Lecture Notes in Mathematics

Finite Fields and Error-Correcting Codes

Karl-Gustav Andersson

(Lund University)

(version 1.013 - 16 September 2015)

Translated from Swedish by Sigmundur Gudmundsson

Contents

CHAPTER 1

Finite Fields

1. Basic Definitions and Examples

In this introductory section we discuss the basic algebraic operations *addition* and *multiplication* from an abstract point of view. We consider a set A equipped with two operations defined in such a way that to each pair of elements $a, b \in A$ there are associated two new elements $a + b$ and $a \cdot b$ in A called the *sum* and the *product* of a and b, respectively. We assume that for the sum we have the following four axioms.

(A1) $$a + (b + c) = (a + b) + c$$

(A2) $$a + b = b + a$$

(A3) there exists an element $0 \in A$ such that

$$a + 0 = a \quad \text{for all } a \in A$$

(A4) for every $a \in A$ there exists an element $-a \in A$ such that

$$a + (-a) = 0.$$

These axioms guarantee that *subtraction* is well-defined in A. It is easily checked that (A1)–(A4) imply that the equation $a + x = b$ in A has the unique solution $x = b + (-a)$. In what follows we will write $b - a$ for $b + (-a)$.

The corresponding axioms for the multiplication are

(M1) $$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

(M2) $$a \cdot b = b \cdot a$$

(M3) there exists an element $1 \in A$ such that

$$1 \cdot a = a \cdot 1 = a \quad \text{for all } a \in A$$

(M4) for every $a \neq 0$ in A there exists an element $a^{-1} \in A$ such that

$$a \cdot a^{-1} = 1.$$

Sometimes we will only assume that some of these axioms for the *multiplication* are satisfied. If they all apply then, precisely as for the subtraction, a division is well-defined in A i.e. the equation $ax = b$ with $a \neq 0$ has the unique solution $x = a^{-1} \cdot b$.

Finally, we always assume the distributive laws for A:

(D) $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$

Definition 1.1. A *ring* A is a set equipped with an addition and a multiplication such that all the rules (A1)–(A4) are satisfied and furthermore (M1) and (D). If A also satisfies (M2) it is said to be a *commutative ring* and if (M3) is fulfilled we say that the ring has a *unity.* A ring that contains at least two elements and satisfies all the rules (M1)–(M4) for the multiplication is called a *field.*

Example 1.2. The rational numbers $\mathbb{Q}$, the reals $\mathbb{R}$ and the complex numbers $\mathbb{C}$ are important examples of fields, when equipped with their standard addition and multiplication. The integers $\mathbb{Z}$ form a commutative ring but are not a field since (M4) is not valid in $\mathbb{Z}$.

Example 1.3. The set $M_2(\mathbb{R})$ of 2×2 real matrices forms a ring. Here 0 is the zero matrix and 1 is the unit matrix. In $M_2(\mathbb{R})$ the commutative law (M2) is not satisfied. The rule (M4) is not fulfilled either, since there exist non-zero matrices that are not invertible. For example we have

$$\begin{pmatrix} 1 & -2 \\ -2 & 4 \end{pmatrix} \begin{pmatrix} 4 & -2 \\ 2 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

It follows from this relation that none of the two matrices on the left-hand side are invertible.

Definition 1.4. Two elements $a \neq 0$ and $b \neq 0$ in a ring are called *zero divisors* if $a \cdot b = 0$.

Example 1.5. The two matrices

$$\begin{pmatrix} 1 & -2 \\ -2 & 4 \end{pmatrix} \text{ and } \begin{pmatrix} 4 & -2 \\ 2 & -1 \end{pmatrix}$$

in Example 1.3 are zero divisors in the ring $M_2(\mathbb{R})$.

We shall now discuss, in more detail, a family of rings that will play an important role in what follows. Let $n \geq 2$ be a given integer. We say that two integers a and b are *congruent modulo* n if their difference $a-b$ is divisible by n. For this we simply write $a \equiv b \pmod{n}$. For example we have $13 \equiv 4 \pmod{3}$. Denote by $[a]$ the class of integers that are congruent to a modulo n. We can then define an addition and a multiplication of such congruence classes by

$$[a]+[b]=[a+b] \quad \text{and} \quad [a]\cdot[b]=[a\cdot b].$$

Here we must verify that these definitions do not depend on the choice of representatives for each congruent class. So assume that $a \equiv a_1 \pmod{n}$ and $b \equiv b_1 \pmod{n}$. Then $a_1 = a + kn$ and $b_1 = b + ln$ for some integers k and l. This implies that

$$a_1+b_1 = a+b+(k+l)n \quad \text{and} \quad a_1b_1 = ab+(al+bk+kln)n,$$

hence a_1+b_1 is congruent with $a+b$ and a_1b_1 with ab modulo n. Denote by $\mathbb{Z}_n$ the set of congruence classes modulo n i.e.

$$\mathbb{Z}_n = \{[0],[1],[2],\dots,[n-1]\}.$$

It is easily checked that the above defined addition and multiplication turn $\mathbb{Z}_n$ into a commutative ring.

Example 1.6. In the ring $\mathbb{Z}_{11}$ we have

$$[5]+[9]=[14]=[3] \quad \text{and} \quad [5]\cdot[9]=[45]=[1]$$

and in $\mathbb{Z}_{12}$ the following equalities hold

$$[4]+[9]=[13]=[1] \quad \text{and} \quad [4]\cdot[9]=[36]=[0].$$

As a direct consequence of the example we see that $[5]$ is the multiplicative inverse of $[9]$ in the ring $\mathbb{Z}_{11}$. The following result gives a criteria for an element of $\mathbb{Z}_n$ to have a multiplicative inverse.

Theorem 1.7. *Let $[a]$ in $\mathbb{Z}_n$ be different from $[0]$. Then there exists an element $[b]$ in $\mathbb{Z}_n$ such that $[a][b]=[1]$ if and only if a and n are relatively prime i.e. they do not have a non-trivial common divisor.*

Proof. Let us first assume that a and n have a common divisor $d \geq 2$. Then $a = kd$ and $n = ld$ for some integers k and l with $0 < l < n$. This implies that $[l][a] = [lkd] = [kn] = [0]$. Hence there does not exist a multiplicative inverse $[b]$ to $[a]$, because in that case

$$[l]=[l][1]=[l][a][b]=[0][b]=[0].$$

On the other hand, if a and n are relatively prime then it is a consequence of the Euclidean algorithm that there exist integers b and c such that $1 = ab + nc$. This gives $[1] = [a][b]$. □

Example 1.8. We will now use the Euclidean algorithm to determine whether or not [235] has a multiplicative inverse in $\mathbb{Z}_{567}$.

$$\begin{aligned}
567 &= 2\cdot 235 + 97\\
235 &= 2\cdot 97 + 41\\
97 &= 2\cdot 41 + 15\\
41 &= 3\cdot 15 - 4\\
15 &= 4\cdot 4 - 1
\end{aligned}$$

This shows that 567 and 235 are relatively prime, and by following the calculations backwards we see that

$$1 = 4\cdot 4 - 15 = 4\cdot(3\cdot 15 - 41) - 15 = 11\cdot 15 - 4\cdot 41 = \cdots = 63\cdot 567 - 152\cdot 235.$$

Hence the multiplicative inverse of [235] is $[-152] = [415]$.

If $n = p$ is a prime, then it is clear that none of the numbers $1, 2, \ldots, p-1$ has a common divisor with p. This shows that all the classes $[1], [2], \ldots, [p-1]$ in $\mathbb{Z}_p$, different from [0], have a multiplicative inverse, so $\mathbb{Z}_p$ is a field. If n is not a prime, then $n = kl$ for some integers $k, l \geq 2$. Then none of the two classes $[k]$ and $[l]$ has an inverse in $\mathbb{Z}_n$, so $\mathbb{Z}_n$ is not a field. We summarize:

Theorem 1.9. *The ring $\mathbb{Z}_n$ is a field if and only if n is a prime.*

We conclude this section by defining the notion of an isomorphism between rings. Let A_1 and A_2 be two rings and assume that there exists a bijective map f from A_1 to A_2 such that

$$f(a+b) = f(a) + f(b) \quad \text{and} \quad f(a\cdot b) = f(a)\cdot f(b)$$

for all elements a and b in A_1. In that case, we say that the rings A_1 and A_2 are *isomorphic* and that f is an *isomorphism* from A_1 to A_2. Two rings that are isomorphic are actually just two different representations of the same ring. An isomorphism corresponds to just changing the names of the elements. All calculations in one of the rings correspond to exactly the same calculations in the other.

Example 1.10. Let M be the ring of all 2×2 matrices of the form

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

where a and b are real numbers and the operations are the standard matrix addition and matrix multiplication. Then the map

$$M \ni \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mapsto a + ib \in \mathbb{C}$$

defines an isomorphism from M to the ring $\mathbb{C}$ of complex numbers. The reader is encouraged to check this fact.

Exercises

Exercise 1.1. Show that the following rules are valid in any ring:

(1) $0 \cdot a = a \cdot 0 = 0$, (*Hint*: $0 \cdot a + 0 \cdot a = 0 \cdot a$.)

(2) $(-a)b = a(-b) = -ab$,

(3) $(-a)(-b) = ab$.

Exercise 1.2. Show that a field does not have any zero divisors.

Exercise 1.3. Show that if a is not a zero divisor in the ring A then the following cancelation law applies

$$ax = ay \Rightarrow x = y$$

for all x and y in A.

Exercise 1.4. Let M be the set of all matrices

$$\begin{pmatrix} a & 2b \\ -b & a \end{pmatrix},$$

where a and b are integers. Show that, with the standard matrix addition and multiplication, M forms a commutative ring with unity. Does M have any zero divisors?

Exercise 1.5. Let $\mathbb{Q}[\sqrt{2}]$ be the set of all numbers of the form $a + b\sqrt{2}$, where a and b are rational. Show that the usual addition and multiplication of real numbers turn $\mathbb{Q}[\sqrt{2}]$ into a field.

Exercise 1.6. Let $\mathbb{Z}[i]$ be the set of Gaussian integers $a + ib$, where a and b are integers. Show that $\mathbb{Z}[i]$, with the usual addition and multiplication of complex numbers, is a commutative ring with unity. For which elements $u \in \mathbb{Z}[i]$ does there exist a multiplicative inverse v i.e. an element v such that $uv = 1$?

Exercise 1.7. Show that a ring A is commutative if and only if

$$(a + b)^2 = a^2 + 2ab + b^2$$

for all a and b in A.

Exercise 1.8. Find out if the determinant

$$\begin{vmatrix} 325 & 131 & 340 \\ 142 & 177 & 875 \\ 214 & 122 & 961 \end{vmatrix}$$

is an odd number or an even one.

Exercise 1.9. Solve in $\mathbb{Z}_{23}$ the equations

$$[17]\cdot x = [5] \quad \text{and} \quad [12]\cdot x = [7].$$

Exercise 1.10. Determine if [121] and [212] are invertible in $\mathbb{Z}_{9999}$ or not. Find the inverses if they exist.

Exercise 1.11. Consider the elements [39], [41], [46] and [51] in $\mathbb{Z}_{221}$.

(1) Which of these are zero divisors?
(2) Which have a multiplicative inverse? Find the inverses if they exist.

Exercise 1.12. Solve the following systems of equations

$$\begin{cases} 4x+7y & \equiv 3 \pmod{11} \\ 8x+5y & \equiv 9 \pmod{11} \end{cases}, \qquad \begin{cases} 4x+7y & \equiv 5 \pmod{13} \\ 7x+5y & \equiv 8 \pmod{13} \end{cases}.$$

Exercise 1.13. Determine the digits x and y such that the following decimal numbers are divisible by 11

$$2x653874 \quad , \quad 37y64943252.$$

(*Hint*: $10^n \equiv (-1)^n \pmod{11}$.)

Exercise 1.14. Let A be a *finite* commutative ring with a unity. Show that if $a \in A$ is not a zero divisor, then a has a multiplicative inverse. (*Hint*: Consider the map $x \mapsto ax\ ,\ x \in A$.)

Exercise 1.15. Let a be a non-zero element in a field A.

(1) Show that if $a^{-1} = a$, then either $a = 1$ or $a = -1$.
(2) Prove *Wilson's theorem* stating that for every prime p we have

$$(p-1)! \equiv -1 \pmod{p}.$$

2. Calculations with Congruences

Let F be a finite field with q elements and $F^* = \{x \in F\ ;\ x \neq 0\}$. We order the elements of F^* in a sequence $x_1, x_2, \dots, x_{q-1}$. Then for every fixed $a \in F^*$ the sequence $ax_1, ax_2, \dots, ax_{q-1}$ contains exactly the same elements i.e. those of F^*, since if $ax_i = ax_j$ then multiplication by a^{-1} gives $x_i = x_j$. We have therefore shown that

$$\prod_{i=1}^{q-1}(ax_i) = \prod_{i=1}^{q-1} x_i\ .$$

By collecting a from each of the different factors on the left-hand side and dividing by $\prod_{i=1}^{q-1} x_i$, we obtain $a^{q-1} = 1$ and have thereby proven the following result.

