over K. For example, $\sqrt{2} \in \mathbb{R}$ is algebraic over $\mathbb{Q}$ but π is not. An extension E of K is called algebraic over K (or an *algebraic extension* of K) if every element of E is algebraic over K.

The set $I = \{f \in K[x] : f(\alpha) = 0\}$ of polynomials that has an algebraic element $\alpha \in K \subseteq F$ as root forms an ideal in $K[x]$. Since $K[x]$ is a principal ideal domain, there is a unique monic polynomial $g \in K[x]$ such that $I = \langle g \rangle$, ideal generated by g. This polynomial g is irreducible and it is called the *minimal polynomial* of α over K. The *degree* of α is defined as the degree of g. The minimal polynomial has the property that for any polynomial f over K, $f(\alpha) = 0$ if and only if $g|f$.

It is sometimes useful to regard an extension field F as a vector space over its subfield K. If F, considered as a vector space over K, is finite dimensional, then F is called a *finite extension* of K. The dimension of F over K is called the *degree* of F over K, and is denoted by $[F : K]$.

The following are some of the standard results for extension fields.

Lemma 1.4. *If F is a finite extension of K and E is a finite extension of F, then E is a finite extension of K and $[E : K] = [E : F][F : K]$.*

Lemma 1.5. *Every finite extension is an algebraic extension.*

Lemma 1.6. *Let $\alpha \in F$ be algebraic of degree n over K and let p be the minimal polynomial of α over K. Then:*

(1) $K(\alpha)$ is isomorphic to $K[x]/\langle p \rangle$.
(2) $[K(\alpha) : K] = n = \deg p(x)$ and $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a basis of $K(\alpha)$ over K.
(3) Every $\beta \in K(\alpha)$ is algebraic over K and its degree over K is a divisor of n.

Lemma 1.7. *Let α, β be two roots of an irreducible polynomial f over K. Then $K(\alpha)$ and $K(\beta)$ are isomorphic by an isomorphism that maps α to β and keeps the*

elements of K fixed.

Given a polynomial f over a field K, it is often the case that K does not contain all (or any of) the roots of f and we need to consider extension fields of K. The smallest field F that contains all the roots of f is called the *splitting field* of f over K. In $F[x]$ f can be written as a product of linear factors, that is, there exist elements $\alpha_1, \alpha_2, \ldots, \alpha_n \in F$ such that $f(x) = a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$ where $a \in K$ is the leading coefficient of f. It is also true that $F = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$. It is well-known that splitting fields exist and they are unique (up to isomorphism). The splitting field of a polynomial f over a field K is a finite, therefore algebraic, extension of F since it is obtained from K by adjoining finitely many elements.

1.3.3. *Structure of Finite Fields*

Finite fields play a central role in algebraic coding theory. For linear codes, finite fields have been traditionally used as the alphabet of a code. More recently, linear codes over rings have also gained considerable interest. In this section we give a description of the basic properties of finite fields.

The field $\mathbb{Z}_p$, the integers modulo p for a prime p, is the most familiar example of a finite field, but there are many other finite fields as well. The fields $\mathbb{Z}_p$ play an important role in general field theory since every field of characteristic p must contain an isomorphic copy of $\mathbb{Z}_p$. The most fundamental properties of finite fields are given by the following theorems.

Theorem 1.6. *Let F be a finite field. Then F has p^n elements, where prime p is the characteristic of F and n is the degree of F over its prime subfield $\mathbb{Z}_p$.*

Lemma 1.8. *In a finite field F with $q = p^n$ elements every $a \in F$ satisfies $a^q = a$. Therefore, the polynomial $x^q - x$ factors in $F[x]$ as*

$$x^q - x = \prod_{a \in F} (x - a)$$

Consequently, F is the splitting field of $x^q - x$ over $\mathbb{Z}_p$.

Here is the main characterization of finite fields:

Theorem 1.7. *For every prime p and every positive integer n there exists a finite field with p^n elements. Any finite field with $q = p^n$ elements is isomorphic to the splitting field of $x^q - x$ over $\mathbb{Z}_p$.*

This theorem provides a justification for speaking of *the* finite field (or *the* Galois field) with q elements, or *the* finite field of order q. We shall denote this field by $\mathbb{F}_q$ or GF(q). In particular, for a prime p the notations $\mathbb{F}_p$ and $\mathbb{Z}_p$ are interchangeable.

The subfields of a given finite field are uniquely determined. Given a finite field $\mathbb{F}_q$, $q = p^n$ there is a unique subfield of order p^m, for each $m|n$.

For a finite field $\mathbb{F}_q$ we denote by $\mathbb{F}_q^*$ the multiplicative group of nonzero elements of $\mathbb{F}_q$. It is well known that $\mathbb{F}_q^*$ is a cyclic group. A generator of the cyclic group $\mathbb{F}_q^*$ is called a *primitive element* of $\mathbb{F}_q$. The existence of primitive elements implies that every finite field is a simple algebraic extension of its prime subfield, which in turn implies that for any positive integer n and every prime p, there exists an irreducible polynomial of degree n in $\mathbb{F}_p[x]$. Irreducible polynomials having primitive elements as their roots are given special names.

Definition 1.12. Let α be a primitive element of $\mathbb{F}_{q^n}$. The minimal polynomial of α over $\mathbb{F}_q$ is called a *primitive polynomial* for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

1.3.4. *Roots of Irreducible Polynomials*

Irreducible polynomials and their roots are important for constructing finite fields. They are also important for the construction of certain algebraic codes. In this section we summarize important facts about the set of roots of an irreducible polynomial.

Lemma 1.9. *Let $f \in \mathbb{F}_q[x]$ be an irreducible polynomial and let α be a root of f in an extension of $\mathbb{F}_q$. Then for a polynomial $h \in \mathbb{F}_q[x]$, $h(\alpha) = 0$ if and only if $f|h$.*

One of the important properties of the roots of a polynomial $p(x)$ over a finite field $\mathbb{F}_q$ is that if α is a root of p, then so is α^q. This follows from the fact that $a^q = a$ and $(a+b)^q = a^q + b^q$ in $\mathbb{F}_q$. It also follows that $\alpha, \alpha^q, \alpha^{q^2}, \ldots$ are all roots of $p(x)$. If $p(x)$ is an irreducible polynomial of degree m, then a root α of $p(x)$ lies in $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$, and $\mathbb{F}_{q^m}$ is the smallest such field. Moreover, $\{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}\}$ is the set all roots of $p(x)$. That means that the splitting field of a polynomial of degree m over $\mathbb{F}_q$ is $\mathbb{F}_{q^m}$. The elements $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}} \in \mathbb{F}_{q^m}$ are called *conjugates* of α with respect to $\mathbb{F}_q$. The conjugates of $\alpha \in \mathbb{F}_q^*$ with respect to any subfield of $\mathbb{F}_q$ have the same order in the group $\mathbb{F}_q^*$. Therefore, we can make the following definition.

Definition 1.13. The multiplicative order of any root of an irreducible polynomial $f(x) \in \mathbb{F}_q[x]$ in its splitting field is called the *order* of $f(x)$.

It follows that all the conjugates of a primitive element are also primitive. As an example, let us consider $\alpha \in \mathbb{F}_{16}$, where α is a root of the irreducible polynomial $f(x) = x^4 + x + 1$ over $\mathbb{F}_2$. The conjugates of α with respect to $\mathbb{F}_2$ are $\alpha, \alpha^2, \alpha^4 = \alpha + 1$, and $\alpha^8 = \alpha^2 + 1$, each of them being a primitive element of $\mathbb{F}_{16}$. The conjugates of α with respect to $\mathbb{F}_4$ are α and $\alpha^4 = \alpha + 1$.

On the basis of previous results, we can compute minimal polynomials as in the following lemma.

Lemma 1.10. *Let $\alpha \in \mathbb{F}_{q^m}$. Then the minimal polynomial of α over $\mathbb{F}_q$ is $m_\alpha(x) = (x-\alpha)(x-\alpha^q)\cdots(x-\alpha^{q^d-1}) \in \mathbb{F}_q[x]$ where d is the smallest positive integer such that $\alpha^{q^d} = \alpha$.*

Example 1.4. Let $p(x) = x^4+x^3+1 \in \mathbb{F}_2$. It can be verified that $p(x)$ is a primitive polynomial for $\mathbb{F}_{16}$ over $\mathbb{F}_2$. Let α be a root of $p(x)$ in $\mathbb{F}_{16}$ (hence a primitive element of $\mathbb{F}_{16}$). Let us compute the minimal polynomials of all of the elements of $\mathbb{F}_{16}$ over $\mathbb{F}_2$. Let $[\beta]$ denote the set of conjugates of $\beta \in \mathbb{F}_{16}$ with respect to $\mathbb{F}_2$. Then,

$$
\begin{aligned}
[\alpha] &= \{\alpha, \alpha^2, \alpha^4, \alpha^8\} \\
[\alpha^3] &= \{\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24} = \alpha^9\} \\
[\alpha^5] &= \{\alpha^5, \alpha^{10}\} \\
[\alpha^7] &= \{\alpha^7, \alpha^{14}, \alpha^{28} = \alpha^{13}, \alpha^{26} = \alpha^{11}\}
\end{aligned}
$$

Each conjugacy class $[\alpha^i]$ has the same minimal polynomial m_i. For example, the minimal polynomial of α^3 is $m_3(x) = (x-\alpha^3)(x-\alpha^6)(x-\alpha^9)(x-\alpha^{12}) = x^4 + x^3 + x^2 + x + 1$, and $m_3(x) = m_6(x) = m_9(x) = m_{12}(x)$. We can compute other minimal polynomials similarly and obtain

$$m_5(x) = m_{10}(x) = x^2 + x + 1, \quad m_7(x) = m_{11} = m_{13}(x) = m_{14}(x) = x^4 + x + 1$$

1.3.5. *Roots of Unity*

The polynomial $x^n - 1$ over $\mathbb{F}_q$ is very important in algebraic coding theory due to its connections with cyclic codes. In this section we review results on this polynomial, its roots, and its factorization.

First, we observe that if $(n, q) \neq 1$, then we can write $n = mp^k$ where $(m, q) = 1$ and $p = \text{char}(\mathbb{F}_q)$. Then, $x^n - 1 = x^{mp^k} - 1 = (x^m - 1)^{p^k}$. Therefore, we will always

assume that $(n, q) = 1$.

Let $\mathbb{F}_{q^m}$ be the splitting field of $x^n - 1$ over $\mathbb{F}_q$. Since $(x^n - 1)' = nx^{n-1}$ is relatively prime with $x^n - 1$, the polynomial $x^n - 1$ does not have multiple roots. Thus, $x^n - 1$ has n distinct roots in $\mathbb{F}_{q^m}$. The roots of $x^n - 1$ in $\mathbb{F}_{q^m}$ are called *n-th roots of unity over* $\mathbb{F}_q$. The set W_n of n-th roots of unity over $\mathbb{F}_q$ has a nice algebraic structure.

Lemma 1.11. *When $(n, q) = 1$, W_n is a cyclic group, a cyclic subgroup of the multiplicative group $\mathbb{F}^*_{q^m}$ for a suitable $m \in \mathbb{Z}$.*

An n-th root of unity over $\mathbb{F}_q$ of order n, that is a generator of the cyclic group W_n, is called a *primitive n-th root of unity* over $\mathbb{F}_q$. We can determine m (the smallest integer such that $\omega \in \mathbb{F}_{q^m}$) in terms of n and q. Let $\omega \in W_n$ be a primitive n-th root of unity. Since ω has order n, we have $\omega \in \mathbb{F}_{q^r} \Leftrightarrow \omega^{q^r} = \omega \Leftrightarrow \omega^{q^r-1} = 1 \Leftrightarrow n|(q^r - 1)$.
Since m is the smallest integer for which $\omega \in \mathbb{F}_{q^m}$, we have the following result.