Theorem 2.1. *Let F be a finite field with q elements and $a \neq 0$ be an element of F. Then*

$$a^{q-1} = 1.$$

Specializing to the case when $F = \mathbb{Z}_p$, for some prime p, we obtain the following result due to Pierre de Fermat in 1640:

Theorem 2.2 (Fermat's little theorem)**.** *If p is a prime number and a is an integer not divisible by p, then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Example 2.3. We now want to calculate the least positive remainder when dividing 3^{350} by 17. Since 17 is a prime, Fermat's theorem tells us that $3^{16} \equiv 1 \pmod{17}$. Hence

$$3^{350} = 3^{21 \cdot 16 + 14} \equiv 3^{14} \pmod{17}.$$

A continued calculation modulo 17 gives

$$3^{14} = 9^7 = 9 \cdot 81^3 \equiv 9 \cdot (-4)^3 = 9 \cdot (-4) \cdot 16 \equiv 9 \cdot (-4) \cdot (-1) = 36 \equiv 2.$$

The remainder that we are looking for is therefore 2.

Alternatively, one can show that $3^{14} \equiv 2$ by observing that $3^{14} \cdot 3^2 = 3^{16} \equiv 1$. This implies that $[3^{14}] = [9]^{-1} = [2]$, since $2 \cdot 9 = 18 \equiv 1$.

The next result generalizes Fermat's little theorem.

Theorem 2.4. *Let p and q be different prime numbers and m be a positive integer. Then*

$$a^{m(p-1)(q-1)+1} \equiv a \pmod{pq}$$

for every integer a.

Proof. If p does not divide a, then it follows from Fermat's theorem that

$$a^{p-1} \equiv 1 \pmod{p}.$$

This implies that

$$a^{m(p-1)(q-1)} \equiv 1 \pmod{p}.$$

Multiplication by a gives

$$a^{m(p-1)(q-1)+1} \equiv a \pmod{p}.$$

This equality is of course also valid when p divides a, since then $a \equiv 0 \pmod{p}$. In the same way, we see that

$$a^{m(p-1)(q-1)+1} \equiv a \pmod{q}.$$

Since both p and q divide the difference $a^{m(p-1)(q-1)+1} - a$ so does the product pq and the statement is proven. □

Example 2.5. Theorem 2.4 has an interesting application in cryptology. Assume that a receiver, for example a bank, receives messages from a large number of senders and does not want the content to be read by unauthorized individuals. Then the messages must be encrypted. This means that an encrypting key must me available to the sender. One way to achieve this is to use a system with a *public key*. Such systems are based on the idea that there exist functions that are easily computed but the inverse operation is very difficult without some additional information. The following method (the RSA-system) was suggested by Rivest, Shamir and Adelman in 1978.

Choose two large[1] different primes p and q and set $n = pq$. Then pick a large number d relatively prime to $(p-1)(q-1)$. According to Theorem 1.7 of the last section, d has a multiplicative inverse e in the ring $\mathbb{Z}_{(p-1)(q-1)}$, which can be determined by the Euclidean algorithm. The numbers n and e are made public as well as necessary information on how they should be used for the encrypting. The numbers p, q and d are kept secret by the receiver.

Assume that all the messages are of the form of one or more integers between 1 and n. A sender interested in sending such a number M will encrypt it by calculating $C \equiv M^e \pmod{n}$. After receiving C, the receiver calculates the unique number D between 1 and n satisfying $D \equiv C^d \pmod{n}$. According to Theorem 2.4 we have the equality $D \equiv M \pmod{n}$. Indeed, since e is the multiplicative inverse of d in the ring $\mathbb{Z}_{(p-1)(q-1)}$, it follows that $ed = m(p-1)(q-1)+1$ for some integer m, so

$$D \equiv C^d \equiv M^{ed} = M^{m(p-1)(q-1)+1} \equiv M \pmod{n}.$$

Now the interesting question is, if it is possible to use only the public information e and n to get hold of the content of the message sent. To do this within a reasonable amount of time one would need to know the prime numbers p and q. These can be determined by factorizing n. Even with our modern computers this should in general be an impossible task.

In the next example we deal with the problem of finding a simultaneous solution to several different congruences.

Example 2.6. In a 2000 years old book by the Chinese author Sun-Tsu one can read:

[1] By large numbers we here mean numbers with hundreds of digits.

“There exists an unknown number which divided by 3 leaves the remainder 2, by 5 the remainder 3 and by 7 the remainder 2. What is this number?”

In other words, one should find an integer x that simultaneously solves the three congruences

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 2 \pmod 7. \end{aligned}$$

The method that Sun-Tsu presented for solving the problem gives the Chinese remainder theorem.

Theorem 2.7. *Assume that the integers $n_1, n_2, \ldots, n_k$ are pairwise relatively prime. Then the system of congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\cdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

has a unique solution x modulo $n = n_1 n_2 \cdots n_k$.

Proof. Define

$$N_i = \frac{n}{n_i} = \prod_{j \neq i} n_j.$$

Then the numbers N_i and n_i are relatively prime for each i. Hence there exist integers s_i and t_i such that

$$s_i N_i + t_i n_i = 1.$$

Set

$$x = \sum_{j=1}^{k} a_j s_j N_j = a_1 s_1 N_1 + \cdots + a_k s_k N_k.$$

We have $s_i N_i \equiv 1 \pmod{n_i}$ and $N_j \equiv 0 \pmod{n_i}$ when $j \neq i$. This implies that

$$x \equiv a_i \pmod{n_i} \quad , \quad i = 1, \ldots, k.$$

We still have to show that the solution x is uniquely determined modulo n. Assume that $\tilde{x}$ was another solution. Then $x \equiv \tilde{x} \pmod{n_i}$ for all i. Since the numbers n_i are pairwise relatively prime, it follows that $x \equiv \tilde{x} \pmod{n}$ and the result follows. □

Example 2.8. In the last example we have $n_1 = 3$, $n_2 = 5$, $n_3 = 7$ and $N_1 = 35$, $N_2 = 21$, $N_3 = 15$. We find

$$\begin{aligned} 2 \cdot 35 - 23 \cdot 3 &= 1 \\ 1 \cdot 21 - \ \ 4 \cdot 5 &= 1 \\ 1 \cdot 15 - \ \ 2 \cdot 7 &= 1. \end{aligned}$$

So the above method gives the solution

$$x = 2 \cdot 2 \cdot 35 + 3 \cdot 1 \cdot 21 + 2 \cdot 1 \cdot 15 = 233.$$

The least positive solution is

$$233 - 2n = 233 - 210 = 23.$$

The Chinese remainder theorem has another, a bit more abstract, formulation. If $A_1, \dots, A_k$ are k rings, then we can form a new ring denoted by $A_1 \times \cdots \times A_k$ consisting of all elements $(a_1, \dots, a_k)$ where $a_i \in A_i$. The addition and the multiplication in the new ring are defined by

$$\begin{aligned} (a_1, \dots, a_k) + (b_1, \dots, b_k) &= (a_1 + b_1, \dots, a_k + b_k) \\ (a_1, \dots, a_k) \cdot (b_1, \dots, b_k) &= (a_1 \cdot b_1, \dots, a_k \cdot b_k). \end{aligned}$$

Assume now that $n = n_1 n_2 \cdots n_k$ where the numbers n_i are pairwise relatively prime. Then the Chinese remainder theorem states that for given integers $a_1, \dots, a_k$ with $0 \leq a_i < n_i$, there exists precisely one integer a with $0 \leq a < n$ such that

$$a \equiv a_i \pmod{n_i} \quad , \quad i = 1, \dots, k.$$

It is easily checked that the map that takes a to $(a_1, \dots, a_k)$ is an isomorphism between $\mathbb{Z}_n$ and $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$.

Example 2.9. Let $n = 1001 = 7 \cdot 11 \cdot 13$ and consider the two elements $[778]$ and $[431]$ in $\mathbb{Z}_{1001}$. Then

$$\begin{aligned} 778 &\equiv 1 \pmod{7} & 431 &\equiv 4 \pmod{7} \\ 778 &\equiv 8 \pmod{11} & 431 &\equiv 2 \pmod{11} \\ 778 &\equiv 11 \pmod{13} & 431 &\equiv 2 \pmod{13}. \end{aligned}$$

Instead of calculating the product $778 \cdot 431$ modulo 1001, we can also calculate

$$(1, 8, 11) \cdot (4, 2, 2) = (4, 16, 22) \equiv (4, 5, 9)$$

in the ring $\mathbb{Z}_7 \times Z_{11} \times Z_{13}$ and then, as in the proof of the Chinese remainder theorem, determine the corresponding element in $\mathbb{Z}_{1001}$. This sort of arithmetic is sometimes useful when performing this type of calculations with large numbers.

Exercises

Exercise 2.1. Find the multiplicative inverse of [45] in $\mathbb{Z}_{101}$. Then determine the integer x between 1 and 100 such that

$$45^{99} \equiv x \pmod{101}\,.$$

Exercise 2.2. In each of the following cases, find the least non-negative integer x satisfying

$$\begin{aligned} x &\equiv 3^{5000} \pmod{13}, & x &\equiv 3^{100} \pmod{101}, \\ x &\equiv 3^{40} \pmod{23}, & x &\equiv 2^{1000} \pmod{7}. \end{aligned}$$

Exercise 2.3. Show that if p and q are different primes, then

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}.$$

Exercise 2.4. Let $p_1, p_2, \dots, p_k$ be different primes and r be a positive integer divisible by $p_i - 1$ for all $i = 1, \dots, k$. Show that

$$a^{r+1} \equiv a \pmod{p_1 \cdot p_2 \cdots p_k}$$

for all integers a.

Exercise 2.5. Show that all integers n satisfy

(1) $n^7 \equiv n \pmod{42}$,
(2) $n^{13} \equiv n \pmod{2730}$.

(*Hint*: Use the result from Exercise 2.4.)

Exercise 2.6. Find the least positive integer M, such that

$$M^{49} \equiv 21 \pmod{209}.$$

Exercise 2.7. Show that if p is a prime and m is a positive integer, then

$$a^{(p-1)p^{m-1}} \equiv 1 \pmod{p^m}$$

for all integer a not divisible by p. (*Hint*: Copy the proof of Theorem 2.1 with F^* equal to the set of all invertible elements in $\mathbb{Z}_{p^m}$.)

Exercise 2.8. Show that all odd integers k satisfy

(1) $k^4 \equiv 1 \pmod{16}$,
(2) $k^{2^n} \equiv 1 \pmod{2^{n+2}}$ where $n \geq 2$.

Exercise 2.9. Find all integers x such that

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 3 \pmod{7} \\ x \equiv 7 \pmod{16}\,. \end{cases}$$

Exercise 2.10. Find the least positive integer x satisfying

$$\begin{cases} 2x \equiv 9 \pmod{11} \\ 7x \equiv 2 \pmod{19}\,. \end{cases}$$

Exercise 2.11. Verify that

$$\begin{cases} 95 \equiv 3 \pmod{23} \\ 95 \equiv 2 \pmod{31} \end{cases}$$

and apply this to calculate $95^{36} \pmod{713}$.

3. Vector Spaces

Definition 3.1. A *vector space* (or a *linear space*) over a field F is a set V, containing an element denoted by $\underline{0}$, and for each pair $u, v \in V$ and each $\alpha \in F$ having a well-defined *sum* $u + v \in V$ and a *product* $\alpha u \in V$ such that the following rules are satisfied

(i) $$u + (v + w) = (u + v) + w$$

(ii) $$u + v = v + u$$

(iii) $$\alpha(\beta u) = (\alpha\beta)u$$

(iv) $$1u = u$$

(v) $$0u = \underline{0}$$

(vi) $$\alpha(u + v) = \alpha u + \alpha v$$

(vii) $$(\alpha + \beta)u = \alpha u + \beta u\,.$$

Remark 3.2. It follows from these rules that all the axioms for addition, (A1)–(A4) from Section 1, are satisfied in a vector space. From (iv) , (v) and (vii) we get

$$u + \underline{0} = 1u + 0u = (1 + 0)u = 1u = u$$

so (A3) applies. The axiom (A4) can be verified as follows

$$u + (-1)u = 1u + (-1)u = (1 + (-1))u = 0u = \underline{0}\,.$$

Remark 3.3. The elements of a vector space are often called *vectors*. In (v) we underlined the zero on the right-hand side to emphasize that it is a vector. In what follows, we will simply denote also the zero vector by 0.

The basic theory for vector spaces over a general field F is the same as for the special case when $F = \mathbb{R}$. A number of vectors $u_1, \dots, u_l$ in

V are said to be *linearly dependent* if there exist $\alpha_1, \ldots, \alpha_l \in F$, not all zero, such that

$$\alpha_1 u_1 + \cdots + \alpha_l u_l = 0 \, .$$

We say that $u_1, \ldots, u_l$ are *linearly independent* if they are not linearly dependent. The vectors $u_1, \ldots, u_l$ *generate* the vector space V if every vector $u \in V$ is a *linear combination* of $u_1, \ldots, u_l$ i.e. if

$$u = \alpha_1 u_1 + \cdots + \alpha_l u_l$$

for some $\alpha_1, \ldots, \alpha_l \in F$. A *basis* for V is a collection of vectors $e_1, \ldots, e_n$ which are linearly independent and generate V. This is equivalent to the statement that every vector $u \in V$ can, in a unique way, be written as

$$u = \alpha_1 e_1 + \cdots + \alpha_n e_n,$$

where $\alpha_1, \ldots, \alpha_n \in F$. The coefficients $\alpha_1, \ldots, \alpha_n$ are called the *coordinates* of the vector u in the basis $e_1, \ldots, e_n$. Two different bases for a given vector space always contain equally many elements and a vector space is said to have the *dimension* n if it has a basis with n vectors. If a vector space V is generated by a finite number of vectors $v_1, \ldots, v_m$, then we can always pick a basis from these. If the vectors $v_1, \ldots, v_m$ are linearly independent then they form a basis. Otherwise, one of them, for example v_m, is a linear combination of the others. Then V is generated by $v_1, \ldots, v_{m-1}$. In this way, we can continue until we obtain a collection of linearly independent vectors which generate V.

Example 3.4. For a given field F the standard example of a vector space over F is its n-fold product

$$F^n = \{(\alpha_1, \ldots, \alpha_n) \; ; \; \alpha_i \in F\}$$

with addition and multiplication, by elements from F, in each component. Every vector space V over F of dimension n can be identified with F^n by choosing a basis in V.

Example 3.5. Let $\mathbf{f}$ be a *subfield* of a larger field F. This means that $\mathbf{f}$ is a subset of F and that $\mathbf{f}$ is itself a field with the same operations as defined in F. For this to be the case, it is necessary that $\mathbf{f}$ contains at least two elements, that the operations addition and multiplication applied to two elements in $\mathbf{f}$ again give an element in $\mathbf{f}$, and that $-\alpha$ and α^{-1} also belong to $\mathbf{f}$ for every $\alpha \neq 0$ in $\mathbf{f}$. In this case, we can think of F as a vector space over the subfield $\mathbf{f}$. It follows from the rules for F that the axioms (i)–(vii) for a vector space are satisfied. It is clear, that if we view the finite field F as a vector space over $\mathbf{f}$, then it is generated by a finite number of vectors. In other words there exists a basis $e_1, \ldots, e_n$ of elements in F such that every $u \in F$ can, in a unique way, be written as

$$u = \alpha_1 e_1 + \cdots + \alpha_n e_n$$

with $\alpha_1, \ldots, \alpha_n \in \mathbf{f}$. Here the dimension of F is n. If p is the number of elements in the subfield $\mathbf{f}$, then each coordinate α_i can be chosen in p different ways, so F has exactly p^n elements.

In connection with error-correcting codes, we will later deepen our discussion on vector spaces over finite fields. Here we just show how Example 3.5 can be used to see that the number of elements of a finite field must be a power of a single prime.

Let F be a finite field and as usual denote the unity in F by 1. Consider the sums

$$1\ ,\ 1+1\ ,\ 1+1+1\ ,\ \ldots\ ,\ m1\ ,\ \ldots$$

where $m1$ means the sum of m copies of the unity. Since F is finite, there exist integers $r < s$ such that $r1 = s1$. If $m = s - r$, then $m1 = 0$. The least positive integer p such that $p1 = 0$ is called the *characteristic* of the field F. The characteristic p must be a prime, since if p were the product of two integers p_1 and p_2 greater than 1 then

$$(p_1 1) \cdot (p_2 1) = p1 = 0$$

and hence $p_1 1 = 0$ or $p_2 1 = 0$. This contradicts the fact that p is the *least* positive integer with $p1 = 0$. Now set

$$\mathbf{f} = \{m1\ ;\ m \in Z\} = \{\ 0\ ,\ 1\ ,\ 1+1\ ,\ \ldots\ ,\ (p-1)1\ \}\ .$$

Then it is easily checked that $\mathbf{f}$ is a subfield of F and that the map $m \mapsto m1$ gives an isomorphism between $\mathbb{Z}_p$ and $\mathbf{f}$. Because $\mathbf{f}$ has p elements, it follows from Example 3.5 that the field F has p^n elements for some positive integer n. We can now formulate our result as the following theorem.

Theorem 3.6. *For every finite field F there exist a prime number p and a positive integer n such that the number of elements in F is p^n. The prime p is the characteristic of the field.*

Remark 3.7. The notion of a characteristic can also be defined for infinite fields, but here there are two cases. Either, there exists a least positive integer p such that $p1 = 0$ which we then call the characteristic, or the elements $m1$ are non-zero for all non-zero m. In the latter case we say that the characteristic is 0. As examples we have $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ which all are fields of characteristic 0.

Exercises

Exercise 3.1. Let V be a vector space over a field F. A subset U of V is called a *subspace* of V if

$$u, v \in U \Rightarrow \alpha u + \beta v \in U \quad , \quad \text{for all } \alpha, \beta \in F.$$

Check that every subspace U of V is a vector space with the same operations as in V.

Let F be the field $\mathbb{Z}_3$ and U be the subspace of F^4 generated by the vectors $(0,1,2,1)$, $(1,0,2,2)$ and $(1,2,0,1)$. Find a basis for U and determine its dimension.

Exercise 3.2. Let F be a field with characteristic $p \neq 0$.

(1) Show that $pa = 0$ for all $a \in F$.

(2) Show that

$$(a+b)^p = a^p + b^p$$

for all $a, b \in K$.

(*Hint*: Show first that for $0 < k < p$ the binomial coefficients $\binom{p}{k}$ are divisible by p.)

Exercise 3.3. (1) Show that for a field of characteristic $p \neq 0$

$$(a_1 + a_2 + \cdots + a_l)^p = a_1^p + a_2^p + \cdots + a_l^p \,.$$

(2) Prove Fermat's little theorem by choosing all $a_i = 1$ in (1).

4. Polynomial Rings

According to Theorem 3.6, any finite field must have p^n elements, where p is a prime number and n is some positive integer. So far, we have only dealt with the fields $\mathbb{Z}_p$ for which $n = 1$. To be able to construct fields with $n > 1$, we need to discuss polynomials with coefficients in finite fields.

A polynomial with coefficients in a field F is an expression of the form

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0, \tag{1}$$

where $a_i \in F$. Strictly speaking, a polynomial is just a finite sequence $a_0, a_1, \ldots, a_n$ of elements in F and the letter x should be seen as a *formal* symbol. The value $f(\alpha)$ of the polynomial f at $\alpha \in F$ is

$$a_n \alpha^n + a_{n-1} \alpha^{n-1} + \cdots + a_1 \alpha + a_0 \in F.$$

Example 4.1. Consider the polynomials

$$f(x) = x^3 + 1 \quad \text{and} \quad g(x) = x^4 + x^2 + x + 1$$

with coefficients in $\mathbb{Z}_2$ (observe that we do not write out the terms with coefficient 0). Despite the fact that the values of f and g are equal for all $\alpha \in \mathbb{Z}_2 = \{0, 1\}$, the polynomials should be considered as *different*.

If $a_n \neq 0$ in equation (1), then we say that the polynomial $f(x)$ is of degree n and $f(x)$ is said to be *monic* if $a_n = 1$. The set of all polynomials with coefficients in a field F is denoted by $F[x]$. The addition and multiplication of polynomials are defined as usual when the coefficients lie in $\mathbb{R}$ or $\mathbb{C}$. The division algorithm, the factor theorem and the Euclidean algorithm can be proven, in the general case, in exactly the same way as when $F = \mathbb{R}$. The division algorithm tells us that if f and g are polynomials such that deg $f \geq$ deg g, then there exist polynomials q and r such that

$$f(x) = q(x)g(x) + r(x),$$

where either $r(x)$ is the zero polynomial or deg $r <$ deg g. If r is the zero polynomial, then we say that g divides f and write $g|f$. The statement of the factor theorem is that $f(\alpha) = 0$ if and only if $(x - \alpha)$ divides $f(x)$. Finally, the Euclidean algorithm gives a method for finding a greatest common divisor of two polynomials f and g. That h is a greatest common divisor of f and g means that h divides both f and g, furthermore that any other polynomial that divides both f and g must divide h. The greatest common divisor is not uniquely determined, but two different greatest common divisors h_1 and h_2 only differ by a constant multiple. This follows from the fact that h_1 divides h_2 and h_2 divides h_1. This is only possible if $h_1 = ah_2$ for some $a \in F$. If we demand that the greatest common divisor of f and g is a monic polynomial, then it is uniquely determined and is denoted by (f, g).

Example 4.2. We will now illustrate the Euclidean algorithm by calculating the greatest common divisor of the following polynomials in $\mathbb{Z}_3[x]$:

$$f(x) = x^5 + 2x^3 + x^2 + 2, \qquad g(x) = x^4 + 2x^3 + 2x^2 + 2x + 1.$$

Observe that since the coefficients are in $\mathbb{Z}_3$, we can apply identities such as $4 \equiv 1$ and $2 \equiv -1$. (In what follows, we will leave out the brackets around elements in $\mathbb{Z}_n$.)

$$\begin{aligned} x^5 + 2x^3 + x^2 + 2 &= (x + 1)(x^4 + 2x^3 + 2x^2 + 2x + 1) + (x^3 + 1) \\ x^4 + 2x^3 + 2x^2 + 2x + 1 &= (x + 2)(x^3 + 1) + (2x^2 + x + 2) \end{aligned}$$

$$x^3 + 1 = (2x + 2)(2x^2 + x + 2).$$

The last non-vanishing remainder $2x^2 + x + 2$ is a greatest common divisor of f and g. The corresponding monic polynomial is obtained by multiplying by $2^{-1} = 2$. This gives $(f, g) = x^2 + 2x + 1$.

Definition 4.3. A polynomial $s(x)$ in $F[x]$ of degree $n \geq 1$ is said to be *irreducible* if it does not have a non-trivial divisor i.e. if there does not exist a polynomial $g(x)$, with $1 \leq \deg\, g < n$, that divides $s(x)$. Irreducible polynomials are also called *prime polynomials*.

Example 4.4. The polynomial $f(x) = x^3 + 2x + 1$ is irreducible in $\mathbb{Z}_3[x]$. To checking this, observe that if $f(x)$ were reducible then at least one if its factors would be of degree 1. Then $f(x)$ would necessarily have a zero in $\mathbb{Z}_3$, but this is not the case since $f(0) = 1$, $f(1) = 1$ and $f(-1) = 1$.

We will now prove that every monic polynomial in $F[x]$ can be written as a product of monic prime polynomials and that this product is unique up to the order of its factors. For this we need the following lemma.

Lemma 4.5. *Assume that f, g and h are three polynomials in $F[x]$ such that $f(x)$ divides the product $g(x)h(x)$. If f and g are relatively prime i.e. $(f, g) = 1$ then f divides h.*

Proof. It follows from the Euclidean algorithm that since $(f, g) = 1$ there exist two polynomials $c(x)$ and $d(x)$ such that

$$1 = c(x)f(x) + d(x)g(x).$$

Hence

$$h(x) = c(x)f(x)h(x) + d(x)g(x)h(x).$$

Both terms on the right-hand side are divisible by f so f must divide h. □

Theorem 4.6. *Let F be a field and $f(x)$ be a monic polynomial with coefficients in F. Then there exist a number of different monic prime polynomials $s_1(x), \dots, s_l(x)$ in $F[x]$ and positive integers $m_1, \dots, m_l$ such that*

$$f(x) = s_1(x)^{m_1} \cdots s_l(x)^{m_l}.$$

The prime polynomials s_i and the integers m_i are, up to order, uniquely determined.

Proof. We prove by induction, over the degree of f, that f can be written as a product of prime polynomials. When the degree of f is 1 there is nothing to prove. Now assume that the degree of f

is n and that the statement is correct for any polynomial of lower degree. If f is a prime polynomial we are done. Otherwise, we can write $f(x) = g_1(x)g_2(x)$ for some polynomials of g_1 and g_2 both of degree less than n. According to the induction hypothesis these can be written as a product of prime polynomials. This proves that f has a prime factorization.