Lemma 1.12.[64] *If $\mathbb{F}_{q^m}$ is the splitting field of $x^n - 1$ over $\mathbb{F}_q$, then m is the smallest positive integer for which $n|(q^m - 1)$, that is, m is the smallest positive integer for which $q^m \equiv 1 \mod n$. This integer m is called the* order *of $q \mod n$, which is denoted by $o_n(q)$.*

1.3.6. *Factorization of $x^n - 1$*

The factorization of the polynomial $x^n - 1$ over a finite field is very important for the study of cyclic codes. For $(n, q) = 1$, the polynomial $x^n - 1$ over $\mathbb{F}_q$ has no multiple factors and can be factored using the fact that it has n distinct roots. It is therefore the product of the distinct minimal polynomials. Let α be a primitive element of $\mathbb{F}_{q^m}$, where $m = o_n(q)$. Then we know that $\omega = \alpha^{(q^m-1)/n}$ is a primitive n-th root of unity. Therefore, the roots of $x^n - 1$ are given by $\omega, \omega^2, \ldots, \omega^{n-1}, \omega^n = 1$. We need to determine the minimal polynomials for these roots and take the product of distinct ones.

For $0 \leq i \leq n - 1$, the conjugates of ω^i are $\omega^i, \omega^{iq}, \omega^{iq^2}, \ldots, \omega^{iq^{d-1}}$ where d is the smallest positive integer such that $\omega^{iq^d} = \omega^i$. Since

$$\omega^{iq^d} = \omega^i \Leftrightarrow \omega^{iq^d-i} = 1 \Leftrightarrow n|(iq^d - i) \Leftrightarrow iq^d \equiv i \mod n,$$

the minimal polynomial for ω^i (and its conjugates) is

$$m_i(x) = (x - \omega^i)(x - \omega^{iq}) \cdots (x - \omega^{iq^{d-1}}).$$

The set of exponents of ω in the last product is called *i-th cyclotomic coset* of q modulo n. These sets can be defined independently of a primitive n-th root of unity. In fact the relation $\sim$ defined on $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ by $i \sim j$ if and only if $j \equiv iq^r \mod n$ for some integer r, is an equivalence relation and the equivalence classes are exactly the cyclotomic cosets of q modulo n. There is a one-to-one correspondence between irreducible factors of $x^n - 1$ over $\mathbb{F}_q$ and cyclotomic cosets of q modulo n; every irreducible factor of degree k corresponds to a cyclotomic coset of size k and k must divide m. We now illustrate this factorization with an example.

Example 1.5. Let $q = 2, n = 15$ and consider the polynomial $f(x) = x^{15} - 1 = x^{15} + 1$ over $\mathbb{F}_2$. Since, $m = o_{15}(2) = 4$, the splitting field of $f(x)$ over $\mathbb{F}_2$ is $\mathbb{F}_{16}$. The polynomial $p(x) = x^4 + x^3 + 1$ is primitive over $\mathbb{F}_2$. Let α be a root of $p(x)$, then it is a primitive element of $\mathbb{F}_{16}$ and happens to be a primitive 15-th root of unity. So, the roots of $x^{15} - 1$ are $1, \alpha, \alpha^2, \ldots, \alpha^{14}$. We already computed the minimal polynomials in this case. Therefore, we obtain the factorization $x^{15} - 1 = (x + 1)(x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1)(x^4 + x^3 + 1)$ over $\mathbb{F}_2$.

Exercise 1.3.2. Obtain a factorization of $x^{11} - 1$ over $\mathbb{F}_3$ using cyclotomic cosets and an irreducible polynomial of degree 5.

1.4. Some Classes of Linear Codes

In this section we will review some of the most fundamental and standard classes of algebraic codes. The material in this section can be found in most standard books on coding theory such as.[64]

1.4.1. *Cyclic Codes*

Cyclic codes are very important for both theoretical and practical purposes. Their nice structure facilitates their implementation in practice. On the other hand they establish a fundamental link between coding theory and algebra. We begin with the definition of a cyclic code.

Let $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$ be a vector in $V := \mathbb{F}_q^n$. We may associate to vector $\mathbf{v} \in V$ a polynomial in $\mathbb{F}_q[x]$ as follows:

$$\phi : \mathbf{v} = (v_0, v_1, \ldots, v_{n-1}) \to v(x) = v_0 + v_1 x + \cdots + v_{n-1} x^{n-1}.$$

The map ϕ is a vector space isomorphism from V onto the subspace $\phi(V)$ of $\mathbb{F}_q[x]$. Given this map, we can identify $\phi(V)$ with V without an explicit reference to ϕ. Hence we will think of the vectors in V as polynomials of degree $< n$.

Definition 1.14. A linear code is *cyclic* if it is invariant under *(right) cyclic shift* i.e., $(c_0, c_1, \ldots, c_{n-1}) \in C$ implies $(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$.

Viewing a codeword $\mathbf{c}$ as a polynomial $c(x)$ in a cyclic code C implies that $xc(x)$ mod $(x^n - 1) \in C$. Thus, a linear code C is cyclic if and only if C is an ideal of the factor ring

$$R_n = \frac{\mathbb{F}_q[x]}{\langle x^n - 1 \rangle}.$$

This relation links algebra to coding theory and enables us to use the algebraic structure of ideals in order to better understand the cyclic codes. From algebra, we know that $\mathbb{F}_q[x]$ is a principal ideal domain and $\mathbb{F}_q[x]/\langle f(x) \rangle$ is a principal ideal ring. Below are the most basic facts about the structure of cyclic codes.

Theorem 1.8. [64] *Let C be an ideal in R_n, i.e. a cyclic code of length n.*
1) There is a unique monic polynomial $g(x) \in R_n$ of minimum degree which generates C, i.e. $C = \langle g(x) \rangle$. This polynomial is called the generator polynomial *of C. (The generator polynomial is usually not the only polynomial that generates C. The next lemma characterizes all the polynomials that generate C.)*
2) $g(x) | x^n - 1$.
3) If $deg(g(x)) = r$, then C has dimension $n - r$. In fact,

$$C = \langle g(x) \rangle = \{ r(x)g(x) : \deg(r(x)) < n - r \}$$

4) If $g(x) = g_0 + g_1 x + \cdots + g_r x^r$, then $g_0 \neq 0$ and C has a generator matrix of the form

$$\begin{bmatrix} g_0 & g_1 & g_2 & \ldots & g_r & 0 & 0 & 0 & \ldots & 0 \\ 0 & g_0 & g_1 & g_2 & \ldots & g_r & 0 & 0 & \ldots & 0 \\ 0 & 0 & g_0 & g_1 & \ldots & & g_r & 0 & & 0 \\ \vdots & & & & & & & \ldots & & 0 \\ 0 & 0 & 0 & \ldots & 0 & g_0 & g_1 & g_2 & \ldots & g_r \end{bmatrix}$$

where each row is a right cyclic shift of the previous row.

Lemma 1.13. [53] *Let C be a cyclic code of length n with the least degree generator polynomial $g(x)$. Then,*

$$C = \langle f(x)g(x) \rangle$$

if and only if $(f(x), h(x)) = 1$, where $h(x) = (x^n - 1)/g(x)$, called the check polynomial of C.

Proof. $\Longrightarrow$: Suppose $\langle g(x) \rangle = \langle f(x)g(x) \rangle$. Then $g(x) = g(x)f(x)t(x)$ for some $t(x) \in \mathbb{F}_q[x]$. Since $(g(x), h(x)) = 1$, there are polynomials $A(x), B(x)$ in $\mathbb{F}_q[x]$ such that $A(x)g(x) + B(x)h(x) = 1$. Replacing $g(x)$ with $g(x)f(x)t(x)$, we have $(A(x)g(x)t(x)) \cdot f(x) + B(x)h(x) = 1$. Therefore, $(f(x), h(x)) = 1$.
$\Longleftarrow$: It is clear that $\langle f(x)g(x) \rangle \subseteq \langle g(x) \rangle$. Since $(f(x), h(x)) = 1$, there exist $s(x), t(x) \in \mathbb{F}_q[x]$ such that $s(x)f(x) + t(x)h(x) = 1$. Hence, $s(x)f(x)g(x) + t(x)(x^n - 1) = g(x)$. Reducing $\mod x^n - 1$ we get, $s(x)f(x)g(x) = g(x)$. Thus, $g(x) \in \langle f(x)g(x) \rangle$, and $\langle g(x) \rangle \in \langle f(x)g(x) \rangle$. □

There is an alternative way of describing cyclic codes. Every cyclic code of length n has a unique, monic generator polynomial of degree $\leq n$ that divides $x^n - 1$. Therefore, to find all the cyclic codes one needs to factor $x^n - 1$. If the factorization is $x^n - 1 = m_1(x)m_2(x) \cdots m_t(x)$, then there are a total of 2^t distinct factors of $x^n - 1$, hence 2^t cyclic codes. If α is a root of some $m_i(x)$ in some extension of $\mathbb{F}_q$, then m_i is the minimal polynomial of α over $\mathbb{F}_q$. So for any $f(x) \in \mathbb{F}_q[x]$, $f(\alpha) = 0$ if and only if $m_i(x) | f(x)$. Therefore, we can specify C through the roots of its generator polynomial. If $g(x) = q_1(x) \cdots q_r(x)$, product of some irreducible factors of $x^n - 1$, then $\langle g(x) \rangle = \{f(x) \in R_n : f(\beta_1) = f(\beta_2) = \cdots = f(\beta_r) = 0\}$ where β_i is a root of $q_i(x)$. Notice that the every element in the set $Z = \{\beta_i : 1 \leq i \leq r\}$ is an n-th root of unity and therefore is a power of the primitive n-th root of unity, say ω, over $\mathbb{F}_q$. The set Z is called the *zero set of the code* C and uniquely identifies it.

1.4.2. *BCH Codes*

A very important class of cyclic codes is BCH codes, discovered by Bose, Ray-Chaudhuri and Hocquenghem. They are defined by specifying the roots of a cyclic code.

Definition 1.15. Let $q, n, b, d \in \mathbb{N}$, where q is a prime power, $(n, q) = 1$, and $2 \leq d \leq n$. Let ω be a primitive n-th root of unity over $\mathbb{F}_q$,(we know that ω

lies in $\mathbb{F}_{q^m}$ where $m = ord_n(q)$), m_i be the minimal polynomial of ω^i and $Z := \{b, b+1, \ldots, b+d-2\}$. Then the *BCH code* $C \subseteq \mathbb{F}_q^n$ of *designed distance* d is a cyclic code of length n over $\mathbb{F}_q$ defined by the following equivalent conditions:
i) $\mathbf{v} \in C$ if and only if $\mathbf{v}(\omega^i) = 0$ for all $i \in Z$.
ii) The polynomial $lcm\{m_i : i \in Z\}$ is the least degree (monic) generator polynomial of C.
iii) A parity check matrix of C is the matrix

$$\begin{bmatrix} 1 & \omega^b & \omega^{2b} & \ldots & \omega^{b(n-1)} \\ 1 & \omega^{b+1} & \omega^{2(b+1)} & \ldots & \omega^{(b+1)(n-1)} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & \omega^{b+d-2} & \omega^{2(b+d-2)} & \ldots & \omega^{(b+d-2)(n-1)} \end{bmatrix}$$

Remark. If $b = 1$ in the last definition the resulting BCH code is called a *narrow-sense BCH code*. If $n = q^m - 1$, the BCH code is called *primitive*.
A well-known result about BCH codes is the BCH bound.

Theorem 1.9. *(BCH bound) A BCH code of designed distance d defined by 1.15 has minimum distance $\geq d$.*

The BCH bound can be proven by applying Lemma 1.2 on the parity check matrix. Alternatively, it can be proven using Mattson-Solomon polynomials.[64]

A practical example for the use of BCH codes is the European and trans-Atlantic information communication system, which has been using such codes for many years.[49] The message symbols are of length 231 and the generator polynomial is of degree 24 so that 231+24=255=$2^8 - 1$ is the length of the codewords. The code detects at least 6 errors and its failure (incorrect decoding) probability is one in sixteen million.

Exercise 1.4.1. Determine the parameters of the binary, narrow-sense BCH code of length 15, and designed distance 5.

1.4.3. *Reed Solomon Codes*

A special case of BCH codes is *Reed-Solomon codes* (or *RS codes* for short) which are defined as narrow sense BCH codes of designed distance d and of length $n = q - 1$ over $\mathbb{F}_q$. Hence $m = 1$ and $\mathbb{F}_q$ posses a primitive n-th root of unity. The generator

polynomial of least degree for an RS code is

$$g(x) = \prod_{i=1}^{d-1}(x - \omega^i),$$

where ω is a primitive element of $\mathbb{F}_q$. It turns out that an RS code has parameters $[n, k, n-k+1]_q$ where $n = q-1$, i.e., they are MDS codes.