What is left to prove is the uniqueness. Assume that we have two prime factorizations for $f(x)$

$$s_1(x)^{m_1} \cdots s_l(x)^{m_l} = t_1(x)^{n_1} \cdots t_j(x)^{n_j}. \tag{2}$$

Let us first consider $t_1(x)$. We shall show that $t_1(x)$ is equal to one of the factors $s_i(x)$ on the left-hand side. Since s_1 and t_1 are monic prime polynomials, we know that either $s_1 = t_1$ or s_1 and t_1 are relatively prime. If $s_1 = t_1$ we are done. Otherwise $s_1(x)^{m_1}$ and $t_1(x)$ are relatively prime. According to Lemma 4.5, $t_1(x)$ must then divide the product

$$s_2(x)^{m_2} \cdots s_l(x)^{m_l}.$$

We can now continue the same procedure. Either $t_1 = s_2$ or else divides $t_1(x)$ the product

$$s_3(x)^{m_3} \cdots s_l(x)^{m_l}.$$

Sooner or later we end up with $t_1(x) = s_i(x)$ for some i. We can then divide both sides of equation (2) by $t_1(x)$ and repeat the procedure now for $t_2(x)$. When we have, in this way, divided out all the factors $t_i(x)$ on the right-hand side, all the factors $s_i(x)$ on the left-hand side must have disappeared. Otherwise a product of such factors would be equal to 1, which is impossible. This proves the uniqueness of the prime factorization. □

For a given field F the set $F[x]$, equipped with the polynomial addition and the polynomial multiplication, forms a ring. As we have seen above, there are great similarities between $F[x]$ and the ring $\mathbb{Z}$ of integers. For both $\mathbb{Z}$ and $F[x]$ we have the division algorithm, the Euclidean algorithm and furthermore a unique prime factorization. The prime numbers in $\mathbb{Z}$ correspond to the prime polynomials in $F[x]$. We shall now copy the construction of the rings $\mathbb{Z}_n$ from $\mathbb{Z}$ to $F[x]$. Let $s(x)$ be a given non-zero polynomial with coefficients in F. Two polynomials $f(x)$ and $g(x)$ in $F[x]$ are said to be *congruent* modulo $s(x)$ if their difference $f(x) - g(x)$ is divisible by $s(x)$. For this we simply write $f \equiv g \pmod{s}$. Denote by $[f(x)]$ the class of polynomials which are congruent to $f(x)$ modulo $s(x)$. Then we define an addition and a multiplication by

$$[f(x)] + [g(x)] = [f(x) + g(x)] \quad \text{and} \quad [f(x)] \cdot [g(x)] = [f(x)g(x)].$$

In the same way as for the integers, one can check that these definitions are independent of the choice of the representatives for the congruence classes. Denote by

$$F[x]/(s(x))$$

the set of congruence classes modulo $s(x)$. It is easily checked that $F[x]/(s(x))$, equipped with this addition and this multiplication, is a commutative ring.

Example 4.7. For the ring $\mathbb{Z}_5[x]/(x^3+1)$ we have

$$\begin{aligned}[x^2+2x+1]\cdot[x^2+x+2] &= [x^4+3x^3+5x^2+5x+2] \\ = [x^4+3x^3+2] &= [(x+3)(x^3+1-1)+2] \\ = [(x+3)(-1)+2] &= [-x-1] = [4x+4].\end{aligned}$$

Observe that x^3 can always be substituted by -1, since we are calculating modulo x^3+1.

In analogy with the rings $\mathbb{Z}_n$ one can show that $F[x]/(s(x))$ is a field if and only if $s(x)$ is a prime polynomial. If $s(x)$ is not a prime polynomial, then $s(x) = s_1(x)s_2(x)$ for some polynomials s_1 and s_2 of positive degree. Then $[s_1(x)][s_2(x)] = 0$, so $F[x]/(s(x))$ has zero divisors and hence is not a field. If $s(x)$ is a prime polynomial, then $(f,s) = 1$ for every non-zero polynomial $f(x)$ of degree less than s. By the Euclidean algorithm there exist polynomials $c(x)$ and $d(x)$ such that

$$1 = c(x)f(x) + d(x)s(x).$$

This implies that $[1] = [c(x)][f(x)]$, so $[c(x)]$ is the inverse of $[f(x)]$. According to the division algorithm, every congruence class in $F[x]/(s(x))$ is represented by a polynomial of degree less than $s(x)$. This means that every non-zero element has an inverse, so $F[x]/(s(x))$ is a field.

Example 4.8. The polynomial x^2+1 is irreducible in the ring $\mathbb{R}[x]$ of polynomials with real coefficients. This means that

$$R[x]/(x^2+1)$$

is a field. Every congruence class is represented by a polynomial of degree one and if we apply $[x^2+1] = 0$, then we easily get

$$[a+bx][c+dx] = [(ac-bd)+(ad+bc)x]$$

With this we easily see that $\mathbb{R}[x]/(x^2+1)$ is isomorphic to the field $\mathbb{C}$ of complex numbers.

Exercises

Exercise 4.1. Let $f(x)$ be the polynomial $x^{214}+3x^{152}+2x^{47}+2$ in $\mathbb{Z}_5[x]$. Find the value $f(3)$ in $\mathbb{Z}_5$.

Exercise 4.2. Show that if $f(x)$ is a polynomial of degree n with coefficients in a field F, then f has at most n zeros in F.

Exercise 4.3. Determine the greatest common divisor (f,g) of the following polynomials in $\mathbb{Z}_2[x]$:

(1) $f(x)=x^7+1 \quad , \quad g(x)=x^5+x^3+x+1$.

(2) $f(x)=x^5+x+1 \quad , \quad g(x)=x^6+x^5+x^4+x+1$.

Exercise 4.4. Find the greatest common divisor $h=(f,g)$ of the polynomials $f(x)=x^{17}+1$ and $g(x)=x^7+1$ in $\mathbb{Z}_2[x]$ and determine two polynomials $c(x)$ and $d(x)$ such that

$$h(x)=c(x)f(x)+d(x)g(x).$$

Exercise 4.5. Show that there exists only one irreducible polynomial in $\mathbb{Z}_2[x]$ of degree two. Determine whether the polynomial x^5+x^4+1 in $\mathbb{Z}_2[x]$ is irreducible or not.

Exercise 4.6. Determine all monic irreducible polynomials in $\mathbb{Z}_3[x]$ of degree 2.

Exercise 4.7. Find in $\mathbb{Z}_3[x]$ the prime factorization for the following polynomials:

(1) $x^5+x^4+x^3+x-1$

(2) x^4+2x^2+2x+2

(3) x^4+1

(4) x^8+2.

Exercise 4.8. How many zero divisors do there exist in the ring $\mathbb{Z}_5[x]/(x^3+1)$?

Exercise 4.9. (1) Let F be a finite field. Show that the product of all non-zero elements in F is equal to -1. (*Hint*: Apply Theorem 2.1 and the relationship between zeros and coefficients.)

(2) Show that for every prime number p we have

$$(p-1)! = -1 \pmod{p}.$$

(Compare this result with Exercise 1.15.)

Exercise 4.10. Let F be a field with q elements, where $q=2m+1$ is odd. Show that $x\in F$ is the square of some non-zero element in F if and only if $x^m=1$. (*Hint*: Show first that $a^2=b^2$ implies that $a=b$ or $a=-b$ and then use Exercise 4.2.)

Exercise 4.11. Show that for a field with an even number of elements, every element is the square of one and only one element.

5. Finite Fields

Example 5.1. We shall here determine all irreducible polynomials in $\mathbb{Z}_2[x]$ of degree less than or equal to 4. There exist only two polynomials of degree 1, namely

$$x \quad \text{and} \quad x+1.$$

These are trivially irreducible. A polynomial of degree 2 or 3 is irreducible if and only if it has no zeros in $\mathbb{Z}_2$. It is easily checked that such a polynomial has no zeros exactly when it has an odd number of terms and the constant term is 1. This shows that the irreducible polynomials of degree 2 and 3 are exactly the following:

$$x^2+x+1$$

$$x^3+x^2+1 \quad \text{and} \quad x^3+x+1.$$

If a polynomial of degree 4 is irreducible, then necessarily it does not have a factor of degree 1, i.e. it does not have a zero in $\mathbb{Z}_2$, and it is not a product of two irreducible factors of degree 2. The second condition only excludes $(x^2+x+1)^2 = x^4+x^2+1$, since there only exists one prime polynomial of degree 2. The other polynomials in $\mathbb{Z}_2$ of degree 4 that do not have a zero are

$$x^4+x^3+1\,,\ x^4+x+1 \quad \text{and} \quad x^4+x^3+x^2+x+1.$$

These are all the prime polynomials in $\mathbb{Z}_2[x]$ of degree 4.

If $s(x)$ is any of the irreducible polynomials of degree 4 mentioned above, then $\mathbb{Z}_2[x]/(s(x))$ is a field with $2^4 = 16$ elements. This follows from the fact that every congruence class is represented by a unique polynomial of degree 3 and for this each coefficient can be chosen in exactly two ways, namely as 0 or 1. Any irreducible polynomial of degree 2 or 3 induces a field with $2^2 = 4$ or $2^3 = 8$ elements, respectively.

In the next section, we will show that for every prime number p and every positive integer n there exists an irreducible polynomial in $\mathbb{Z}_p[x]$ of degree n. As a direct consequence of this, there exists for each such p and n a field with p^n elements. We shall also show that any two finite fields with the same number of elements are isomorphic. This means that up to isomorphism there exists, for each prime p and each positive integer n, exactly one finite field with p^n elements. These fields are denoted by $GF(p^n)$ and called the Galois field of order p^n in honour of the French mathematician Évariste Galois (1811-1832). In this section we shall give examples of how to do calculations in finite fields.

Example 5.2. In order to find the multiplicative inverse of $[x^2+1]$ in the field $\mathbb{Z}_2[x]/(x^3+x^2+1)$ we apply the Euclidean algorithm:

$$\begin{aligned} x^3+x^2+1 &= (x+1)(x^2+1)+x \\ x^2+1 &= x\cdot x+1. \end{aligned}$$

This leads to (observe that $+ = -$ in $\mathbb{Z}_2$)

$$\begin{aligned} 1 &= (x^2+1)+x\cdot x = (x^2+1)+x((x^3+x^2+1)+(x+1)(x^2+1)) \\ &= (x^2+x+1)(x^2+1)+x(x^3+x^2+1). \end{aligned}$$

We end up with $[x^2+1]^{-1} = [x^2+x+1]$.

We will now turn our attention to calculations concerning powers. If a is a non-zero element of a finite field F then some of its power must be 1. We know for example from Theorem 2.1 that $a^{q-1}=1$, where q is the number of elements in F.

Definition 5.3. The *order* of a non-zero element a in a finite field is the least positive integer m such that $a^m=1$. We denote the order of a by $o(a)$.

Example 5.4. Here we determine the order of $[10]$ in the field $\mathbb{Z}_{73}$:

$$\begin{aligned} 10^2 &= 100 \equiv 27 \\ 10^3 &\equiv 270 \equiv -22 \\ 10^4 &\equiv -220 \equiv -1. \end{aligned}$$

This implies that $10^5 \equiv -10$, $10^6 \equiv -27$, $10^7 \equiv 22$ and $10^8 \equiv 1$. The order of $[10]$ is therefore 8.

According to Fermat's little theorem, we know that for any non-zero element a in the field $\mathbb{Z}_{73}$ we have $a^{72}=1$. The following result shows that it is not a coincidence that the order 8 in Example 5.4 divides 72.

Lemma 5.5. *Let a be a non-zero element in a finite field. If $a^n=1$ for some positive number n, then the order of a divides n.*

Proof. Assume the converse. If m is the order of a, then there exist integers q and r with $0<r<m$, such that

$$n = qm + r.$$

From this it follows that

$$1 = a^n = (a^m)^q \cdot a^r = a^r.$$

This contradicts the fact that $m = o(a)$, since $0<r<m$. □

The next result gives us a method for constructing elements of high order.

Lemma 5.6. *Assume that the elements a_1 and a_2 in a finite field have the orders m_1 and m_2, respectively, and that m_1 and m_2 are relatively prime. Then $a = a_1a_2$ has the order m_1m_2.*

Proof. Assume that $a^k = 1$. Then we have

$$1 = a^{km_1} = a_1^{km_1} \cdot a_2^{km_1} = a_2^{km_1}.$$

According to Lemma 5.5, m_2 must divide km_1. Since $(m_1, m_2) = 1$ the number m_2 must divide k. Using a similar argument, we see that m_1 divides k. This means that k is divisible by m_1m_2, since m_1 and m_2 are relatively prime. The order of a is therefore at least m_1m_2. That it is exactly m_1m_2 follows from

$$a^{m_1m_2} = (a_1^{m_1})^{m_2} \cdot (a_2^{m_2})^{m_1} = 1.$$

□

Example 5.7. In the field $\mathbb{Z}_{73}$ we have

$$8^2 = 64 \equiv -9$$
$$8^3 \equiv -72 \equiv 1$$

so the order of [8] is 3. According to Example 5.4 and Lemma 5.6 the order of $[80] = [7]$ is $8 \cdot 3 = 24$.

Before we can formulate the main result of this section we need the following lemma.