RS codes are used to obtain high sound quality of compact discs.

There is an alternative description of RS codes that motivates the construction of algebraic geometry codes: Let $1 \leq n \leq q$, $1 \leq k \leq n$ and let

$$P_k = \{f(x) \in \mathbb{F}_q[x] : \deg f(x) < k\}.$$

First, choose n distinct elements $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{F}_q$, then define a Reed-Solomon code by

$$GRS_q(n, k) = \{(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)) : f(x) \in P_k\}.$$

It can easily be verified that the code $GRS_q(n, k)$ is a linear code with the parameters $[n, k, n-k+1]_q$ over $\mathbb{F}_q$.

Exercise 1.4.2. Show that an RS code of length $n = q$ defined by the second method is equivalent to a cyclic code.

1.4.4. *Hamming Codes*

Hamming codes are an important class of linear codes. The binary Hamming code with parameters [7,4,3] was one of the first codes designed and used in practice by R. Hamming.[39] In general, they are defined via a parity check matrix over any finite field $\mathbb{F}_q$. First, choose a positive integer r. Let H be a matrix whose columns consist of all vectors of length r over $\mathbb{F}_q$ whose first non-zero entry is 1. What are the parameters of the Hamming code? A counting argument shows that there are $1 + q + q^2 + \cdots + q^{r-1} = \frac{q^r-1}{q-1}$ such vectors, therefore, H is an r by n matrix, where $n = \frac{q^r-1}{q-1}$. What is the rank of H? It is easy to see that after a permutation of columns (if necessary), H can be put into the form $\left(I_r \middle| H'\right)$ where I_r is the identity matrix of order r. Therefore, the rank of H is r, and its nullity, which is the dimension of the Hamming code, is $n - r$. Finally, we want to determine the minimum distance of Hamming code. One can easily show that no two columns are linearly independent (i.e., no column is a scalar multiple of

another), and there exist three columns that are linearly dependent. Hence, by Lemma 1.2 the minimum distance is 3, and the parameters of the Hamming code are $[n, n-r, 3]_q$, where $n = \frac{q^r-1}{q-1}$. Given these parameters, it is easy to show that Hamming codes are perfect. They are an infinite family of perfect codes. Besides Hamming codes, the only linear perfect codes are the Golay codes. Moreover, all binary Hamming codes are cyclic.[64] More generally, Hamming codes are equivalent to cyclic codes when $(r, q-1) = 1$.[64]

1.4.5. *Quadratic Residue Codes*

Quadratic residue codes are also a special class of cyclic codes. To define them, we first need to introduce the concept of a quadratic residue. Let p be an odd prime. An integer a such that $(a, p) = 1$ is called a quadratic residue $\mod p$ if the equation $x^2 \equiv a \mod p$ has a solution. Otherwise, a is called a quadratic non residue. The set of quadratic residues and non-residues $\mod p$ are denoted by QR and NR respectively. For example, for $p = 23$, $QR = \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$ and NR is the rest of the non-zero integers modulo 23. It is well known that of the $p-1$ non-zero integers $\mod p$, exactly half of them are in QR and the other half are in NR. It is also easy to show that if $x, y \in QR$, then $xy \in QR$, and if $x, y \in NR$, then $xy \in QR$. On the other hand, if $x \in QR$ and $y \in NR$ then $xy \in NR$.

Let p be an odd prime, and let q be a prime that is a quadratic residue $\mod p$. From the closure properties of QR and NR, it follows that whenever an element from a cyclotomic coset $cl_i = \{i, iq, iq^2, \dots\}$ of $q \mod p$ is in QR, the entire set cl_i is contained in QR. The same is true for NR. Therefore, the QR and NR are unions of cyclotomic cosets of $q \mod p$. For such primes p and q let ω be a primitive p-th root of unity over $\mathbb{F}_q$, and let $q(x) = \prod_{r \in QR} (x - \omega^r)$ and $n(x) = \prod_{s \in NR} (x - \omega^s)$. Then, since QR and NR are unions of cyclotomic cosets, the polynomials $q(x)$ and $n(x)$ are in $\mathbb{F}_q[x]$. Moreover, $x^p - 1 = (x-1)q(x)n(x)$. The q-ary cyclic codes generated by $Q(p) = \langle q(x) \rangle$, $\overline{Q(p)} = \langle (x-1)q(x) \rangle$, $N(p) = \langle n(x) \rangle$, $\overline{N(p)} = \langle (x-1)n(x) \rangle$ are called quadratic residue (QR) codes. Clearly, $Q(p) \supseteq \overline{Q(p)}$, and $N(p) \supseteq \overline{N(p)}$. It is also clear that $\dim Q(p) = \dim N(p) = p - \deg(q(x)) = \frac{p+1}{2}$. It can be shown that the codes $Q(p)$ and $N(p)$ are equivalent, hence they have the same minimum distance d. The square root bound[53] states that $d^2 \geq p$. Furthermore, if $p = 4m-1$ then $d^2 - d + 1 \geq p$.

Example 1.6. Let $q = 2$, and $p = 2$. Then p is a quadratic residue $\mod 23$ ($5^2 \equiv 2 \mod 23$). In general, 2 is a quadratic residue $\mod p$ (p odd prime) if and only if $p \equiv \pm 1 \mod 8$. Then we know that $x^{23} - 1 = (x-1)q(x)n(x)$ over $\mathbb{F}_2$, where $\deg(q(x)) = \deg(n(x)) = 11$. The resulting quadratic residue codes $Q(p)$ and $N(p)$ have dimension 12. Moreover, by the square root bound, the minimum distance is at least 6. The actual minimum distance turns out to be 7. This is the famous binary Golay code with parameters [23,12,7], denoted by G_{23}. Its extension is a [24,12,8]-code, G_{24}. These two codes have some fascinating properties. G_{23} is the only binary, multiple error correcting, perfect code. G_{24} leads to a unique combinatorial design called a Steiner triple system (a 5-design).[58] It also give a construction of a densest lattice in dimension 24, called the Leech lattice.[72] Moreover, both G_{23} and G_{24} led to the discovery of some new simple groups.[72]

Similarly, the ternary Golay code, G_{11} is also a QR residue code with parameters $[11, 6, 5]_3$. It is well known that the Golay codes are the only multiple error correcting perfect codes (up to equivalence).[58]

Exercise 1.4.3. Show that the Golay codes G_{23}, G_{11} are perfect.

1.5. Constacyclic and Quasi Twisted Codes

This section is largely from,[7] parts of it reprinted with kind permission of Springer Science and Business Media.

1.5.1. *Constacyclic Codes*

There are several generalizations of cyclic codes. One immediate generalizaton is the class of *constacyclic* codes. Let $a \in \mathbb{F}_q^* := \mathbb{F}_q - \{0\}$. A linear code of length n over $\mathbb{F}_q$ is called *constacyclic* if it is invariant under the constacyclic shift:

$$(c_0, c_1, \ldots, c_{n-1}) \longmapsto (ac_{n-1}, c_0, \ldots, c_{n-2})$$

Notice that in the case $a = 1$ we recover cyclic codes. When $a = -1$, they are called *negacyclic* codes. Most of the results about cyclic codes are also true for constacyclic codes. These are summarized in the following proposition. Recall the identification of words (vectors) of $\mathbb{F}_q^n$ with polynomials of degree $\leq n - 1$.

Lemma 1.14. *i) Constacyclic codes are precisely the ideals in the ring* $\frac{\mathbb{F}_q[x]}{\langle x^n - a\rangle}$. *ii)The ring* $\frac{\mathbb{F}_q[x]}{\langle x^n - a\rangle}$ *is a principal ideal ring and for a conctacyclic code C there exists a polynomial $g(x)$ (called the generator polynomial) of smallest degree such that*

$C = \langle g(x) \rangle$ *where* $g(x)|(x^n - a)$ *and* $\dim(C) = n - \deg(g(x))$.
iii)If $g(x) = g_0 + g_1 x + \ldots + g_r x^r$ *then a generator matrix for* C *is*

$$G = \begin{pmatrix} g_0 & g_1 & g_2 \ldots & g_r & 0 & \ldots & 0 \\ 0 & g_0 & g_1 \ldots & g_{r-1} & g_r & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & 0 & g_0 & g_1 & g_2 \ldots & g_r \end{pmatrix}$$

where each row of G *is a constacyclic shift of the previous one.*

Proof. Everything is proved as in the cyclic case. □

Similarly to cyclic codes, a constacyclic code can be specified through the roots of its generator polynomial. In studying cyclic codes the factorization of $x^n - 1$ was crucial. Now, we are interested in factorizing $x^n - a$ over $\mathbb{F}_q$. Before looking at this factorization, we remark that in certain cases constacyclic codes are equivalent to cyclic codes.

Lemma 1.15. *If* $\mathbb{F}_q$ *contains an* n*-th root* δ *of* a*, then a constacyclic code of length* n *is equivalent to a cyclic code of length* n.

The following lemma tells us exactly when an element $a \in \mathbb{F}_q$ has an n-th root in $\mathbb{F}_q$.

Lemma 1.16.[64] *Let* $a = \alpha^i$ *where* α *is a primitive element of* $\mathbb{F}_q$. *Then the equation* $x^n = a$ *has a solution in* $\mathbb{F}_q$ *if and only if* $(n, q-1)|i$, *where* $(n, q-1)$ *denotes the greatest common divisor of the integers* n *and* $q - 1$.

Proof. The equation $x^n = a$ has a solution $x = \alpha^j \iff \alpha^{nj} = \alpha^i$
$\iff \alpha^{nj-i} = 1$
$\iff (q-1)|(nj - i)$
$\iff i = nj + r(q-1)$ for some integers r, j.
$\iff (n, q-1)|i$ □

So in our investigation of constacyclic codes, we are going to consider the case $(n, q-1) \not| i$.

1.5.2. *Factorization of $x^n - a$ and a BCH bound*

Let $a \in \mathbb{F}_q^*$ be such that it does not have an n-th root in $\mathbb{F}_q$. We also assume that $(n, q) = 1$ so that the polynomial $x^n - a$ does not have multiple roots. The roots of $x^n - a$ are $\delta, \delta\zeta, \delta\zeta^2, \ldots, \delta\zeta^{n-1}$ where ζ is a primitive n-th root of unity and $\delta^n = a$. Then ζ lies in F_{q^m} where $m = ord_q(n)$. By assumption $\delta \notin \mathbb{F}_q$. Since $\delta^n = a$, $\delta^{nr} = a^r = 1$, where r is the order of a in the multiplicative group $\mathbb{F}_q^*$ which is equal to $\frac{q-1}{(i,q-1)}$, $a = \alpha^i$ and α is a primitive element of $\mathbb{F}_q$. Hence δ is an nr-th root of 1. Therefore, $\delta \in F_{q^s}$ where $s = ord_q(nr)$. Now, $q^s - 1 \equiv 0 \mod nr \Longrightarrow q^s - 1 \equiv 0 \mod n$. This implies that $m|s$. Consequently, $F_{q^m} \subseteq F_{q^s}$. Hence, the field F_{q^s} contains both ζ and δ and we may take $\delta = w^t$ and $\zeta = w^{rt}$ where w is a primitive element of F_{q^s} (hence a primitive $(q^s - 1)$- st root of unity) and $q^s - 1 = ntr$, for some integer t. So $\zeta = \delta^r$ And $x^n - a$ factors as follows:

$$x^n - a = \prod_{i=0}^{n-1}(x - \delta\zeta^i) = \prod_{i=0}^{n-1}(x - w^{t(1+ir)}) = \prod_{i=0}^{n-1}(x - \delta^{1+ir})$$

Each irreducible factor of $x^n - a$ corresponds to a cyclotomic coset modulo nr (*not* modulo n) i.e. the degree of each irreducible factor is the same as size of a cyclotomic coset modulo nr. Since all the roots of $x^n - a$ are nr-th roots of unity, we have that $(x^n - a)|(x^{nr} - 1)$ also, $(x^{nr} - 1)|(x^{n(q-1)} - 1)|(x^{q^s-1} - 1)$