Lemma 5.8. *Let a and b be elements of a finite field F of order m and n, respectively, and assume that m does not divide n. Then there exists an element in F of order greater that n.*

Proof. If m does not divide n, then there exists a prime power p^k that divides m but not n. Then $m = m'p^k$ and $n = n'p^l$, where $0 \leq l < k$ and n' is not divisible by p. According to Lemma 5.6, this means that $(p^k, n') = 1$ and the order of $a^{m'} \cdot b^{p^l}$ is $p^k n' > n$. □

Theorem 5.9. *If F is a finite field with q elements, then there always exists an element in F of order $q - 1$.*

Proof. Let b be a non-zero element in F such that the order of b is larger than or equal to the order of any other element of F. Set $n = o(b)$. According to Lemma 5.8 the order of any element in F must divide n, since otherwise there would exist an element of order greater than n. This means that any non-zero element of F must satisfy the equation

$$x^n = 1.$$

The polynomial $x^n - 1$ has therefore $q-1$ different zeros. Following the factor theorem we therefore have $n \geq q-1$. On the other hand Theorem 2.1 tells us that the order never can be greater than $q-1$. Hence $n = q-1$ so we have proven the result. □

Definition 5.10. Let F be a field with q elements. An element of order $q-1$ in F is said to be a *primitive element.*

Example 5.11. We shall show that [3] is a primitive element for $\mathbb{Z}_{101}$. Since the order of [3] must divide $100 = 2^2 \cdot 5^2$, it is enough to check the powers 2, 4, 5, 10, 20, 25 and 50:

$$\begin{aligned}
3^2 &= 9 \\
3^4 &= 81 \equiv -20 \\
3^5 &\equiv -60 \\
3^{10} &\equiv 3600 \equiv -36 \\
3^{20} &\equiv 1296 \equiv -17 \\
3^{25} &\equiv 1020 \equiv 10 \\
3^{50} &\equiv 100 \equiv -1
\end{aligned}$$

The least positive integer m for which $3^m \equiv 1$ is therefore 100.

For a primitive element a in a field F with q element the powers

$$a^0, a^1, a^2, \dots, a^{q-2}$$

are all different. Otherwise we would have $a^j = a^k$ for some integers $j < k$ between 0 and $q-2$. Then $a^{k-j} = 1$, which contradicts the fact that the order of a is $q-1$. For every non-zero b in F there exists a uniquely determined j with $0 \leq j \leq q-2$ such that $b = a^j$. We call j the *index* of b and write $j = \mathrm{ind}(b)$. The index is also called the *discrete logarithm* of b with respect to the primitive element a. The index can be used to simplify calculations of products and quotients in finite fields. If the field has q elements then we have

$$\begin{aligned}
\mathrm{ind}(b_1 \cdot b_2) &\equiv \mathrm{ind}(b_1) + \mathrm{ind}(b_2) \pmod{q-1} \\
\mathrm{ind}(b_1 \cdot b_2^{-1}) &\equiv \mathrm{ind}(b_1) - \mathrm{ind}(b_2) \pmod{q-1}.
\end{aligned}$$

Example 5.12. We have seen in Example 5.1 that the polynomial $x^4 + x^3 + 1$ is irreducible $\mathbb{Z}_2[x]$. The field

$$F = Z_2[x]/(x^4 + x^3 + 1)$$

has $2^4 = 16$ elements. Each element in F can be described with a string of four binary digits given by the coefficients of the polynomial of degree 3 representing the congruence class. As an example, the string 1011 denotes the class $[x^3+x+1]$. The class $[x]$ is a primitive element in F and this induces a table containing each element in F^* :

index	0	1	2	3	4	5	6	7
element	0001	0010	0100	1000	1001	1011	1111	0111
index	8	9	10	11	12	13	14	
element	1110	0101	1010	1101	0011	0110	1100	

As an example, the calculation of the element of degree 5 goes as follows

$$\begin{aligned}[x^5] &= [x \cdot x^4] = [x \cdot (x^3+1)] = [x^4+x] \\ &= [(x^3+1)+x] = [x^3+x+1] .\end{aligned}$$

We illustrate how the table can be used by calculating

$$(1111) \cdot (1101)^{-1}.$$

The index for this element is

$$6 - 11 = -5 \equiv 10 \pmod{15}$$

Hence

$$(1111) \cdot (1101)^{-1} = (1010).$$

Exercises

Exercise 5.1. Determine all irreducible polynomials of degree 5 in $\mathbb{Z}_2[x]$.

Exercise 5.2. Prove that $\mathbb{Z}_3[x]/(x^3+x^2+2)$ is a field with 27 elements and determine the multiplicative inverse to $[x+2]$.

Exercise 5.3. Prove that $\mathbb{Z}_{11}[x]/(x^2+x+4)$ is a field and determine the multiplicative invers to $[3x+2]$. How many elements does the field have ?

Exercise 5.4. (1) Determine the order of the elements [3] and [4] in $\mathbb{Z}_{37}$. (2) Determine a primitive element in $\mathbb{Z}_{37}$.

Exercise 5.5. Determine a primitive element in $\mathbb{Z}_{73}$.

Exercise 5.6. (1) Show that $L = \mathbb{Z}_2[x]/(x^3+x+1)$ is a field. (2) Show that $[x]$ is a primitive element and calculate, as in Example 5.12, an index table for L. (3) Calculate $[x^2+1] \cdot [x^2+x+1]^{-1}$.

Exercise 5.7. Use the table in Example 5.12 to calculate the following

(1) $(1001) \cdot ((1011)^2 + (0011)^{-2})$,
(2) $((1010)^2 + (0101)^3) \cdot ((0001) + (1101)^2)^{-1}$.

6. The Existence and Uniqueness of $GF(p^n)$

To show that there exists a field with p^n elements we shall here prove that for each prime p and every positive integer n there exists an irreducible polynomial of degree n in $\mathbb{Z}_p[x]$. We start by noticing that the total number of monic polynomials

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

with coefficients in $\mathbb{Z}_p$ is equal to p^n. According to Theorem 6, every such polynomial can, in a unique way, up to the term order, be written as a product

$$f(x) = s_1(x)^{m_1} \cdots s_l(x)^{m_l}, \tag{3}$$

where $s_1(x), \dots, s_l(x)$ are monic prime polynomials in $\mathbb{Z}_p[x]$. If d_i is the degree of $s_i(x)$ then

$$n = m_1 d_1 + \cdots + m_l d_l. \tag{4}$$

The number of monic polynomials of degree n in $\mathbb{Z}_p[x]$ is equal to the number of ways, as in (3), to write monic polynomials of degree n as a product of prime polynomials. If I_d denotes the number of monic prime polynomials of degree d, then according to (4), the total number of monic polynomials of degree n in $\mathbb{Z}_p[x]$ is equal to the coefficient for t^n in the product

$$(1 + t + t^2 + \cdots)^{I_1}(1 + t^2 + t^4 + \cdots)^{I_2}(1 + t^3 + t^6 \cdots)^{I_3} \cdots \; .$$

Since we know that the number of these coefficients is equal to p^n , we have

$$\prod_d \left(\frac{1}{1 - t^d}\right)^{I_d} = \frac{1}{1 - pt} \quad .$$

By taking logarithms on each side we obtain

$$\sum_d -I_d \left(\ln(1 - t^d)\right) = -\ln(1 - pt)$$

and by Taylor expanding on both sides we get

$$I_1(t+\frac{t^2}{2}+\frac{t^3}{3}+\cdots)+I_2(t^2+\frac{t^4}{2}+\frac{t^6}{3}+\cdots)+I_3(t^3+\frac{t^6}{2}+\frac{t^9}{3}+\cdots)+\cdots$$
$$= pt + \frac{p^2t^2}{2} + \frac{p^3t^3}{3} + \cdots .$$

Comparing coefficients of each side for t^n gives

$$\sum_{d|n} I_d \cdot \frac{d}{n} = \frac{p^n}{n} .$$

Observe that on the left-hand side we only have terms where d divides n. Multiplying by n gives the following result:

Theorem 6.1. *If I_d is the number of monic irreducible polynomials of degree d in $\mathbb{Z}_p[x]$, then*

$$\sum_{d|n} dI_d = p^n.$$

Example 6.2. If $p = 2$ and $n = 6$ then we obtain

$$I_1 + 2I_2 + 3I_3 + 6I_6 = 2^6 = 64.$$

According to Example 5.1 we have $I_1 = 2$, $I_2 = 1$ and $I_3 = 2$, so $I_6 = 9$.

By applying Theorem 6.1 repeatedly we can, in this way, determine the numbers I_d. But to do this in one go, we will make use of the *Möbius inversion formula* proven in the next section.

The Möbius function $\mu(n)$ is defined for positive integers n and takes only three values 0, 1 and -1. It is given by

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^k & \text{if } n \text{ is the product of } k \textit{ different} \text{ primes} \\ 0 & \text{otherwise.} \end{cases}$$

If we apply the Möbius inversion formula to the equation in Theorem 6.1 then we get

$$nI_n = \sum_{d|n} \mu(d)p^{n/d}.$$

The right-hand side contains a lowest power of p. If the lowest power is p^m, then

$$\frac{nI_n}{p^m} = \pm 1 + (\text{a number of } p\text{-powers with coefficients } \pm 1).$$

Hence

$$\frac{nI_n}{p^m} = \pm 1 \pmod p$$

and in particular $nI_n \neq 0$.

Theorem 6.3. *For each prime number p and each positive integer n there exists an irreducible polynomial of degree n in $\mathbb{Z}_p[x]$.*

It is a direct consequence of Theorem 6.3 that there exists a field with p^n elements. We shall now focus our attention on proving that, up to isomorphisms, there exists only one such field.

Let F be an arbitrary finite field of characteristic p. Then F contains the subfield

$$\mathbf{f} = \{ \, 0 \, , \, 1 \, , \, \dots \, , \, (p-1)1 \, \}$$

which is isomorphic to $\mathbb{Z}_p$. If $m1 \in \mathbf{f}$ and $\beta \in F$, then $(m1) \cdot \beta = m\beta$. We can therefore consider F as a vector space over $\mathbb{Z}_p$. Since F is finite, this vector space is finite dimensional. This implies that for every $\alpha \in F$ there exists a positive integer d such that the powers

$$\alpha^0, \alpha^1, \alpha^2, \dots, \alpha^d$$

are linearly dependent, i.e. there exist $a_0, a_1, \dots, a_d \in \mathbb{Z}_p$ not all zero such that

$$a_0 1 + a_1\alpha + a_2\alpha^2 + \cdots + a_d\alpha^d = 0 \, .$$

Let d be the smallest such integer and set $s(x) = a_0 + a_1x + \cdots + a_dx^d$. Then $s(x)$ has the lowest degree amongst the non-trivial polynomials in $\mathbb{Z}_p[x]$ having α as a zero. We can always choose $a_d = 1$, and then $s(x)$ is uniquely determined and called the *minimal polynomial* to α. The minimal polynomial is irreducible in $\mathbb{Z}_p[x]$ because if $s(x)$ was a product $s_1(x)s_2(x)$ of factors of lower degree than d, then s_1 or s_2 would have α as zero and this would contradict the fact that $s(x)$ is the minimal polynomial of α.

Theorem 6.4. *Let F be a finite field of charateristic p and let α be an element of F. If L is the smallest subfield of F containing α and if $s(x)$ is the minimal polynomial to α, then L is isomorphic to the field $\mathbb{Z}_p[x]/(s(x))$.*

Proof. Set

$$L = \{f(\alpha) \; ; \; f \in \mathbb{Z}_p[x]\}.$$

Every subfield of F containing α must include L, since such a field contains all powers of α and all linear combinations of such powers. We shall show that L is isomorphic to the field $\mathbb{Z}_p[x]/(s(x))$. It follows from this that L itself is a field and hence the smallest subfield of F containing α. Consider the map

$$\mathbb{Z}_p[x]/(s(x)) \ni [f(x)] \mapsto f(\alpha) \in L.$$

It is well-defined since if f and g belong to the same congruence class i.e. if $f(x) = g(x) + h(x)s(x)$ for some polynomial h, then

$$f(\alpha) = g(\alpha) + h(\alpha)s(\alpha) = g(\alpha)\,.$$

It immediately follows from the definition that $[f(x)]+[g(x)]$ is mapped to $f(\alpha)+g(\alpha)$ and $[f(x)]\cdot[g(x)]$ to $f(\alpha)g(\alpha)$. It remains to show that the map is bijective. It is clear that it is surjective. To show that it is injective, we first observe that if the minimal polynomial $s(x)$ has degree d, then it is enough to consider polynomials $f(x)$ of degree less than d. Every congruence class in $\mathbb{Z}_p[x]/(s(x))$ is represented by such a polynomial. Assume that $f(\alpha) = g(\alpha)$ for two different polynomials of degree less than d. Then α is a zero of $f - g$, which contradicts the fact that $s(x)$ is the minimal polynomial of α. This shows that the map is injective and the statement is proven. □

Corollary 6.5. *Let F be a field with p^n elements and let $s(x)$ be a monic prime polynomial in $\mathbb{Z}_p[x]$ with zero α in F. Then $s(x)$ is the minimal polynomial of α and the degree of s divides n.*

Proof. The element α is a zero of both $s(x)$ and its minimal polynomial $t(x)$. Hence α is a zero to the greatest common divisor (s,t). Since s and t are irreducible, we must have $s = (s,t) = t$. If $s(x)$ has the degree d and L is the smallest subfield containing α, then Theorem 6.4 tells us that L has p^d elements. Because F can be seen as a vector space over L, we have

$$|F| = |L|^m$$

for some positive integer m, where $|F|$ and $|L|$ denote the number of elements in F and L, respectively. This means that

$$p^n = p^{dm}$$

and from this follows that d divides n. □

We now have all the tools needed to prove that two finite fields with the same number of elements must be isomorphic. Let F be an arbitrary field with $q = p^n$ elements. According to Theorem 2.1 every element in F is a zero of the polynomial $x^q - x$. We have multiplied the equation in the theorem by x to include $x = 0$. According to Theorem 4.6, $x^q - x$ can be written as a product of prime polynomials in $\mathbb{Z}_p[x]$:

$$x^q - x = \prod_i s_i(x). \tag{5}$$

Here is the sum of the degrees of the polynomials s_i equal to q. Since $x^q - x$ has q different zeros in F, the prime polynomials on the right-hand side must all be different and for each polynomial s_i its degree must be the number of its different zeros in F. The above corollary shows that the degree of the polynomial s_i divides n.