Example 1.7. Let $q = 5$ and $n = 6$ and let us consider the polynomial $x^6 - 3$ over $\mathbb{F}_5$(hence constacyclic codes of length 6 over $\mathbb{F}_5$ with $a = 3$). A primitive element of $\mathbb{F}_5$ is 2, $3 = 2^3$ in $\mathbb{F}_5$, order of 3 in $\mathbb{F}_5$ is 4 and $(n, q - 1) = (6, 4) = 2 \not| 3$ so that there is no 6-th root of 3 in $\mathbb{F}_5$. According to the discussion above,

$$x^6 - 3 = \prod_{i=0}^{5}(x - \delta^{4i+1}) = (x^2 + 3x + 3)(x^2 + 2x + 3)(x^2 + 3)$$

where δ is a primitive $6 \cdot 4 = 24$-th root of unity. The powers of δ that appear in this factorization are $1, 5, 9, 13, 17, 21$ and these are precisely union of three (the same as the number of irreducible factors over $\mathbb{F}_5$) cyclotomic cosets modulo 24: $cl_1 = \{1, 5\}$, $cl_9 = \{9, 21\}$, $cl_{13} = \{13, 17\}$. On the other hand, $x^{24} - 1$ and $x^6 - 1$ factor over $\mathbb{F}_5$ as follows:

$$\begin{aligned} x^{24} - 1 =& (x^2 + 3x + 3)(x^2 + 2x + 3)(x^2 + 3)(x^2 + 4x + 1)(x^2 + x + 2) \\ & (x^2 + 2x + 4)(x^2 + x + 1)(x^2 + 4x + 2)(x^2 + 3x + 4)(x^2 + 2) \\ & (x + 3)(x + 4)(x + 2)(x + 1) \end{aligned}$$

$x^6 - 1 = (x^2 + 4x + 1)(x^2 + x + 1)(x + 1)(x + 4)$ The factors of $x^6 - 1$ correspond to the following cyclotomic cosets modulo 24: $cl_0 = \{0\}, cl_4 = \{4, 20\}$, $cl_8 = \{8, 16\}, cl_{12} = \{12\}$ which are obtained by shifting the cosets corresponding to $x^6 - 3$ by 1.

1.5.3. *BCH Bound for Constacyclic Codes*

Lemma 1.17. *Let C be a constacyclic code of length n over $\mathbb{F}_q$ and let the generator polynomial $g(x)$ have the elements $\{\delta\zeta^i : 1 \leq i \leq d-1\}$ among its roots. Then the minimum distance of $C \geq d$.*

Proof. Consider the constacyclic code C of length n with generator polynomial $g(x)|(x^n - a)$ having $\{\delta\zeta, \delta\zeta^2, \ldots, \delta\zeta^{d-1}\} = \{\delta^{r+1}, \delta^{2r+1}, \ldots, \delta^{(d-1)r+1}\}$ among its roots. The corresponding cyclic code $\psi(C)$ generated by $g(\delta x)|(x^n - 1)$ has the elements $\zeta, \zeta^2, \ldots, \zeta^{d-1}$ among the roots. By the BCH bound, the minimum distance of $\psi(c) \geq d$. Therefore, $d(C) \geq d$ as well. □

We now give an example of a constacylic code that is optimal.

Example 1.8. Let $q = 3$ and $n = 28$ and consider constacyclic codes of length 28 over $\mathbb{F}_3$ with $a = 2$. We remark that the condition $(n, q-1) \not| i$ implies that we should consider only even lengths over $\mathbb{F}_3$. We find that $r = 2$ and therefore $(x^{28} - 2)|(x^{56} - 1)$. The factorization of $x^{28} - 2$ over $\mathbb{F}_3$ is as follows:

$$\begin{aligned} x^{28} - 2 &= \prod_{i=0}^{27}(x - \delta\zeta^i) = \prod_{i=0}^{27}(x - \delta^{2i+1}) \\ &= (x^6 + 2x^4 + x^3 + x^2 + 2)(x^6 + 2x^5 + 2x + 2)(x^2 + x + 2) \\ &\quad (x^6 + x^5 + x + 2)(x^6 + 2x^4 + 2x^3 + x^2 + 2)(x^2 + 2x + 2) \end{aligned}$$

where δ is a primitive 56-th root of 1 and $\zeta = \delta^2$ is a primitive 28-th root of 1 over $\mathbb{F}_3$. The exponents of δ in this factorization are exactly odd integers modulo 56 and they are partitioned into following cyclotomic cosets.
{1,3,9,19,25,27}, {5,13,15,23,39,45}, {7,21}, {11,17,33,41,43,51},
{29,31,37,47,53,55}, {35,49}
Let $g(x)$ be the polynomial of smallest degree which contains $\delta^i, i = 7, 11, 29, 35$ among its roots. Then

$g(x) = x^{20}+2x^{19}+x^{17}+2x^{16}+2x^{13}+2x^{12}+2x^{11}+x^{10}+x^9+2x^8+x^7+2x^4+2x^3+x+1$

and the consecutive powers $\alpha^i, 14 \leq i \leq 27$ of α are also among the zeros of $g(x)$. Therefore, by the BCH bound for constacyclic codes, the constacylic code of length 28 generated by $g(x)$ has minimum distance at least 15 (and its dimension is 8). It turns out that these are the parameters of an *optimal* linear code over $\mathbb{F}_3$ of length 28 and dimension 8.[33]

Exercise 1.5.1. Construct a constacyclic code of length 26, dimension 16, and minimum distance 8 over $\mathbb{F}_5$ with constant $a = 2$ or 3. Note that such a code would be optimal.

1.5.4. *Quasi Twisted Codes*

The class of quasi-twisted (QT) and their special case of quasi-cyclic (QC) codes are a generalization of constacyclic (cyclic) codes and they have been shown to be promising towards solving the main problem in coding theory: to construct codes with the best possible parameters. A large number of new codes in these classes have been discovered in recent years. Often, computers are employed in finding these codes. For a sample of results in this area see[6–8,22,23,34,38,68] among others.

Let $n = lm$ where $l, m \in \mathbb{N}$, $a \in \mathbb{F}_q^*$ and define $\mu_{a,l} : C \to \mathbb{F}_q^n$ by

$\mu_{a,l}\big((c_0, \ldots, c_{n-1})\big) = (a \cdot c_{0-l}, \ldots, a \cdot c_{(l-1)-l}, c_{l-l}, \ldots, c_{n-l-1})$ where the subscripts are taken modulo n.

Definition 1.16. A linear code C is called l-quasi-twisted (l-QT) if $\mu_{a,l}(C) = C$.

In words, a constacyclic shift of a codeword by l positions is still a codeword. Some of the most important classes of codes can be realized as special cases of QT codes. For example the case $a = 1$ gives QC codes , $l = 1$ gives constacyclic codes (also known as pseudocyclic codes), $l = 1$ and $a = 1$ yields cyclic codes.

1.5.5. *Structure of* 1*-Generator QT codes*

An l-QT code over $\mathbb{F}_q$ of length $n = ml$ can be viewed as an $\mathbb{F}_q[x]/\langle x^m - a\rangle$ submodule of $(\mathbb{F}_q[x]/\langle x^m - a\rangle)^l$ (after a permutation of the coordinates). Then an r-generator QT code is spanned by r elements of $(\mathbb{F}_q[x]/\langle x^m - a\rangle)^l$. In this chapter we restrict ourselves to 1-generator QT codes. Let

$$G_0 = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_{m-1} \\ ag_{m-1} & g_0 & g_1 & \cdots & g_{m-2} \\ ag_{m-2} & ag_{m-1} & g_0 & \cdots & g_{m-3} \\ \vdots & \vdots & \vdots & & \vdots \\ ag_1 & ag_2 & ag_3 & \cdots & g_0 \end{bmatrix}_{m\times m}.$$

An $(m \times m)$ matrix of the type G_0 is called a twistulant matrix of order m or simply a twistulant matrix. It is shown in[7] that the generator matrices of QT codes can be transformed into blocks of twistulant matrices by suitable permutation of columns. Therefore, generator matrices of an r-generator and 1-generator QT codes can be assumed to be in the following forms:

$$\begin{bmatrix} G_{11} & G_{12} & \ldots & G_{1l} \\ G_{21} & G_{22} & \ldots & G_{2l} \\ \vdots & \vdots & & \vdots \\ G_{r1} & G_{r2} & \ldots & G_{rl} \end{bmatrix}_{rm\times n}, \text{ and } \begin{bmatrix} G_1 & G_2 & \ldots & G_l \end{bmatrix}_{m\times n},$$

respectively, where each G_{ij} (or G_k) is a twistulant matrix of the form 1.5.5.

Most of the work in the literature is concerned with 1-generator QC or QT codes. Often, computer searches with heuristic search algorithms are employed (e.g.[24,37]) to find new codes. A number of papers focus on rate $1/l$ and related QC codes (e.g.[35,38]). More recently, a different search algorithm was devised for a certain type of 1-generator QC[68] and QT[7] codes inspired by the work in.[43] This method produced a number of new codes over most small finite fields for which a database of best known codes is available (e. g.[5,7,22,23,25,69,70]). The method is described in detail in the rest of this section.

Let $1 \leq i \leq l$. For fixed i consider the following i^{th} *restriction map* on an l-QT code C of length $n = ml$:

$$\Pi_i : \mathbb{F}_q^n \to \mathbb{F}_q^m$$

$$(c_0, c_1, \ldots, c_{(ml-1)}) \to (c_{(i-1)m}, c_{(1+(i-1)m)}, \ldots, c_{(m-1+(i-1)m)}).$$

In view of the structure of QT codes described above, $\Pi_i(C)$ is a constacyclic code for all i. This yields the following theorem.

Theorem 1.10. *Let C be a 1-generator l-QT code over $\mathbb{F}_q$ of length $n = ml$. Then, a generator $\mathbf{g}(\mathbf{x}) \in (\mathbb{F}_q[x]/\langle x^m - a\rangle)^l$ of C has the following form*

$$\mathbf{g}(\mathbf{x}) = (f_1(x)g_1(x), f_2(x)g_2(x), \ldots, f_l(x)g_l(x)),$$

where $g_i(x)|(x^m-a)$ *and* $(f_i(x),(x^m-a)/g_i(x))=1$ *for all* $1\leq i\leq l$.

Proof. Since $\Pi_i(C)$ is a constacyclic code for every i we have the result. □

The following theorem plays an important role in some search methods mentioned above.

Theorem 1.11. *Let* C *be a* 1*-generator* l*-QT code of length* $n=ml$ *with a generator of the form:*

$$\mathbf{g}(\mathbf{x})=(f_1(x)g(x),f_2(x)g(x),\ldots,f_l(x)g(x))$$

where $g(x)|(x^m-a), g(x), f_i(x)\in\mathbb{F}_q[x]/\langle x^m-a\rangle$, *and* $(f_i(x),h(x))=1$, $h(x)=\frac{x^m-a}{g(x)}$ *for all* $1\leq i\leq l$. *Then* $l\cdot(d+1)\leq d(C)$, *where* $\{\delta\zeta^i : s\leq i\leq s+(d-1)\}$ *are among the zeros of* $g(x)$ *for some integers s,d* ($d>0$) *and dimension of* C *is equal to* $n-\deg(g(x))$.

Next, we present two examples that illustrate how the results in this section and the last theorem in particular is used in designing a computer search algorithm to discover new linear codes.

Example 1.9. This example presents a ternary QT code that has the best known parameters among all linear codes with the same length and dimension.[7] Let q=3, m=40 and a=2 and consider constacyclic codes of length 40 over $\mathbb{F}_3$. The order of 2 mod 3 is 2 and $x^{40}-2$ factors over $\mathbb{F}_3$ as

$$x^{40}-2=\prod_{i=0}^{39}(x-\delta^{2i+1})$$

The exponents of δ (a primitive $80-th$ root of 1) are odd integers mod 80 and the corresponding powers of ζ (a primitive 40-th root of 1) are broken into the following cyclotomic cosets mod 40:
{0,1,4,13}, {2,7,22,27}, {3,10,14,31}, {5,9,16,28}, {6,15,18,19}
{8,25,29,36}, {11,23,30,34}, {12,17,32,37}, {20,21,24,33}
{26,35,38,39}
Let $h(x)$ be the polynomial corresponding to cyclotomic cosets containing 0,3 and 12 and let

$$g(x)=\frac{x^{40}-2}{h(x)}=x^{28}+2x^{27}+2x^{25}+x^{24}+2x^{23}+x^{21}+2x^{20}+x^{19}+x^{18}+2x^{17}+2x^{15}+x^{14}+x^{13}+2x^{11}+x^8+2x^7+2x^5+x^3+x^2+2.$$

Then $g(x)$ has degree 28 and contains consecutive powers $18 \leq i \leq 30$ of δ among its roots. Therefore, the constacylic code of length 40 generated by $g(x)$ has dimension 12 and minimum distance ≥ 14 and a quasi-twisted code of the form (gf_1, gf_2, gf_3) where $(f_i, h) = 1$ has length 120, dimension 12 and minimum distance at least 42. Let $f_1 = x^{10} + x^9 + x^8 + x^2$, $f_2 = 2x^{10} + x^9 + x^6 + x$ and $f_3 = 2x^{11} + x^{10} + x^9 + x^8 + x^5 + x^4 + x^2 + 2x$ (found by a computer search). Then f_i's satisfy $(f_i, h) = 1$. The QT code with these generators has actual minimum distance of 66, 3 units larger than the previously best known linear code over $\mathbb{F}_3$ with parameters [120,12,63].[33] The weight enumerator of this code is as follows:
$0^1 66^{4000} 69^{15120} 72^{35200} 75^{77728} 78^{108000} 81^{122160} 84^{97120} 87^{47520} 90^{18832} 93^{5040} 96^{720}$
where the bases are the weights and the exponents are the number of codewords of the given weight.

Example 1.10. This example presents a best known code over $\mathbb{F}_4$ that is QT.[5] We represent the elements of $\mathbb{F}_4$ by $\{0, 1, a, b\}$, where $b = a^2 = a + 1$. Let $g(x) = \frac{x^{39}-a}{h(x)}$ where $h(x) = (x^6 + ax^5 + x^4 + ax^3 + x + b)(x^6 + x^5 + ax^3 + x^2 + x + b)$. Then $g(x)$ generates a quaternary constacyclic code with parameters $[39, 12, 18]$. According to,[33] these are the parameters of the best-known code for this length and dimension. Searching over the codes with a generator of the form $(g(x), g(x)f_1(x))$, we find, by the help of a computer, that if we choose $f_1(x) = x + bx^3 + ax^7 + bx^9 + bx^{10} + x^{11}$, then we obtain a $[78, 12, 44]_4$-code. This turns out to be a best known code. The weight enumerator of this code is:
$0^1 44^{6786} 46^{24921} 48^{103194} 50^{321750} 52^{816075} 54^{1695096} 56^{2737215} 58^{3417453}$
$60^{3298464} 62^{2414529} 64^{1301391} 66^{491400} 68^{124371} 70^{21294} 72^{3159} 74^{117}$.

Finally, we would like to remark that most of the search over QC/QT codes have been among 1-generator codes. There are few papers in the literature that report new codes from multiple generator QC codes. Two such examples are[21].[36]

1.6. Thoughts for Practitioners

1.6.1. *Computing Minimum Distance of a Linear Code*

The problem of finding the minimum weight of a general binary linear code was conjectured to be NP-complete by Berlekamp, McEliece and van Tilborg in 1978.[10] Carey and Johnson, among others, repeatedly called for the resolution of the conjecture.[31,45,46] The increased interest in the topic resulted in the proved hardness

of a number of related problems[1,2,18,26,51,71] over the years. Yet, the original conjecture remained open for almost two decades. In 1997, employing a polynomial transformation from maximum-likelihood decoding to minimum distance, Vardy showed that finding the minimum distance of a linear code over a fixed finite field is NP-complete.[75,76] More recently, Dumer, Micciancio and Sudan showed that the minimum distance of a linear code over a finite field cannot be approximated to within any constant factor in random polynomial time(RP), unless RP equals NP.[28] Furthermore, the last result was translated to prove the hardness of approximating the minimum distance within an additive error that is linear in the block length of the code.[29]

For a $[n, k, d]_q$ linear code, computing the minimum weight via complete codeword enumeration involves finding the minimum weight for $(q^k - 1)$ codewords of length n. This is computationally infeasible even for small values of the parameters. The fastest algorithm for finding the minimum weight of a linear code over a finite field is based on an unpublished work by Brouwer that was later improved by Zimmermann.

1.6.1.1. *The Brouwer-Zimmermann Algorithm for Linear Codes*

The work of Zimmermann was only published in German[19] but English summaries are available.[11,73,79] In determining the minimum weight of a $[n, k, d]_q$ linear code, the algorithm employs mutually disjoint(or partially disjoint) information sets and partial codeword enumeration to compute an upper bound d_u on d, while keeping track of a lower bound d_l of d that grows linearly with the number of disjoint information sets. Termination is reached when $d_l \geq d_u$. For a $[n, k, d]_q$ cyclic code having an information set formed by k consecutive columns, there always exist $\lfloor n/k \rfloor$ mutually disjoint information sets. Moreover, the generator matrix corresponding to a single information set is sufficient for codeword enumeration for all $\lfloor n/k \rfloor$ generator matrices.[11] Thus, for some cyclic codes, a faster growth of d_l can be achieved using a single information set. This result can be extended to the case of constacyclic codes as well.

Often times, one is interested in finding the minimum weight of a linear code but only if it is within a certain range. In this case, the termination point of the algorithm can be adjusted. The MAGMA algebra system[12] supports such a feature via

the functions VerifyMinimumDistanceLowerBound(C, d) and VerifyMinimumDistanceLowerBound(C, d). The authors have devised a recent combinatorial search algorithm that makes an extensive use of this functionality.[3] The algorithm examines a large number of codes in the search space and employs the VerifyMinimumDistanceUpperBound() function to quickly discard codes with minimum distance below a prescribed value.

As far as parallel computing is concerned, an easy parallelization of the Brouwer-Zimmermann algorithm has been implemented by van Dijk, Egner, Greferath and Wassermann.[73] Their approach is based on the revolving door algorithm by Nijenhuis and Wilf, and a combinatorial result by of Lüneburg[52] and Knuth.[47] Furthermore, the autoson program by McKay can be used to distribute the work over a network of Unix workstations.[54]

Finally, for certain codes of high rate $R = k/n > 1/2$, finding the weight distribution of the dual code and using the MacWilliams transform might prove faster than running the Brouwer-Zimmermann Algorithm.

1.7. Codes over $\mathbb{Z}_4$ and Database of $\mathbb{Z}_4$ Codes

1.7.1. *Codes over* $\mathbb{Z}_4$

After the discovery of good binary non-linear codes from codes over $\mathbb{Z}_4$, the ring of integers modulo 4 (sometimes called "quaternary codes")[40,55] there has been intensive research on this class of codes. A *code* C of length n over $\mathbb{Z}_4$ is a subset of $\mathbb{Z}_4^n$. C is a *linear code* over $\mathbb{Z}_4$ if it is an additive subgroup of $\mathbb{Z}_4^n$, hence a submodule of $\mathbb{Z}_4^n$. An element of C is called a *codeword* and a *generator matrix* is a matrix whose rows generate C. The *Hamming weight* $w_H(x)$ of a vector $x = (x_1, x_2, \ldots, x_n)$ in $\mathbb{Z}_4^n$ is the number of components $x_i \neq 0$. The *Lee weight* $w_L(x)$ of a vector x is $\sum_{i=1}^{n} \min\{|x_i|, |4 - x_i|\}$. The Hamming and Lee distances $d_H(x, y)$ and $d_L(x, y)$ between two vectors x and y are $w_H(x - y)$ and $w_L(x - y)$, respectively. The minimum Hamming and Lee weights, d_H and d_L, of C are the smallest Hamming and Lee weights, respectively, amongst all non-zero codewords of C.

The *Gray map* $\phi : \mathbb{Z}_4^n \to \mathbb{Z}_2^{2n}$ is the coordinate-wise extension of the function from $\mathbb{Z}_4$ to $\mathbb{Z}_2^2$ defined by $0 \to (0,0), 1 \to (1,0), 2 \to (1,1), 3 \to (0,1)$. The image $\phi(C)$, of a linear code C over $\mathbb{Z}_4$ of length n by the Gray map, is a (in general non-linear) binary code of length $2n$. The Gray map is an isometry from $(\mathbb{Z}_4^n, w_L)$ to $(\mathbb{Z}_2^{2n}, w_H)$. Therefore, the minimum Hamming weight of $\phi(C)$ is equal to the

minimum Lee weight of C.

The *dual code* $C^\perp$ of C is defined as $\{x \in \mathbb{Z}_4^n \mid x \cdot y = 0, \forall\ y \in C\}$, where $x \cdot y$ is the standard inner product of x and y. C is *self-orthogonal* if $C \subseteq C^\perp$ and C is *self-dual* if $C = C^\perp$.

Two codes are said to be *equivalent* if one can be obtained from the other by permuting the coordinates and (if necessary) changing the signs of certain coordinates. Codes differing by only a permutation of coordinates are called *permutation-equivalent*. Any linear code C over $\mathbb{Z}_4$ is permutation-equivalent to a code with generator matrix G of the form

$$G = \begin{bmatrix} I_{k_1} & A_1 & B_1 + 2B_2 \\ 0 & 2I_{k_2} & 2A_2 \end{bmatrix},$$

where A_1, A_2, B_1, and B_2 are matrices with entries 0 or 1 and I_k is the identity matrix of order k. Such a code has size $4^{k_1}2^{k_2}$. The code is a free module if and only if $k_2 = 0$. If C has length n and minimum Lee weight d_L, the code is referred to as an $[n, 4^{k_1}2^{k_2}, d_L]$-code.

1.7.2. *A Database of $\mathbb{Z}_4$ Codes*

Cyclic codes, QC codes and QT codes over $\mathbb{Z}_4$ are studied in[6,8] and many new codes are discovered whose Gray images have better parameters than best known binary linear codes. Among other results in this area, two new non-linear binary codes have been constructed using $\mathbb{Z}_4$ linear codes and their binary images. One of the codes has binary parameters $(64, 2^{37}, 12)$.[20] Another code has binary parameters $(92, 2^{24}, 28)$.[8] The latter code is QC over $\mathbb{Z}_4$ and its generator polynomial is related to the generator polynomial of the binary Golay code G_{23}. Moreover, many $\mathbb{Z}_4$ codes have been discovered whose Gray images have better parameters than the comparable binary linear codes (such codes are called "good codes").[4,6,8] Since the Gray image of a $\mathbb{Z}_4$ linear code is most often non-linear, it is appropriate to compare their parameters with the codes in.[50] However, the database in[50] is very limited and often does not extend to the parameters of interest. Despite extensive research on codes over $\mathbb{Z}_4$, there has been no database of best known $\mathbb{Z}_4$ codes. Recently, such a database has been created by the authors. It is available online at http://Z4codes.info.

While the Hamming distance has been the dominant metric in the field case, researchers have explored different distance functions for codes over $\mathbb{Z}_4$. Most re-

searchers have focused their work on the Lee distance but Euclidean and Hamming metrics have also been considered. In order to deal with the presence of multiple distance functions we had to adopt a list, rather than the typical tabular structure for our database. Moreover, we chose not to overwrite existing codes when an improved code has been found but only add the new code to the list. Finally, for the sake of flexibility and convenience, we have decided to provide the willing researchers with editing privileges that would allow them to upload their new results instantly.

1.8. Directions for Future Research

In this section we list a few open problems in algebraic coding theory, related to the material that is discussed in this chapter. These problems appear in,[5] portions reprinted, with permission, from[5]

1.8.1. *QCT Codes*

This subsection reviews a generalization of QT codes (hence of QC codes as well), called QCT codes that are first introduced in,[5] and investigates their structural properties. It then presents open problems in this class.

Let $a_1, a_2, \ldots, a_l$ be non-zero constants (not necessarily distinct) in $\mathbb{F}_q$. A linear code of length $n = ml$ will be called a QCT code if it is invariant under the following shift:

$$(c_1, c_2, \ldots, c_{(m-1)l}, c_{(m-1)l+1}, \ldots, c_{ml}) \rightarrow$$
$$(a_1 c_{ml}, a_2 c_{ml-1}, \ldots, a_l c_{(m-1)l+1}, c_1, \ldots, c_{(m-1)l+1})$$

We remark that if all the constants are equal then we obtain a QT code, if they are all equal to 1 then we obtain a QC code. If $l = 1$ then we obtain constacyclic and cyclic codes as special cases.