Let us now consider the formula in Theorem 6.1. It shows that the sum of the degrees of *all* prime polynomials in $\mathbb{Z}_p[x]$ dividing n is equal to p^n. This means that the product on the right-hand side of equation (5) must contain a prime polynomial the degree of which divides n. In particular, according to Theorem 6.3, the right hand-side of (5) must contain a prime polynomial of degree n. This is the minimal polynomial of each of its n zeros in F. Let α be such a zero. Then it follows from Theorem 6.4 that the smallest subfield of F containing α is isomorphic to the field $\mathbb{Z}_p[x]/(s(x))$ and consequently contains p^n elements. The field F is therefore isomorphic to $\mathbb{Z}_p[x]/(s(x))$. We have hereby proven the following result.

Theorem 6.6. *Let $s(x)$ be a prime polynomial of degree n in $\mathbb{Z}_p[x]$. Then every field with p^n elements is isomorphic to $\mathbb{Z}_p[x]/(s(x))$.*

Remark 6.7. In particular, we have shown that if s_1 and s_2 are two different prime polynomials of degree n in $\mathbb{Z}_p[x]$ then the fields $\mathbb{Z}_p[x]/(s_1(x))$ and $\mathbb{Z}_p[x]/(s_2(x))$ are isomorphic.

7. The Möbius Inversion Formula

Let us first remember the fact that the Möbius function $\mu(n)$ is defined for positive integers n, as 0 if n has multiple prime factors and as $(-1)^k$ if n is the product of k different primes. As a special case we have $\mu(1) = 1$.

Lemma 7.1.

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \textit{for } n = 1 \\ 0 & \textit{for } n > 1 \,. \end{cases}$$

Proof. When $n = 1$ the sum is equal to $\mu(1) = 1$. If $n > 1$ and $n = p_1^{m_1} \cdots p_r^{m_r}$ is the prime factorization of n, we set $n^* = p_1 \cdots p_r$. Then

$$\begin{aligned} \sum_{d|n} \mu(d) &= \sum_{d|n^*} \mu(d) \\ &= 1 - r + \cdots + (-1)^k \binom{r}{k} + \cdots + (-1)^r \binom{r}{r} \\ &= (1-1)^r \end{aligned}$$

$$= 0.$$

The binomial coefficients $\binom{r}{k}$ tell us how many different numbers d are products of k prime factors chosen amongst $p_1, \dots, p_r$. □

Theorem 7.2 (Möbius inversion formula)**.** *Let $f(n)$ and $g(n)$ be defined for positive integers n and assume that*

$$f(n) = \sum_{d|n} g(d)$$

for all n. Then

$$g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right).$$

Proof. It follows from

$$f\left(\frac{n}{d}\right) = \sum_{d'|\frac{n}{d}} g(d'),$$

that

$$\sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \sum_{d'|\frac{n}{d}} g(d') = \sum_{d'|n} g(d') \sum_{d|\frac{n}{d'}} \mu(d) = g(n).$$

For the last equality we have used Lemma 7.1, which gives

$$\sum_{d|\frac{n}{d'}} \mu(d) = \begin{cases} 1 & \text{if } d' = n \\ 0 & \text{if } d' < n\,. \end{cases}$$

□

CHAPTER 2

Error-Correcting Codes

1. Introduction

When transferring or storing information there is always a risk of errors occurring in the process. To increase the possibility of detecting and possibly correcting such errors, one can add a certain redundance to the text carrying the information, for example, in form of control digits. We shall now give two simple examples.

Example 1.1. Assume that a sender transmits a text which is divided into a number of six digit binary words. Each such word consists of six digits which each is either 0 or 1. To increase the possibility for a receiver to detect possible errors, that might have occurred during the transfer, to each word the sender can add the seventh binary digit in such a way that in each seven digit word there always is an even number of ones. If the receiver registers a word with an odd number of ones, then he will know that an error has occurred and can possibly ask the sender to repeat the message.

Example 1.2. If the receiver in Example 1.1 does not have the opportunity to ask for a repetition, the sender can proceed in a different way. Instead of adding the seventh digit he can send every six digit word three times in a row. If the three words are not identical when they reach the receiver, he will know that an error has occurred and could try to correct it at each place by choosing a digit that occurs at the corresponding places in at least two of the received words. He can of course not be completely sure that the erroneous word has been corrected, but if the probability for more than one error to occur is low, then the chances are good.

One disadvantage of the method in Example 1.2 is that, compared with the original text, the message with the error-correcting mechanism takes three times as long to send. Hence it seems a worthwhile exercise to find more effective methods and this is the purpose of the theory of error-correcting codes. This was started off by the work of Shannon, Golay and Hamming at the end of the 1940s and has since evolved rapidly using ever more sophisticated mathematical methods. Here the theory of finite fields plays a particularly important role.

For writing a text we must have an *alphabet.* This is a finite set F of symbols called *letters.* As is common in coding theory, we assume that F is a finite field. When $F = \mathbb{Z}_2$, as in the above examples, the code is said to be *binary.* A *word* is a finite sequence $x_1x_2 \dots x_m$ of letters. We shall here only deal with so called *block codes*. This means that the words are all of the same length m and can therefore be seen as elements in the vector space F^m . When appropriate, we write the words as vectors $x = (x_1, \dots, x_m)$ in F^m. A *coding function* E *is* an injective map

$$E : F^m \to F^n$$

from F^m into a vector space F^n of higher dimension i.e. $m < n$. The image $C = E(F^m)$ is what we call a *code.* To improve the possibility for detecting and correcting errors, it is useful that the elements of the code C lie far apart from each other in F^n. This to minimize the probability that a sent code word is received erroneously as a different code word.

Definition 1.3. The Hamming distance $d(x, y)$ between two vectors $x = (x_1, \dots, x_n)$ and $y = (y_1, \dots, y_n)$ in F^n is defined as the number of coordinates i where $x_i \neq y_i$.

Example 1.4. In the space $\mathbb{Z}_2^5$ the Hamming distance satisfies $d(10111, 11001) = 3$ and in $\mathbb{Z}_3^4$ we have $d(1122, 1220) = 2$.

Remark 1.5. If it is equally likely that an erroneously received letter is any other letter from the alphabet, then the Hamming distance is a natural measure for how big the error is. In some situations, other measures are more appropriate, but here we will only deal with the Hamming distance.

Definition 1.6. Let C be a code in F^n. Then we define its separation $d(C)$ as the least distance between two different words in the code i.e.

$$d(C) = \min\{d(x, y) \; ; \; x, y \in C \; , \; x \neq y\}.$$

Theorem 1.7. *Let C be a code with separation $d(C)$.*

1. *If $d(C) \geq k + 1$ then C can detect up to k errors in each word.*
2. *If $d(C) \geq 2k + 1$ then C can correct up to k errors in each word.*

Remark 1.8. The consequence of (2) is that if $d(C) \geq 2k + 1$ then, for each word containing at most k errors, there exists a uniquely determined closest code word. We assume that the erroneous word is corrected by picking instead the closest word in the code. For practical purposes, it is of great importance to find effective algorithms correcting errors and the existence of such algorithms can be a strong argument for the choice of a particular code. In the following we will focus on how to construct codes with high separation and not on error-correcting algorithms.

Proof of Theorem 1.7. (1) If $d(C) \geq k+1$, then any two code words are different at at least $k+1$ places. A received word with at most k letters wrong cannot be a code word and is therefore detected as erroneous.

To prove (2) we assume that x is a received word different from a code word y at most k places. If z was another code word with this property then the triangular inequality gives $d(y,z) \leq d(y,x) + d(x,z) \leq 2k$. This contradicts the assumption that $d(C) \geq 2k+1$. This means that we can correct x to y. □

If we are interested in constructing a code $C = E(F^m)$ in F^n with a given separation $\sigma = d(C)$, then there is a natural limit for which m we can choose. We shall now give a theoretical estimate of the largest possible value of m.

Definition 1.9. For every non-negative integer r we define the sphere $S(x,r)$, with centre $x \in F^n$ and radius r, by

$$S(x,r) = \{y \in F^n;\ d(x,y) \leq r\}.$$

Lemma 1.10. *If F has q elements then the sphere $S(x,r)$ contains exactly*

$$\binom{n}{0} + \binom{n}{1}(q-1) + \binom{n}{2}(q-1)^2 + \cdots + \binom{n}{r}(q-1)^r$$

words.

Proof. The result follows from the fact that if $0 \leq j \leq r$, then there exist $\binom{n}{j}(q-1)^j$ words which have exactly j coordinates different from x. □

Theorem 1.11. *Assume that F has q elements, that the code C in F^n contains M words and has separation $2k+1$. Then*

$$M\left[\binom{n}{0} + \binom{n}{1}(q-1) + \cdots + \binom{n}{k}(q-1)^k\right] \leq q^n. \tag{6}$$

Proof. The spheres of radius k and centre in *different* code words in C cannot intersect, since $d(C) = 2k+1$. Because the number of elements in F^n is q^n, the result then follows from Lemma 1.10. □

Remark 1.12. If $C = E(F^m)$ then $M = q^m$.

Remark 1.13. The inequality (6) is called the *sphere packing bound* or the *Hamming bound*. In case of equality, the corresponding code C is said to be *perfect*. For such a code, every word y in F^n lies in exactly one sphere $S(x, k)$ with x in C.

Exercises

Exercise 1.1. In Examples 1.1 and 1.2 we defined two coding functions from $\mathbb{Z}_2^6$ to $\mathbb{Z}_2^7$ and $\mathbb{Z}_2^{18}$, respectively. Determine the separation for the corresponding codes. Compare the result with Theorem 1.11.

Exercise 1.2. Let $\sigma > 0$ be an *odd* integer and C be a code in $\mathbb{Z}_2^n$ with M words and separation σ. Show that there exists a code $\widehat{C}$ in $\mathbb{Z}_2^{n+1}$ with M words and separation $\sigma + 1$. (*Hint*: Compare with Example 1.1)

Exercise 1.3. Construct a code in $\mathbb{Z}_2^8$ with 4 words and separation 5.

Exercise 1.4. Show that there does not exist a code in $\mathbb{Z}_2^{12}$ with 2^7 words and separation 5.

2. Linear Codes and Generating Matrices

Definition 2.1. A code C in F^n is said to be *linear* if it is a linear subspace of F^n. If the dimension of C is m then it is called an $[n, m]$ code.

Remark 2.2. That C is a linear subspace of F^n means that every linear combination of vectors in C is also contained in C. Then C is itself a vector space with the same operations as F^n, so the dimension of C is well-defined.

In practice, most error-correcting codes are linear or can be obtained from linear ones. A great advantage of linear codes is that it is much easier to determine their separation than in the general case.

Remark 2.3. By the weight $w(x)$ of a code word $x = (x_1, \dots, x_n)$ in F^n we mean the number of coordinates in x that are different from zero. The weight $w(C)$ of a linear code C in F^n is defined by

$$w(C) = \min\{w(x);\ x \in C\ ,\ x \neq 0\}.$$

Theorem 2.4. *For a linear code C the separation $d(C)$ is equal to its weight $w(C)$.*

Proof. A linear code that contains the two words x and y also contains their difference $x - y$. The result follows from the fact that the Hamming distance $d(x, y)$ is equal to the weight $w(x - y)$. □

Remark 2.5. If we are interested in determining the separation for a general code containing M words, then we must, in principle, determine $M(M-1)/2$ different Hamming distances, one for each pair in the code. For a linear code, it is enough to calculate the weight of the $M - 1$ non-zero code words.

Definition 2.6. A *generator matrix* for a linear $[n, m]$ code C in F^n is a $m \times n$ matrix G, with elements in F, such that its rows form a basis for C.