As in the case of a QT code, it is easy to see that after a suitable permutation of the coordinate positions, a generator matrix of a QCT code can be put into blocks of twistulant matrices (each block involving a possibly different constant).

To illustrate this construction, we present two examples of QCT codes which are better than the best-known QC or QT codes over $\mathbb{Z}_4$.[5]

i) A [6,2,6] code generated by

$$G = \left[\begin{array}{cc|cc|cc} 1 & 3 & 0 & 1 & 1 & 2 \\ 1 & 1 & 1 & 0 & 2 & 1 \end{array}\right]$$

This code has minimum Lee weight $d_L = 6$, while the best QC or QT code has $d_L = 5$.[6] In addition, this code is *self-orthogonal*, and the best-known QT self-orthogonal code only has $d_L = 4$.[32]
ii) An [8,4,6] code generated by

$$G = \left[\begin{array}{cccc|cccc} 0 & 0 & 1 & 2 & 0 & 1 & 1 & 1 \\ 2 & 0 & 0 & 1 & 3 & 0 & 1 & 1 \\ 1 & 2 & 0 & 0 & 3 & 3 & 0 & 1 \\ 0 & 1 & 2 & 0 & 3 & 3 & 3 & 0 \end{array}\right]$$

This is a *self-dual* code, and the best QC or QT code with length 8 and dimension 4 has $d_L = 4$.[8,32] Note that the Gray map image of this code is the Nordstrom-Robinson code.[53] Thus this construction provides a new simple description of this code.

In addition to the codes above, many hundreds of QCT codes over $\mathbb{Z}_4$ and over finite fields have been found which have the same parameters as the best-known codes. Therefore, it is likely that this class of codes contains some new codes.

1.8.2. *Algebraic Properties of QCT Codes*

Now we like to investigate the algebraic structure of QCT codes. Let $a_i \in \mathbb{F}_q^*$, $R_i = \frac{\mathbb{F}_q[x]}{\langle x^m - a_i \rangle}$, $1 \leq i \leq l$ and $R = R_1 \times R_2 \times \cdots \times R_l$. A QCT code C, after a suitable permutation of coordinates, can be regarded as an $\mathbb{F}_q[x]$-module of R. We say that C is s-generated if it is generated by s elements. Since each block (of length m) of a QCT code is actually a constacyclic code, we have the following result.

Lemma 1.18. *An s-generated QCT Code C has generators of the form $\{g_1(x), g_2(x), \ldots, g_s(x)\}$ where*

- $g_j(x) = (g_{j1}(x), g_{j2}(x), \ldots, g_{jl}(x))$
- $g_{ji}(x) = f_{ji}(x)g_i(x)$ *for some* $g_i(x) \mid x^m - a_i$, $f_{ji}(x) \in R_i$ *and* $(f_{ji}, h_i) = 1$ *where* $x^m - a_i = g_i(x)h_i(x)$.

Again, we will focus on the 1-generator case. As a corollary we have that a 1-generator QCT code is generated by an element of the form

$$g(x) = (f_1(x)g_1(x), f_2(x)g_2(x), \ldots, f_l(x)g_l(x))$$

where $f_i(x), g_i(x) \in R_i$ and $g_i(x) \mid (x^m - a_i)$. Moreover, we can show that f_i and g_i can be chosen so that $(f_i(x), h_i(x)) = 1$ where $h_i(x) = \frac{x^m - a_i}{g_i(x)}$. For two polynomials

f and g we denote their greatest common divisor by (f, g) and their least common multiple by $[f, g]$.

Next we consider bounds on the parameters of a QCT code.

Theorem 1.12. *Let C be a 1-generator QCT code generated by an element of the form described above.*

(1) $\dim(C) = \deg([h_1, h_2, \ldots, h_l])$

(2) $d(C) \geq \min\{d_i : 1 \leq i \leq l\}$ *where d_i is the minimum distance of the i-th constacyclic block and $d(C)$ is the minimum distance of C.*

Proof. Let $h = [h_1, h_2, \ldots, h_l]$, then clearly, $h(x)g(x) = 0$ which implies that $\dim(C) \leq \deg(h)$. On the other hand, if $f(x)g(x) = 0$ then $f(x)f_i(x)g_i(x) = 0$ in R_i, for $1 \leq i \leq l$. This implies that $h_i(x) \mid f(x)f_i(x)$. Since $(h_i(x), f_i(x)) = 1$, $h_i(x) \mid f(x)$ for $1 \leq i \leq l$. Hence $h(x) \mid f(x)$. This shows $\dim(C) \geq \deg(h)$ and the assertion on the dimension. The statement on the minimum distance is rather obvious. □

Example 1.11.

Let $q = 4$ and let a be a root of the polynomial $x^2 + x + 1 \in \mathbb{F}_2[x]$ so that $\mathbb{F}_q = \mathbb{F}_2(a)$. Next choose $a_1 = 1, a_2 = a,$ and $m = 11$, $g_1(x) = x^5 + ax^4 + x^3 + x^2 + bx + 1$ and $g_2(x) = x^5 + ax^4 + ax^3 + x^2 + x + a$. Then g_1 and g_2 divide $x^{11} - 1$ and $x^{11} - a$ over $\mathbb{F}_q$ (respectively) and they generate cyclic and constacyclic codes with parameters $[11, 6, 5]_q$. A code with these parameters is optimal.[33] Now we consider the QCT code generated by $\langle g1, g2\rangle$. In this case, $h_1 = \frac{x^{11}-1}{g_1}$ and $h_2 = \frac{x^{11}-a}{g_2}$ are relatively prime so that $[h_1, h_2] = h_1h_2$, hence the dimension is 12. The minimum distance of this QCT code is 5 which shows that the lower bound on the minimum distance is attained. Thus we obtain a quaternary $[22, 12, 5]$ code. According to,[33] there exists a quaternary $[22, 12, 7]$ code.

Generalizing from this example, we can say more about the dimension and minimum distance of QCT codes in the special case when all the constants are distinct. If $a_1 \neq a_2$, then $x^m - a_1$ and $x^m - a_2$ are relatively prime. If $x^m - a_1 = g_1h_1$ and $x^m - a_2 = g_2h_2$ then $(h_1, h_2) = 1$ (as well as $(g_1, g_2) = 1$) so that $[h_1, h_2] = h_1h_2$. Then the QCT code C generated by $g = \langle g1, g2\rangle$ has dimension $k_1 + k_2$ where k_1, k_2 are, respectively, the dimensions of the constacyclic codes generated by g_1 and g_2. We also claim that in this case the minimum distance is actually equal to

$\min\{d_1, d_2\}$, where d_i is the minimum distance of the constacyclic code generated by g_i. To see this, consider $\{th_2g = (th_2g_1, 0) : t \in \mathbb{F}_q[x], t \neq 0, \deg(t) < \deg(h_1)\}$. Since $\langle g_1\rangle = \langle h_2g_1\rangle$ (because $(h_1, h_2) = 1$), we see that there is a codeword of weight d_1 in C. Similarly, one can show that C contains a codeword of weight d_2. The same argument can be applied to any l when $a_1, a_2, \ldots, a_l$ are all distinct. This shows that the minimum distance of such a QCT code is not very high. However, there is a way to impose a restriction so that a better bound on the minimum distance is obtained.

Theorem 1.13. *Let C be a 1-generator QCT code generated by, i.e., $\mathbb{F}_q$-span of $g(x) = (f_1(x)g_1(x), f_2(x)g_2(x), \ldots, f_l(x)g_l(x))$ with the conditions on the f_i's and g_i's as described before. Let $h = \min\{\deg(h_i) : 1 \leq i \leq l\}$. Then the subcode C' generated by $g(x), xg(x), x^2g(x), \ldots, x^{h-1}g(x)$ has dimension h and minimum distance $\geq d_1 + d_2 + \cdots + d_l$ where d_i is the minimum distance of the code $\langle g_i\rangle$.*

Example 1.12.

Let $q = 5, m = 13, l = 3, a_1 = 1, a_2 = 2, a_3 = 4$, $g_1 = (x^4{+}x^3{+}4x^2{+}x{+}1)(x{+}4)$, $g_2 = (x^4{+}4x^3{+}4x^2{+}x{+}1)(x{+}3)$, $g_3 = (x^4{+}2x^3{+}2x^2{+}1)(x{+}1)$ where $g_1 \mid (x^{13}{-}1)$, $g_2 \mid (x^{13}{-}2)$ and $g_3 \mid (x^{13}{-}4)$ over $\mathbb{F}_5$. The constacyclic codes $\langle g_1\rangle$, $\langle g_2\rangle$ $\langle g_3\rangle$ all have parameters $[13, 8, 4]$ and they are optimal. The subcode of $\langle f_1g_1, f_2g_2, f_3g_3\rangle$ given in the last theorem has length 39, dimension 8 and minimum distance ≥ 12. However, when we choose $f_1 = x^7, f_2 = x^7 + 2x^6 + 2x^5$ and $f_3 = 3x^6 + x + 2$ the resulting code is a $[39, 8, 21]$ code. This example shows that the actual minimum distance in this construction may be significantly larger than the lower bound promised by the theorem. This code is not the best known code however, according to[33] there is a $[39, 8, 23]$ code.

1.8.3. *Open Problems*

Open Problem I: Let C be a cyclic (or constacyclic) code of length n. How should $a(x)$ be chosen so that the minimum distance of the code $\{|u(x)|a(x)u(x)(\mod x^n - 1)| : u(x) \in C\}$ is as large as possible? Is there a difference between the field version and the ring version of this problem?

The practical evidence from searches over 1-generator QC and QT codes shows that in many cases we do get very large minimum distances. However, to the best of our knowledge, no explanation has been provided for any specific properties of the polynomials that achieve these large minimum distances (one obvious restriction on

$a(x)$ is that it be relatively prime to the complement of the canonical generator). Also, we have not noticed any explicit connection with good QT codes and this problem.

This problem can also be expressed in the following alternative, combinatorial way: Consider a 1-generator QT code C_T with a generator of the form (g, gf) where $x^m - a = gh$ and $(f, h) = 1$. Since g and fg generate the same cyclic or constacyclic code C, C_T is obtained from C by listing the codewords of C in a certain order, then listing them in another order and taking the juxtaposition. Each choice of f corresponds to an ordering of C. What would be a good ordering that preserves the linearity of the code and gives a large minimum distance?

Open Problem II: Naturally, Open Problem I can be stated for 1-generator QCT codes and their subclass described above.

Open Problem III: Find an analogue of Theorem 1.11 for multi-generator QC codes.

1.9. Conclusion and References

Algebraic coding theory is a huge subject now. Despite much work on it, the main problem of coding theory is still a challenging yet promising area of research, looking for creative approaches. In this chapter we present a selected subset of topics from the field with interesting results and related open problems. We give special attention to a promising class of codes (QC codes and their generalizations). Moreover, a new database of $\mathbb{Z}_4$ codes is introduced. The reader is referred to the cited references for more on the subject.

References

1. S. Arora, L. Babai, J. Stern and Z. Sweedyk, *The hardness of approximate optima in lattices, codes, and systems of linear equations*, Proc. 34th Annu. Symp. on the Foundation of Computer Science, Palo Alto, CA, (1993), 724–733.
2. S. Arora, L. Babai, J. Stern, and Z. Sweedyk, *The hardness of approximate optima in lattices, codes, and systems of linear equations*, J Comput. Syst. Sci., **54(2)**(1997), 317–331.
3. T. Asamov and and N. Aydin, *A search algorithm for linear codes: progressive dimension growth*, Des. Codes Cryptogr. **45(2)** (2007), 213–217.
4. N. Aydin and T. Asamov. A, *Database of $\mathbb{Z}_4$ codes*, preprint.
5. N. Aydin, T. Asamov and and T. A. Gulliver, *Some open problems on quasi-twisted and related code constructions and good quaternary codes*, Proceedings 2007 IEEE Int. Symposium on Inform. Theory (2007), 856–860.

6. N. Aydin and T. A. Gulliver, *Some good cyclic and quasi-twisted $\mathbb{Z}_4$-linear codes*, to appear in Ars Comb.
7. N. Aydin, I. Siap, and D. K. Ray-Chaudhuri, *The structure of 1-generator quasi-twisted codes and new linear codes*, Des. Codes Cryptogr. **24** (2001), 313–326.
8. N. Aydin and D. K. Ray-Chaudhuri, *Quasi-cyclic codes over $\mathbb{Z}_4$ and some new binary codes*, IEEE Trans. Inform. Theory **48** (2002), 2065–2069.
9. E. R. Berlekamp, *Algebraic Coding Theory*, McGraw-Hill, New York (1968).
10. E. R. Berlekamp, R. J. McEliece and H.C.A. van Tilborg, *On the inherent intractability of certain coding problems*, IEEE Trans. Inform. Theory, **24** (1978) 384–386.
11. W. Bosma , J. Cannon, *Discovering mathematics with magma: reducing the abstract to concrete*. Springer, Berlin (2006)
12. W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system I: The user language*, J. Symbolic Computation **24** (1997), 235–265.
13. I. Bouyukliev, S. Kapralov, T. Maruta and M. Fukui, *Optimal linear codes of dimension 4 over $\mathbb{F}_5$*, IEEE Trans. Inform. Theory **43** (1997), 308–313.
14. I. Bouyukliev, D. B. Jaffe and V. Vavrek, *The smallest length of eight-dimensional binary linear codes with prescribed minimum distance*, Trans. Inform. Theory **46** (2000), 1539–1544.
15. I. Bouyukliev and J. Simonis, *Some new results for optimal ternary linear codes*, IEEE Trans. Inform. Theory, **48** (2002), 981–985.
16. I. Bouyukliev, M.Grassl and Z. Varbanov, *New bounds for $n_4(k, d)$ and classification of some optimal codes over GF(4)*, Discrete Mathematics **281** (2004), 43–66, 981–985.
17. A. E. Brouwer, *Bounds on the size of linear codes*, in *Handbook of Coding Theory*, V. Pless and W. C. Huffmann, Eds. Amsterdam, The Netherlands: Elsevier (1998).
18. J. Bruck and M. Naor, *The hardness of decoding linear codes with preprocessing*, IEEE Trans. Inform. Theory, **36** (1990), 381–385.
19. A. Betten, H. Fripertinger, A. Kerber, A. Wassermann, and K.-H Zimmermann, *CodierungstheorieKonstruktion und Anwendung Linearer Codes*, Heidelberg, Germany: Springer-Verlag (1998)
20. A. R. Calderbank and G. McGuire, *Construction of a $(64, 2^{37}, 12)$ code via Galois rings*, Des. Codes Cryptogr. **10** (1997), 157–165.
21. E. Z. Chen, *New constructions of a family of 2-generator quasi-cyclic two-weight codes and related codes*, Proceedings 2007 IEEE Int. Symposium on Inform. Theory (2007), 861–864.
22. R. Daskalov and P. Hristov, *New quasi-twisted degenerate ternary linear codes*, IEEE Trans. Inform. Theory, **49** (2003), 2259–2263.
23. R. Daskalov and P. Hristov, *New binary one-generator quasi-cyclic codes*, IEEE Trans. Inform. Theory **49** (2003), 3001–3005.
24. R. Daskalov and T.A. Gulliver, *New quasi-twisted quaternary linear codes*, IEEE Trans. Inform. Theory **46** (2000), 2642–2643.
25. R. Daskalov, E. Metodieva, and P. Khristov, *New bounds for the minimal distance of linear codes over* GF(9). *(Russian)* Problemy Peredachi Informatsii **40(1)** (2004), 15–26; translation in Probl. Inf. Transm. **40(1)** (2004), 13–24.
26. P. Diaconis and R. L. Graham, *The Radon transform on $\mathbb{Z}_2^k$*, Pacific J. Math., **118** (1985), 176–185.
27. S. Dodunekov, S. Guritman, and J. Simonis, *Some new results on the minimum length of binary linear codes of dimension nine*, IEEE Trans. Inform. Theory **45** (2003), 3001–3005.
28. I. Dumer, D. Micciancio and M. Sudan, *Hardness of approximating the minimum distance of a linear code.* In Proceedings of the 40th Annual Symposium on Foundations

of Computer Science (FOCS) (1999), 475-484.
29. I. Dumer, D. Micciancio, M. Sudan, *Hardness of approximating the minimum distance of a linear code*, IEEE Trans. Inform. Theory, **49** (2003), 22–37.
30. D. S. Dummit and R. M. Foote, *Abstract Algebra*, Princeton Hall, 1991.
31. M. R. Garey and D. S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness*, San Francisco, CA: Freeman (1979).
32. D. G. Glynn, T. A. Gulliver and M. K. Gupta, *On some quaternary self-orthogonal codes*, Ars Comb. (to appear).
33. M. Grassl, *Bounds on minimum distances of linear codes*, Available online at http://www.codetables.de.
34. M. Grassl and G. White, *New Codes from Chains of Quasi-cyclic Codes*, Proceedings 2005 IEEE Int. Symposium on Inform. Theory, (2005), 2095–2099.
35. T.A. Gulliver and V.K. Bhargava, *Some best rate 1/p and (p-1)/p quasi-cyclic codes over GF(3) and GF(4)*, IEEE Trans. Inform. Theory, **38(4)** (1992), 1369–1374.
36. T.A. Gulliver and V.K. Bhargava, *Two new rate 2/p binary quasi-cyclic codes*, IEEE Trans. Inform. Theory, **40(5)** (1994), 1667–1668.
37. T.A. Gulliver, *New Optimal Ternary Linear Codes*, IEEE Trans. Inform. Theory, **41** (1995), 1182–1185.
38. T. A. Gulliver and V. K. Bhargava, *New good rate (m-1)/pm ternary and quaternary quasi-cyclic codes*, Des. Codes Cryptogr. **7** (1996), 223–233.
39. R. W. Hamming, *Error-detecting and error-correcting codes*. Bell System Technical Journal. **29** (1950), 147-160.
40. A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane and P. Sole, *The Z_4-linearity of Kerdock, Preperata, Goethals, and related codes*, IEEE Trans. Inform. Theory **40(2)** (1994), 301–319.
41. R. Hill, and E. Kolev, *A survey of recent results on optimal linear codes*, in Combinatorial designs and their applications (F. C. Holroyd, K. A. S. Quinn, C. Rowley, and B. S. Webb eds), Chapman & Hall/CRC, Boca Raton, London New York Washington DC (1999).
42. W. C. Huffman, and V. Pless, *Fundamentals of error-correcting codes*, Cambridge University Press (2003).
43. K. Lally, and P. Fitzpatrick, *Algebraic structures of quasicyclic codes*, Disr. Appl. Math, **111** (2001), 157–175.
44. I. Landjev, A. Rouseva, T. Maruta, and R. Hill, *On optimal codes over the field with five elements*, Des. Codes Cryptogr. **29** (2003), 165–175.
45. D. S. Johnson, *The NP-completeness column: An ongoing guide*, J. Algorithms, **3** (1982), 182–195.
46. D. S. Johnson, *The NP-completeness column: An ongoing guide*, J. Algorithms, **7** (1986), 584–601.
47. D. E. Knuth, *The Art of Computer Programming, Vol. 4: Combinatorial Algorithms, Pre-Fascicle 2C*, to be published
48. R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*, Cambridge University Press (1986).
49. R. Lidl and G. Pilz, *Applied abstract algebra*, Springer (1998).
50. S. Litsyn, *Table of non-linear binary codes*, Available online at http://www.eng.tau.ac.il/∼litysn/tableand/index.html.
51. A. Lobstein and G. D. Cohen, *Sur la complexité d'un probléme de codage*, Theor. Informatics Appl., **21** (1987), 25–32.
52. H. Lüneburg, *Gray-Codes, Abh. Math. Sem. Hamburg*, Heidelberg, Germany: Springer-Verlag **52** (1982), 208–227.

53. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*, North Holland, New York (1977).
54. B. D. McKay, *AutosonA distributed batch system for Unix workstation networks (version 1.3)*, Canberra: Comput. Sci. Dept., Australian Nat. Univ., Tech. Rep. TR-CS-96-03, 1996.
55. A. A. Nechaev, *Kerdock code in cyclic form*, Disc. Math. (USSR), **1** (1989) 123–139 (in Russian). English translation: Disc. Math. and Appl., **1** (1991) 364–384.
56. V. Pless and N. J. Pierce, *Self dual codes over GF(q) satisfy a modified Varshamov bound*, Information and Control, **23** (1973), 35-40.
57. V. Pless, J. S. Leon, and J. Fields, *All $\mathbb{Z}_4$ codes of Type II and length 16 are known*, J. Combin. Theory, Ser. A **78** (1997), 32–50.
58. *V. Pless, Introduction to the Theory of Error-Correcting Codes, Third Edition*, John Wiley & Sons, Inc (1998).
59. V. S. Pless and Z. Qian, *Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$*, IEEE Trans. Inform. Theory **42** (1996), 1594–1600.
60. V. Pless, *On the uniqueness of the Golay codes*, J. Combinatorial Theory, **5** (1968), 215-228.
61. E. M. Rains, *Optimal self-dual codes over $\mathbb{Z}_4$*, Disc. Math. **203** (1999), 215–228.
62. E. M. Rains and N. J. A. Sloane, *Self-dual codes*, in *The Handbook of Coding Theory*, (V. Pless and W. C. Huffman, Eds.), North-Holland, New York (1998).
63. F.S. Roberts, *Applied Combinatorics*, Englewood Cliffs, NJ: Prentice-Hall (1984).
64. S. Roman, *Coding and information theory, Graduate Texts in Mathematics* 134, Springer-Verlag, (1992).
65. S. Roman, *Field theory, Graduate Texts in Mathematics* 158, Springer-Verlag (1995).
66. C. E. Shannon, *A mathematical theory of communication*, Bell Syst. Tech. J. **27** (1948), 379–423, 623–656.
67. W. Z. Shetter, *This essay is redundant.*(2000) Available: http://mypage.iu.edu/ shetter/miniatures/redund.htm
68. I. Siap, N. Aydin and D. K. Ray-Chaudhuri, *New ternary quasi-cyclic codes with better minimum distances*, IEEE Trans. Inform. Theory, **46** (2000) 1554–1558.
69. I. Siap, N. Aydin, and D. Ray-Chaudhuri, *New 1-generator quasi-twisted codes over GF(5), in Codes and Association Schemes*, Piscataway, NJ (1999); DIMACS Ser. Discrete Math. Theoret. Comput. Sci., Amer. Math. Soc., Providence, RI (2001), 265–275.
70. I. Siap, *New codes over GF(8)*, Ars Comb, **71** (2004), 239–247.
71. J. Stern, *Approximating the number of error locations within a constant ratio is NP-copmplete*, Lecture Notes on Computer Science, **673** (1993), 325–331.
72. T. M. Thompson, *From error correcting codes through sphere packings to simple groups*, The Mathematical Association of America (1983).
73. M. van Dijk, M. Egner, S. Greferath, M. Wassermann, *On two doubly even self-dual binary codes of length 160 and minimum weight 24*, IEEE Trans. Inform. Theory **51** (2005), 408–411.
74. J. H. van Lint, *Introduction to Coding Theory*, Springer (1999).
75. A. Vardy, *Algorithmic complexity in coding theory and the minimum distance problem*, In Proceedings of the twenty-ninth annual ACM Symposium on Theory of computing, STOC'97,El Paso, Texas (1997) 92–109.
76. A. Vardy, *The intractability of computing the minimum distance of a code*, IEEE Trans. Inform. Theory, **43(6)** (1997), 1757–1766.
77. J. Walker, *A new approach to the main conjecture on algebraic-geometric MDS codes*, Des. Codes and Cryptogr., **45(1)** (1996), 115–120.

78. Z. X. Wan, *Quaternary Codes*, Singapore: World Scientific (1997).
79. Greg White and Markus Grassl, *A New Minimum Weight Algorithm for Additive Codes*, IEEE International Symposium on Information Theory, (2006), 1119–1123.