Example 2.7. Consider the following 3×7 matrix with elements in $F = \mathbb{Z}_3$

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 2 & 2 & 1 & 1 & 2 \\ 2 & 1 & 2 & 1 & 2 & 1 & 2 \end{bmatrix}.$$

By subtracting the first row from the second and adding the first to the third, we obtain the matrix

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 2 & 0 & 2 & 0 & 2 & 0 \end{bmatrix}.$$

Multiplying the third row by 2 gives

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

Finally, subtracting both the second and the third row from the first yields

$$\widetilde{G} = \begin{bmatrix} 1 & 0 & 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

The rows of $\widetilde{G}$ generate the same subspace of F^7 as the rows of G, because we can write the rows in one matrix as a linear combination of the rows of the other. The two matrices G and $\widetilde{G}$ are therefore generator matrices for the same code C in F^7. We now observe that the first three columns of $\widetilde{G}$ are columns in the identity matrix of order 3. If we interchange the second and the third columns of $\widetilde{G}$ we get

$$\begin{bmatrix} 1 & 0 & 0 & 2 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix} .$$

This matrix generates a code C' in F^7 that is obtained from C by interchanging the letters in position 2 and 3 for all words in C.

Definition 2.8. Two codes C and C' in F^n are said to be *equivalent* if there exists a permutation π of the numbers $1, \dots, n$ such that

$$C' = \{x_{\pi(1)}x_{\pi(2)} \dots x_{\pi(n)} \ ; \ x_1x_2 \dots x_n \in C\} .$$

Remark 2.9. If two codes C and C' are equivalent then their separations are equal i.e. $d(C) = d(C')$.

The ideas presented in Example 2.7 can be applied to prove the following theorem.

Theorem 2.10. *Every linear $[n, m]$ code C is equivalent to a code with a generator matrix of the form*

$$[I_m \mid A]$$

where I_m is the identity matrix of order m and A is an $m \times (n - m)$ matrix.

Definition 2.11. When a generator matrix for a linear code takes the form as in Theorem 2.10 we say that it is of *normal form.*

Let $G = [I_m \mid A]$ be the generator matrix, of a linear $[n, m]$ code C in F^n, of normal form. If the elements in F^m and F^n are seen as row matrices, then the map

$$F^m \ni x \mapsto xG \in F^n$$

gives a natural linear coding function. The first m letters in the word xG are given by x in K^m and the last $n - m$ letters (control digits) by xA.

Exercises

Exercise 2.1. Construct generator matrices for the codes in Examples 1.1 and 1.2.

Exercise 2.2. Let C be a binary linear code with the generator matrix

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

List all the code words in C and determine the separation for C.

Exercise 2.3. The matrix

$$\begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{bmatrix}$$

is a generator matrix for a linear code C in $\mathbb{Z}_3^4$. Determine all the code words in C and the separation $d(C)$. Then show that the code C is perfect.

Exercise 2.4. Let C be a binary linear code with generator matrix

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

Find a generator matrix for C of normal form.

Exercise 2.5. Prove Theorem 2.10 by showing that every $m \times n$ matrix G, with elements in a field F and linearly independent rows, can be transformed into a matrix of the form $[I_m \mid A]$ by repeated use of the following operations:

(1) multiplication of a row with an element in F
(2) addition of a row to another one
(3) swopping two columns.

(*Hint*: Use induction over the number of rows in G)

3. Control Matrices and Decoding

Definition 3.1. The scalar product $< x, y >$ of two vectors $x = (x_1, \dots, x_n)$ and $y = (y_1, \dots, y_n)$ in F^n is defined by

$$<x, y> = x_1 y_1 + \cdots + x_n y_n.$$

Definition 3.2. The *dual* code $C^\perp$ of a linear code C in F^n is the linear code

$$C^\perp = \{y \in F^n; <x, y> = 0 \text{ for all } x \in C\}.$$

Remark 3.3. As for subspaces in $\mathbb{R}^n$, it is easy to show that if the code C in F^n has dimension m, then the dual code $C^\perp$ is of dimension $n - m$. For vector spaces F^n over a finite field F, it is *not* true in general that every vector in F^n can, in a unique way, be written as the sum of a vector in C and a vector in $C^\perp$. It can even happen that $C^\perp = C$. In that case the code is said to be *self-dual.*

Example 3.4. For the matrix

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{bmatrix}$$

the scalar product of the first row with itself is 3, the scalar product of the second row with itself is 6, and the scalar product of the two rows is 3. This means that each scalar product is 0 modulo 3. From this we see that the $[4, 2]$ code over $\mathbb{Z}_3$ with generator matrix G is self-dual.

Definition 3.5. A generator matrix for the dual code $C^\perp$ of C is called a *control matrix* for C.

A word $x \in F^n$ is contained in the code C if and only if the scalar product of x and any row of a control matrix for C is zero. In this way we can easily check if a word belongs to the code or not.

If G is a generator matrix for an $[n, m]$ code C and H is a control matrix for C, then G is an $m \times n$ matrix and H is an $(n - m) \times n$ matrix of rank $(n - m)$. The condition that H is a control matrix for C can be written as

$$G \cdot H^t = 0, \tag{7}$$

where H^t denotes the transpose of the matrix H. The content of equation (7) is namely that the scalar product of the rows of G and the rows of H are zero.

Let us now assume that the generator matrix G is of normal form $[I_m \mid A]$, where A is an $m \times (n - m)$ matrix. If we then choose

$$H = [-A^t \mid I_{n-m}],$$

then it is easily verified that condition (7) is satisfied. We now formulate this as the following theorem.

Theorem 3.6. *If a linear $[n, m]$ code C has the generator matrix $[I_m \mid A]$, then $[-A^t \mid I_{n-m}]$ is a control matrix for C.*

Remark 3.7. If the field F is $\mathbb{Z}_2$, then $-A^t = A^t$ so we can take $[A^t \mid I_{n-m}]$ as a control matrix.

Example 3.8. The binary $[5, 2]$ code which has the generator matrix

$$G = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

has as control matrix

$$H = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

We shall now describe how a receiver can apply a control matrix H of a linear code C to correct errors that possibly have occurred during the transfer of information when using the code C. We start by checking if the received word $x \in F^n$ satisfies the condition $xH^t = 0$. If that is the case then x is orthogonal to all the rows of H and hence a code word. We then assume that no error has occurred and that x is the code word sent. On the other hand, if $xH^t \neq 0$ then an error has occurred. In order to correct it, we consider the set of all words y in F^n such that $yH^t = xH^t$. We call this set the *coset* corresponding to the *syndrome* xH^t. In the coset corresponding to xH^t we choose the word $\bar{y}$ with least weight i.e. the least Hamming distance from the origin. The fact that $\bar{y}H^t = xH^t$ means that the difference $x - \bar{y}$ is a code word and there does not exist any other code word closer to x since $\bar{y}$ is of minimal weight. For this reason it is reasonable to correct x to $x - \bar{y}$. The word $\bar{y}$ is called a *coset leader* corresponding to the syndrome xH^t.

Example 3.9. For the code in Example 3.8 we have the following table of coset leaders of the listed syndromes

coset leader	00000	10000	01000	00100	00010	00001	11000	10010
syndrome	000	101	011	100	010	001	110	111

The syndrome 000 corresponds to the coset of code words. The five following syndromes correspond to cosets consisting of words different from a code word at only one place. For those the coset leaders are uniquely determined since different words of weight one have different syndromes. This is a consequence of the fact that the columns of the control matrix H are all different. The syndrome of a word that has 1 at place j and 0 elsewhere is the j-th row in H^t. The two last coset leaders are not uniquely determined by their syndromes. For example, also 01100 gives the syndrome 111. Here the receiver can act in several ways. One possibility is that he decides to pick one of the coset leaders and uses that one for error-correcting. Other alternatives are that he asks the sender to repeat the message or simply ignores the word.

Let us now apply the above table to the three received words 11111, 01110 and 01101. The first word has the syndrome 001. The corresponding coset leader is 00001 and the corrected word becomes 11110. For 01110 the syndrome is 101 with coset leader 10000. Even in this case the corrected word is $01110 - 10000 = 11110$. For the word 01101 the syndrome is 110 so at least two letters must be wrong. If the receiver picks the coset leader in the list above, then the corrected word becomes 10101.

We conclude this section with a theorem telling us how we can determine the separation of a code from its control matrix.

Theorem 3.10. *A linear code C with the control matrix H has separation σ if and only if there exist σ columns in H that are linearly dependent and furthermore any $\sigma - 1$ of the columns in H are linearly independent.*

Proof. That σ columns in H are linearly dependent means that there exists a word x of weight at most σ such that $xH^t = 0$. The weight of such a word can never be less than σ, since $\sigma - 1$ columns in H are always linearly independent. Hence $w(C) = \sigma$ and the result follows from Theorem 2.4 of the last section. □

Exercises

Exercise 3.1. Construct a control matrix for the code in Example 1.1.

Exercise 3.2. Show that for a linear $[n, m]$ code C the dual code $C^\perp$ has dimension $n - m$. (*Hint*: Use Theorem 2.10)

Exercise 3.3. The matrices

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 1 & 2 & 4 & 0 & 3 \\ 0 & 2 & 1 & 4 & 1 \\ 2 & 0 & 3 & 1 & 4 \end{bmatrix}$$

are generator matrices for two linear codes C_1 and C_2 in $\mathbb{Z}_2^5$ and $\mathbb{Z}_5^5$, respectively. Construct control matrices for C_1 and C_2. What are the separations for C_1 and C_2?

Exercise 3.4. Consider the linear code in $\mathbb{Z}_2^6$ with the generator matrix

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

(1) Which of the following words are code words ?

$$111001 \ , \ 010100 \ , \ 101100 \ , \ 110111 \ , \ 100001.$$

(2) Which of the words can be corrected? Correct those!

Exercise 3.5. Let C be a binary code with generator matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

Correct the following words in C if possible

$$1101011 \ , \ 0110111 \ , \ 0111000 \ .$$

Exercise 3.6. Determine the separation for the linear code in $\mathbb{Z}_3^8$ with control matrix

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 2 & 1 & 2 \\ 0 & 0 & 1 & 0 & 1 & 1 & 2 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}.$$

Exercise 3.7. Let C be the code in $\mathbb{Z}_5^6$ with the generator matrix

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 1 & 3 & 4 \end{bmatrix}.$$

Show that $d(C) = 4$.

4. Some Special Codes

Example 4.1. The matrix

$$H = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

is a control matrix for a binary $[7, 4]$ code consisting of all the words in $\mathbb{Z}_2^7$ such that $xH^t = 0$. The seven columns in H are all different and together they are all the non-zero elements in $\mathbb{Z}_2^3$. Therefore every non-zero syndrome in $\mathbb{Z}_2^3$ has a unique coset leader of weight 1. For example $\bar{y} = 0001000$ has the syndrome $\bar{y}H^t = 011$ corresponding to the fourth column in H. Every word x in $\mathbb{Z}_2^7$ which is not a code word can be corrected to a code word by only changing one digit in x . Which digit is to be changed is determined by which column in H corresponds to the syndrome xH^t .

Codes with the properties explained in the last example carry a special name.

Definition 4.2. A linear $[n, m]$ code over $\mathbb{Z}_2$, with a control matrix such that its columns are all different and constitute all non-zero columns in $\mathbb{Z}_2^{n-m}$, is called a binary *Hamming code.*

Remark 4.3. Hamming codes can only occur for special values of the parameters m and n. If $r = n - m$ then the number of non-zero vectors in $\mathbb{Z}_2^{n-m}$ is $2^r - 1$. This means that for a binary Hamming code we have $n = 2^r - 1$ and $m = n - r = 2^r - 1 - r$ for some positive integer r. In Example 4.1 we have $r = 3$.

Remark 4.4. In the same way as in Example 4.1, we see that for an arbitrary binary Hamming code, it follows that every word in $\mathbb{Z}_2^n$ is either a code word or has Hamming distance 1 from a uniquely determined code word. This implies that the spheres, of radius 1 and centre in a code word, cover $\mathbb{Z}_2^n$ and that two such spheres never intersect. This means that every binary Hamming code is perfect.

Example 4.5. Let C be the $[10, 8]$ code over the field $\mathbb{Z}_{11}$ defined by $xH^t = 0$, where

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{bmatrix}.$$

Observe that the control matrix H is not of the normal form $[-A^t \mid I_2]$. If we so wish, it is easy to transform it to normal form but for our purposes it is more useful as it is. Note that the calculations are taking place in $\mathbb{Z}_{11}$, so $x \in \mathbb{Z}_{11}^{10}$ is a code word if and only if

$$\begin{cases} x_1 + x_2 + \cdots + x_{10} = 0 & \pmod{11} \\ x_1 + 2x_2 + \cdots + 10x_{10} = 0 & \pmod{11}. \end{cases}$$

Assume that when transferring a code word $z = (z_1, \ldots, z_{10})$ *exactly one error* e has occurred at place k so that the received word is

$$x = (z_1, \ldots, z_k + e, \ldots, z_{10}) .$$

Then the syndrome xH^t is equal to (e, ke). From this we can directly determine the error e and also at which place it occurred, by dividing the second component by the first. If for example $x = 0610271355$, then $xH^t = (8,6)$. Since $8^{-1} = 7$ in $\mathbb{Z}_{11}$ we get $k = 6 \cdot 8^{-1} \equiv 42 \equiv 9 \pmod{11}$. If only one error has occurred in x, then this has happened at place 9 and the corresponding digit should be changed to $5 - 8 \equiv 8$.