1.10. Key Concepts in the Chapter

(1) *A linear code* of length n over a field F is a vector subspace of F^n.

(2) *A self-dual code* C is a linear code whose dual $C^\perp$ code is equal to itself, where the dual code is defined by

$$C^\perp := \{\mathbf{v} \in F^n \mid \langle \mathbf{u}, \mathbf{v} \rangle = 0 \text{ for all } \mathbf{u} \in C\}.$$

(3) *A parity check matrix* of a linear code C is a matrix whose null space is C.

(4) *A generator matrix* of a linear code C is a matrix whose row space is C.

(5) *Hamming distance* between $\mathbf{u} = (u_1, u_2, \ldots, u_n), \mathbf{v} = (v_1, v_2, \ldots, v_n)$ in F^n is $d(\mathbf{u}, \mathbf{v}) = |\{i : u_i \neq v_i\}|$, the number of positions in which $\mathbf{u}$ and $\mathbf{v}$ differ.

(6) *A perfect code* is a code for which the sphere packing bound is attained with equality. If the code parameters are $(n, M, d)_q$ then $M \cdot \sum_{j=0}^{t} \binom{n}{j} (q-1)^j = q^n$, where $t = \lfloor \frac{d-1}{2} \rfloor$. For a linear code $[n, k, d]_q$ the equality becomes $\sum_{j=0}^{t} \binom{n}{j} (q-1)^j = q^{n-k}$

(7) *An MDS code* (maximum distance separable code) is code for which the singleton bound is attained. For a linear code $[n, k, d]$ this means $d = n - k + 1$. For a non-linear code with parameters $(n, M, d)_q$ it means $M = q^{n-d+1}$

(8) *A cyclic code* C is a linear code which is closed under cyclic shifts, i.e., if $(u_0, u_1, \ldots, u_{n-1}) \in C$, then $(u_{n-1}, u_0, \ldots, u_{n-2}) \in C$. A cyclic code of length n over $\mathbb{F}_q$ is an ideal in the ring $\dfrac{\mathbb{F}_q[x]}{\langle x^n - 1 \rangle}$

(9) *A quasi-twisted code* (more precisely an l-quasi-twisted code) is a linear code of length $n = ml$ that is closed under the quasi-twisted shifts by l-positions, i.e., if $(c_0, c_1, \ldots, c_{n-1}) \in C$ then $(a \cdot c_{0-l}, \ldots, a \cdot c_{(l-1)-l}, c_{l-l}, \ldots, c_{n-l-1}) \in C$ where the subscripts are taken $\mod n$.

(10) *An n-th root of unity* over $\mathbb{F}_q$ is an element in an extension field of $\mathbb{F}_q$ that is a root of $x^n - 1$. A primitive n-th root of unity ω is an n-th root of unity such that $\omega^k \neq 1$ for any $k < n$.

(11) *A quadratic residue* $\mod p$ is an integer a such that a is relatively prime with p and the equation $x^2 \equiv a \mod p$ has a solution in $\mathbb{Z}_p$.

1.11. Solution to Exercises

(1) Most of these properties follow from the definition and the observation that the minimum distance between two vectors $u = (u_1, u_2, ..., u_n)$ and $v = (v_1, v_2, ..., v_n)$ is $d(u, v) = \sum_{i=1}^{n} d(u_i, v_i)$. So, you can argue component-wise. For example, show that the triangle inequality holds for each component (i.e. $d(u_i, v_i) \leq d(u_i, w_i) + d(w_i, v_i)$) by considering cases where $d(u_i, v_i) = 0$ or 1, then summing up all inequalities for all components.

(2) If the minimum distance is d, $d-1$ or fewer changes cannot change a codeword into another. Similarly, if there are at most $\lfloor \frac{d-1}{2} \rfloor$ then the resulting vector (after errors) will remain closest to the original vector. (One can use the triangle inequality to formally prove this)

(3) For C_2 the minimum distance and minimum weight are both equal to 3. For C_1, the minimum weight is 2 but the minimum distance is 3. Let C be a linear code. Consider the sets $D = \{d(\mathbf{u}, \mathbf{v}) : \mathbf{u}, \mathbf{v} \in C, \mathbf{u} \neq \mathbf{v}\}$ and $W = \{w_H(\mathbf{u}) : \mathbf{u} \in C, \mathbf{u} \neq \mathbf{0}\}$. Using linearity we can show that every number in the set S appears in W and vice versa. Then the minimums of the sets S and W are equal. Let $\mathbf{u}, \mathbf{v} \in C$ such that $\mathbf{u} \neq \mathbf{v}$. Let $\mathbf{w} = \mathbf{u} - \mathbf{v}$, then $w_H(\mathbf{w}) = d(\mathbf{u}, \mathbf{v})$, $\mathbf{w} \in C$ (by linearity of C) and $\mathbf{w} \neq \mathbf{0}$. Conversely, every weight $w_H(\mathbf{u})$, $\mathbf{u} \neq \mathbf{0}$ can be written as the distance $d(\mathbf{u}, \mathbf{0})$.

(4) Let C be a linear code of dimension k. Then it has a basis $\{v_1, v_2 \ldots, v_k\}$ with k elements. Every element of C has a unique representation as a linear combination $a_1v_1 + a_2v_2 + \cdots + a_kv_k$, where each a_i has q possible values. Therefore, the total number of such linear combinations is q^k.

(5) The proof of this lemma is based on the following observation: Let H be a $k \times n$ matrix with columns $h_1, h_2, \ldots, h_n$ so, write H as $H = [h_1, \ldots, h_n]$. Let $v = (v_1, \ldots, v_n)$ be a vector, then the product $H \cdot v$ gives the linear combination $v_1h_1 + v_2h_2 + \cdots + v_nh_n$. We proceed by contradiction. Suppose there is a non-zero vector v of weight less than d in C. Let v have non-zero components at positions $i_1, i_2, \ldots, i_r$ where $0 < r < d$. Then, we have $H \cdot v = 0$ hence $v_{i_1}h_{i_1} + v_{i_2}h_{i_2} + \cdots + v_{i_r}h_{i_r} = 0$. This means that the set $h_{i_1}, h_{i_2}, \ldots, h_{i_r}$ of $r < d$ columns is linearly dependent, but this contradicts the assumption. Hence there is no codeword of weight less than d. On the other hand, existence of a set of s linearly dependent columns implies the existence of a codeword of weight d. To show that the minimum distance of C_2 is 3, note that there is

no duplication among the columns of H_2, hence no two columns are linearly dependent, and there is a set of 3 columns that is linearly dependent (e.g. first, second and last)

(6) $\Rightarrow$: Let f be a polynomial of degree 2 or 3 over a field F and suppose f is irreducible, yet it has a root a in F. Then, $(x-a)|f$, and so $f(x) = (x-a)g(x)$ for some polynomial g where $\deg(g(x)) = \deg(f(x)) - 1 \geq 1$. That means f is reducible, contradicting the hypothesis.

$\Leftarrow$: Suppose f has no roots in f yet it is reducible over F. Then $f(x) = r(x)s(x)$ where both r and s have degree ≥ 1. Since degree of f is 2 or 3, one of r and s must have degree 1, i.e. must be a linear polynomial of the form $ax + b$. However, every linear polynomial over a field has a root. So, either r or s will have a root, and that root will also be a root of f. This is a contradiction again, completing the proof.

For a counterexample to the theorem for polynomials of degree 4 or higher, consider $(x^2 + 1)^2$ over $\mathbb{Z}_3$ or over reals. It is reducible (obviously) yet has no root in either field.

(7) Note $m = o_{11}(3) = 5$. Therefore the splitting field of $x^{11} - 1$ over $\mathbb{F}_3$ is $\mathbb{F}_{3^5}$. So we need a primitive polynomial of order 5. We are given that $f(x) = x^5 + 2x + 1$ is one such polynomial. Let α be a root of $f(x)$. Then it is a primitive element of $\mathbb{F}_{3^5}$ and $\omega = \alpha^{242/11} = \alpha^{22}$ is a 11-th root of unity over $\mathbb{F}_3$. To find the irreducible factors of degree 5 of $x^{11} - 1$ over $\mathbb{F}_3$, we compute the minimal polynomials
$m_1(x) = (x - \omega)(x - \omega^3)(x - \omega^4)(x - \omega^5)(x - \omega^9) = x^5 + x^4 + 2x^3 + x^2 + 2$
$m_2(x) = (x - \omega^2)(x - \omega^6)(x - \omega^7)(x - \omega^8)(x - \omega^{10}) = x^5 + 2x^3 + x^2 + 2x + 2$
Therefore;
$x^{11} - 1 = (x - 1)(x^5 + x^4 + 2x^3 + x^2 + 2)(x^5 + 2x^3 + x^2 + 2x + 2)$.

(8) The parameters are $[15, 7, 5]$. Note that this is an optimal code. By looking at the cyclotomic cosets from Example 1.2, we see that the generator polynomial must have degree 8, hence the dimension of the code is 7. From the table of best known codes, the minimum distance cannot be more than 5. Since we know that it is at least 5, it is therefore exactly 5.

(9) First, performing a permutation if necessary, we can assume that $\alpha_i = \alpha^i$ for $0 \leq i \leq n - 1$ where α is a primitive element of $\mathbb{F}_q$. Given a codeword $(f(\alpha^0), f(\alpha), f(\alpha^2) \ldots, f(\alpha^{n-1}))$ for some $f(x) \in P_k$, we need to show that its

cyclic shift $(f(\alpha^{n-1}), f(\alpha^0), \ldots, f(\alpha^{n-2}))$ is also a codeword. This means that $(f(\alpha^{n-1}), f(\alpha^0), \ldots, f(\alpha^{n-2})) = (g(\alpha^0), g(\alpha^1) \ldots, g(\alpha^{n-1}))$ for some $g(x) \in P_k$. It is easy to verify that the polynomial $g(x) = f(\alpha^{-1}x)$ satisfies this condition.

(10) A code with parameters $[n, k, 2t + 1]$ is perfect if the equality $q^{n-k} = \sum_{j=0}^{t} \binom{n}{j} (q-1)^j$ holds. For the binary Golay code G_{23} this means $2^{11} = \sum_{j=0}^{3} \binom{23}{j} = 1 + 23 + 253 + 1771$, which holds true.

For the ternary Golay code G_{11} this means $3^5 = \sum_{j=0}^{2} \binom{11}{j} 2^j = 1 + 11 \cdot 2 + 4 \cdot \frac{11 \cdot 10}{2}$, which also holds true.

(11) Let $q = 5$, $n = 26$ and $a = 2$ (or 3). Therefore we are considering constacyclic codes of length 26 over $\mathbb{F}_5$ with $a = 2$ or 3. The order, r, of 2 in $\mathbb{F}_5^*$ is 4. So we have

$$x^{26} - 2 = \prod_{i=0}^{25} (x - \delta^{4i+1})$$

where δ is a primitive $26 \cdot 4 = 104 - th$ root of unity. The exponents
$\{1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61, 65, 69, 73, 77, 81, 85, 89,$
$93, 97, 101\}$
of δ in this factorization are partitioned into the following cyclotomic cosets:
$\{1, 5, 21, 25\}, \quad \{9, 17, 45, 85\}, \quad \{13, 65\}, \quad \{29, 41, 89, 101\}$
$\{33, 61, 69, 97\}, \quad \{37, 49, 81, 93\}, \quad \{53, 57, 73, 77\}$
and the corresponding powers of ζ, where ζ is a primitive $26 - th$ root of 1, are
$\{0, 1, 5, 6\}, \quad \{2, 4, 11, 21\}, \quad \{3, 16\}, \quad \{7, 10, 22, 25\}, \quad \{8, 15, 17, 24\}$
$\{9, 12, 20, 23\} \quad \{13, 14, 18, 19\}.$
Let $g(x)$ be the polynomial of smallest degree which has $\zeta^i, 13 \leq i \leq 19$ among its roots (hence the roots of $g(x)$ are precisely ζ^i where i runs through cyclotomic cosets containing 3,8 and 13) . Then $g(x)|(x^{26} - 2)$ and $degg(x) = 8$. Hence the constacyclic code generated by $g(x)$ has length 26, dimension 16, and minimum distance ≥ 8. According to the linear codes table these are the *optimal* parameters. (Consequently, minimum distance is exactly 8)

Index