If we do not want to use the "digit 10" in the code words we can simply remove all the words containing 10 from the code C. Employing the principle of inclusion-exclusion, one can see that we then still have 82,644,629 words left in the code. This means that we could issue so many ten digit telephone numbers and guarantee that the correct person would be reached even if one digits had been pressed wrongly.

To prepare the next example we describe how two given codes can be used to produce a new one.

Theorem 4.6. *Let F be a finite field and C_1, C_2 be two linear codes in F^n of dimension m_1 and m_2, respectively. Then*

$$C = \{(x, x + y) \in F^{2n};\ x \in C_1 \text{ and } y \in C_2\}$$

is a linear $[2n, m_1 + m_2]$ code. If σ_1 is the separation of C_1 and σ_2 the separation of C_2, then the separation of C is

$$\sigma = min(2\sigma_1, \sigma_2).$$

PROOF. We leave it to the reader to prove that C is a linear code of dimension $m_1 + m_2$. To determine the separation of C we must estimate the least possible weight of the non-zero words in C. If $y = 0$, then $w(x, x) = 2w(x) \geq 2\sigma_1$ and equality is obtained for some $x \neq 0$ in C_1. If $y \neq 0$, then $w(x, x+y) \geq w(y) \geq \sigma_2$ and equality holds for $x = 0$ and some $y \in C_2$. Hence the separation of C equals $\min(2\sigma_1, \sigma_2)$. □

Example 4.7. By repeatedly using Theorem 4.6, we shall construct a code which has, amongst other things, been used by Mariner 9 to send pictures of the planet Mars back to Earth.

Let C_1 be the binary [4,3] code consiting of all the words $x = (x_1, x_2, x_3, x_4)$ in $\mathbb{Z}_2^4$ such that

$$x_1 + x_2 + x_3 + x_4 = 0 \pmod{2}.$$

The code C_1 is generated by those words that contain an even number of the digit 1. A non-zero word must therefore contain at least two ones, so the separation of C_1 is 2. As C_2 we take the code consisting of the two words 0000 and 1111. The code C_2 has dimension 1 and separation 4. If we now apply the construction of Theorem 4.6 to C_1 and C_2, then we obtain a $[8, 3 + 1]$ code with separation 4. Call this code C_1' and now choose C_2' to be the code in $\mathbb{Z}_2^8$ containing the two elements for which their digits are either all 0 or all 1. If we then apply

Theorem 4.6 to C_1' and C_2' we get a [16,5] code with separation 8. Call this C_1'' and take C_2'' to be the code in $\mathbb{Z}_2^{16}$ consisting of the two words with all digits equal. If we then yet again employ Theorem 4.6 we yield a [32,6] code with separation 16. This is the code that was used by Mariner 9. Since the separation is 16, Theorem 1.7 tells us that up to 15 errors are detected and that up to 7 errors can be corrected in each word consisting of 32 letters. For this $32 - 6 = 26$ control digits are needed. The Mariner code belongs to a general class called *Reed-Muller* codes.

The last example of this section is a classical code constructed by M. J. E. Golay in 1949.

Example 4.8. Let C be the [12,6] code over $\mathbb{Z}_3$ with generator matrix

$$G = [I_6 \mid A] = \left[\begin{array}{cccccc|cccccc} 1&0&0&0&0&0&0&1&1&1&1&1\\ 0&1&0&0&0&0&1&0&1&2&2&1\\ 0&0&1&0&0&0&1&1&0&1&2&2\\ 0&0&0&1&0&0&1&2&1&0&1&2\\ 0&0&0&0&1&0&1&2&2&1&0&1\\ 0&0&0&0&0&1&1&1&2&2&1&0 \end{array}\right].$$

The five last digits in the five last rows are obtained by a cyclic permutation of the vector 01221. It is easily checked that the scalar products of the rows of G are zero (note that $2 = -1$ in $\mathbb{Z}_3$). The code C is therefore self-dual. In particular, we have $< x, x >= 0$ for every word x in C.

Since the letters in x are 0 or ± 1, this implies that the weight $w(x)$ must be divisible by 3. We will show that there does not exist a word in C of weight 3. Such a word must be of the type $(3 \,|\, 0)$, $(2 \,|\, 1)$, $(1 \,|\, 2)$ or $(0 \,|\, 3)$, where the digits to the left and to the right of $|$ tell us how many of the first six and last six digits in the word are different from 0, respectively. Since the code is self-dual, the scalar product of any code word and any row of the generator matrix G must be zero. This is impossible for the words of the type $(3 \,|\, 0)$ and $(2 \,|\, 1)$. On the other hand, every code word is a linear combination of the rows of G. This is impossible for the types $(1 \,|\, 2)$ and $(0 \,|\, 3)$. This means that the lowest weight of a non-zero word in C is 6, which therefore is the separation of the code. If we now remove the first column of A in the generator matrix we obtain a [11,6] code called the *Golay code* over $\mathbb{Z}_3$ and is denoted by $\mathcal{G}_{11}$. By removing a letter from a word its weight is reduced by at most 1, so $\mathcal{G}_{11}$ has the separation 5 and can therefore correct up to 2 errors.

This shows that $\mathcal{G}_{11}$ is a perfect code. In order to check this one has to show that equality holds in (6) of Theorem 1.11. For $\mathcal{G}_{11}$ we have $M = 3^6$, $n = 11$, $k = 2$ and $q = 3$, so we must verify

$$3^6 \cdot \left[\binom{11}{0} + \binom{11}{1} \cdot 2 + \binom{11}{2} \cdot 2^2 \right] = 3^{11} \,.$$

This is left to the reader.

Remark 4.9. In 1949 Golay also constructed a perfect binary [23,12] code with separation 7 denoted by $\mathcal{G}_{23}$. One can show that Golay's codes are the only perfect codes over a finite field containing more that two words and correcting more than one error. To be more precise, every such code must be equivalent to either $\mathcal{G}_{11}$ or $\mathcal{G}_{23}$.

Exercises

Exercise 4.1. Construct a control matrix for a binary [15,11] Hamming code.

Exercise 4.2. Let F be a finite field and C be an $[n, m]$ code in F^n with separation 3. If C has a control matrix H such that *every* vector in F^{n-m} can be obtained by multiplying some column in H by an element in F, then C is called a Hamming code over K.

(1) Show that every such Hamming code is perfect.
(2) Construct a control matrix for a [8,6] Hamming code over $\mathbb{Z}_7$.
(3) Construct a control matrix for a [13,10] Hamming code over $\mathbb{Z}_3$.
(4) For which values of n and m does there exist an $[n, m]$ Hamming code over $\mathbb{Z}_p$?

Exercise 4.3. Correct, with respect to the code in Example 4.5, the received word 0617960587 under the condition that it contains at most one error.

Exercise 4.4. Let H be the control matrix in Example 4.5. What conclusion can be drawn if one digit, but not both, is zero in the syndrome xH^t for the received word x?

Exercise 4.5. Describe a generator matrix for the code C in Theorem 4.6, if G_1 and G_2 are generator matrices for the codes C_1 and C_2. Do also construct a generator matrix for the code C_1' in Example 4.7.

Exercise 4.6. Show that in a binary self-dual code the weight of any element must be an even number.

Exercise 4.7. Let C be a binary code with generator matrix

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} .$$

(1) Show that C is self-dual.
(2) Use the result of Exercise 4.6 to calculate the separation $d(C)$.

5. Vandermonde Matrices and Reed-Solomon Codes

In this last section we describe a particular type of codes with a high error-correcting capacity. They have, amongst other things, been important for the development of modern CD-technology.

According to Theorem 3.10, a linear code with control matrix H has separation at least σ if *every* collection of $\sigma - 1$ columns in H is linearly independent. We start by showing how to easily construct matrices with a least fixed number of linearly independent columns.

Let F be a finite field and $\beta_0, \beta_1, \ldots, \beta_d$ be different elements of F. Then the factor theorem tells us that a polynomial $c(x)$ in $F[x]$ of degree at most d with zeros $\beta_0, \beta_1, \ldots, \beta_d$ must be the zero polynomial. If

$$c(x) = c_0 + c_1 x + \cdots + c_d x^d \,,$$

then this implies that the system of equations

$$\begin{bmatrix} 1 & \beta_0 & \beta_0^2 & \ldots & \beta_0^d \\ 1 & \beta_1 & \beta_1^2 & \ldots & \beta_1^d \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \beta_d & \beta_d^2 & \ldots & \beta_d^d \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_d \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

only has the trivial solution $c_0 = c_1 = \cdots = c_d = 0$. This means that the coefficient matrix is invertible, so the columns of the transposed matrix

$$\begin{bmatrix} 1 & 1 & \ldots & 1 \\ \beta_0 & \beta_1 & \ldots & \beta_d \\ \beta_0^2 & \beta_1^2 & \ldots & \beta_d^2 \\ \vdots & \vdots & & \vdots \\ \beta_0^d & \beta_1^d & \ldots & \beta_d^d \end{bmatrix} \tag{8}$$

are linearly independent. A matrix of this form is called a *Vandermonde matrix*.

Now let n be an integer greater than d and let $\alpha_0, \alpha_1, \ldots, \alpha_n$ be different elements of the field F. Then every collection of $d+1$ columns from the matrix

$$\begin{bmatrix} 1 & 1 & \ldots & \ldots & 1 \\ \alpha_0 & \alpha_1 & \ldots & \ldots & \alpha_n \\ \alpha_0^2 & \alpha_1^2 & \ldots & \ldots & \alpha_n^2 \\ \vdots & \vdots & & & \vdots \\ \alpha_0^d & \alpha_1^d & \ldots & \ldots & \alpha_n^d \end{bmatrix} \tag{9}$$

are linearly independent. This because the columns form a Vandermonde matrix. According to Theorem 3.10 every matrix of the form (9) is a control matrix of a linear code in F^{n+1} with separation $d+2$.

Example 5.1. Consider the linear [10,6] code over $\mathbb{Z}_{11}$ defined by the control matrix

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 2^2 & 3^2 & 4^2 & 5^2 & 6^2 & 7^2 & 8^2 & 9^2 & 10^2 \\ 1 & 2^3 & 3^3 & 4^3 & 5^3 & 6^3 & 7^3 & 8^3 & 9^3 & 10^3 \end{bmatrix}$$

where we calculate the powers in $\mathbb{Z}_{11}$. According to what we have just proven, four arbitrary chosen columns in H are always linearly independent so the corresponding code has separation 5. Observe that the columns are contained in a four dimensional vector space, so more that four vectors are always linearly dependent.

Since the separation is 5, it follows from Theorem 1.7 that the code corrects two errors. This is an improvement compared with the code in Example 4.5 only correcting one error. The price for this is that the number of code words in $\mathbb{Z}_{11}^{10}$ are now only 11^6 compared with 11^8 in Example 4.5.

The code in Example 5.1 is a so called *Reed-Solomon* code. In general this name is given to every code over a finite field F with a control matrix of the form (9) where $\alpha_0, \alpha_1, \ldots, \alpha_n$ are *all* the non-zero elements of F. If F has q elements then $n = q-2$. Usually, we then list the elements $\alpha_0, \alpha_1, \ldots, \alpha_n$ by choosing a primitive element $\alpha \in F$ and put $\alpha_i = \alpha^i$. Then the control matrix (9) takes the form

$$\begin{bmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & \alpha & \alpha^2 & \ldots & \alpha^{q-2} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^d & \alpha^{2d} & \ldots & \alpha^{(q-2)d} \end{bmatrix}$$

Since $\alpha^{q-1} = 1$ in F, it is of course sufficient to calculate the exponents modulo $q - 1$.

Remark 5.2. If $d = 2k - 1$, in the control matrix (9), then the separation is $2k + 1$ and the corresponding code corrects k errors. In most applications we have $F = GF(2^m)$ and each "letter" in F can then be written as a string of m binary symbols, 0 or 1. If one considers a continuous sequence of $(k-1)m + 1$ binary symbols in one word, then they can not influence more than k letters in $GF(2^m)$. This means that a single "cascade" of binary errors of length $\leq (k-1)m + 1$ can be corrected. This is the reason why Reed-Solomon codes are used in today's CD-technology. This is utilized when playing a disc to eliminate noise caused by dust, fingerprints, small scratches, etc.

Example 5.3. Let us consider the case when $F = GF(2^6)$ and $k = 5$. Since F has 64 elements, every word in a Reed-Solomon code over F has length 63 if the letters are elements in F. This corresponds to binary words of length $6 \cdot 63 = 378$. When $k = 5$ we can correct single cascades of binary errors up to length $(k-1)m + 1 = 25$. In this case the control matrix (9) has $d + 1 = 2k = 10$ rows, so the code has dimension $63 - 10 = 53$, as a vector space over F. This means that it contains $(2^6)^{53} = 2^{318}$ words.

Exercises

Exercise 5.1. Construct a linear [8,4] code over $\mathbb{Z}_{17}$ with separation 5.

Exercise 5.2. Construct a control matrix for a Reed-Solomon code over $F = GF(2^3)$ that corrects 2 errors in F.