# $p$-Adic Codes

The $p$-adic numbers were first considered by Hensel in the 19th century. He observed that the primes play an analogous role in the integers as linear polynomials do in $\mathbb{C}[X]$. The Laurent expansion of a rational function led him to consider the $p$-adic expansion of a rational number. In this chapter, for a fixed prime $p$, we will construct block codes over the rings $\mathbb{Z}/p^h\mathbb{Z}$ simultaneously, by constructing codes over the $p$-adic numbers and then considering the coordinates modulo $p^h$. These codes will be linear over the ring but when mapped to codes over $\mathbb{Z}/p\mathbb{Z}$ will result in codes which are not equivalent to linear codes. We start with a brief introduction to $p$-adic numbers, which will cover enough background for our purposes. The classical cyclic codes, that we constructed in ▶ Chapter 5, lift to cyclic codes over the $p$-adic numbers. In the case of the cyclic Hamming code, this lift extends to a code over $\mathbb{Z}/4\mathbb{Z}$ which, when mapped to a binary code, gives a non-linear code with a set of parameters for which no linear code exists.

## 10.1 $p$-Adic Numbers

Let $p$ be a prime.

The set of **$p$-adic integers**, which is denoted by $\mathbb{Z}_p$, is the set of sequences,

$$a = (a_1, a_2, a_3, \ldots),$$

where $a_i \in \mathbb{Z}/p^i\mathbb{Z}$ for all $i \in \mathbb{N}$ and

$$a_{j+1} \equiv a_j \pmod{p^j}.$$

An ordinary integer $n \in \mathbb{Z}$ is an element of $\mathbb{Z}_p$ defined by the sequence

$$a_j \equiv n \pmod{p^j}.$$

© Springer Nature Switzerland AG 2020
S. Ball, *A Course in Algebraic Error-Correcting Codes*, Compact Textbooks in Mathematics,
https://doi.org/10.1007/978-3-030-41153-4_10

The sequence defined by

$$a_{j+1} = a_j + p^j,$$

$j \in \mathbb{N}$, is a $p$-adic integer which is not an ordinary integer.

For example, with $a_1 = 3$ and $p = 5$, this sequence begins

$$(3, 8, 33, 158, 783, \ldots).$$

We define addition and multiplication on the sequences component-wise, so

$$a + b = (a_1, a_2, a_3, \ldots) + (b_1, b_2, b_3, \ldots) = (a_1 + b_1, a_2 + b_2, a_3 + b_3, \ldots).$$

To verify $a + b \in \mathbb{Z}_p$, observe that

$$a_{j+1} + b_{j+1} \equiv a_j + b_j \pmod{p^j}.$$

Similarly,

$$ab = (a_1, a_2, a_3, \ldots)(b_1, b_2, b_3, \ldots) = (a_1 b_1, a_2 b_2, a_3 b_3, \ldots).$$

To verify $ab \in \mathbb{Z}_p$, observe that

$$a_{j+1} b_{j+1} \equiv a_j b_j \pmod{p^j}.$$

With these definitions multiplication is distributive with respect to addition, so $\mathbb{Z}_p$ is a ring and has a multiplicative identity element

$$1 = (1, 1, 1, \ldots).$$

If $a$ is a sequence for which $a_1 = 0$, then $a$ does not have a multiplicative inverse, so $\mathbb{Z}_p$ is not a field. It is, however, an integral domain ($xy = 0$ implies either $x = 0$ or $y = 0$), so it has a quotient field. This quotient field is called the **field of $p$-adic numbers** and is denoted $\mathbb{Q}_p$. Elements of $\mathbb{Q}_p$ are called **$p$-adic numbers**.

All non-zero elements of $\mathbb{Z}_p$ can be written as the product of a unit times some non-negative power of $p$.

For example, the 5-adic integer

$$(0, 15, 40, 290, 915, \ldots) = 5(3, 8, 58, 183, \ldots, ),$$

since $15 \equiv 0$ modulo 5, $40 \equiv 15$ modulo 25, $290 \equiv 40$ modulo 125, etc.

The field $\mathbb{Q}_p$ consists of the sequences where we allow negative powers of $p$ as well.

For example,

$$5^{-2}(2, 22, 97, 222, \ldots),$$

is a 5-adic number.

The product of $p^{\alpha}(a_1, a_2, a_3, \ldots)$ and $p^{\beta}(b_1, b_2, b_3, \ldots)$ is

$$p^{\alpha+\beta}(a_1b_1, a_2b_2, a_3b_3, \ldots).$$

Returning to the previous examples,

$$5(3, 8, 58, 183, \ldots, )5^{-2}(2, 22, 97, 222, \ldots) = 5^{-1}(1, 1, 1, 1, \ldots).$$

## 10.2 Polynomials over the $p$-Adic Numbers

Let $\overline{\mathbb{Q}}_p$ denote an algebraic closure of $\mathbb{Q}_p$. Recall that, since $\overline{\mathbb{Q}}_p$ is an algebraic closure, the polynomials of positive degree over $\mathbb{Q}_p$ factorise into linear factors over $\overline{\mathbb{Q}}_p$. The following lemma is a straightforward application of the binomial theorem.

**Lemma 10.1** *If* $\alpha, \beta \in \overline{\mathbb{Q}}_p$ *and*

$$\alpha \equiv \beta \pmod{p^r}$$

*then*

$$\alpha^p \equiv \beta^p \pmod{p^{r+1}}.$$

**Proof**

We can write $\alpha = \beta + p^r\gamma$, for some $\gamma \in \mathbb{Z}_p$. Then

$$\alpha^p = (\beta + p^r\gamma)^p \equiv \beta^p \pmod{p^{r+1}}.$$

□

In ▶ Chapter 2 we studied how to factorise cyclotomic polynomials over finite fields and put this to use in ▶ Chapter 5 while constructing cyclic codes. The following theorem tells us that a factorisation over $\mathbb{F}_p$ "lifts" to a factorisation over the $p$-adic numbers. As in ▶ Chapter 5, we will exploit this factorisation to construct cyclic codes and their extensions with some surprising results.

**Theorem 10.2**

*Let $p$ be a prime and let $n$ be a positive integer which is not a multiple of $p$. If $h$ is a monic irreducible divisor of $X^n - 1$ in $(\mathbb{Z}/p\mathbb{Z})[X]$, then there exists a monic irreducible polynomial $h_\infty$ in $\mathbb{Z}_p[X]$ which divides $X^n - 1$ and is congruent to $h$ modulo $p$.*

**Proof**

By induction on $r$, we will find a polynomial $h_r(X) \in (\mathbb{Z}/p^r\mathbb{Z})[X]$ such that $h_r(X)$ divides $X^n - 1$ and $h_r \equiv h$ modulo $p$. Then $h_\infty$ will be the polynomial $h_r$ as $r \to \infty$.

An element $c \in \mathbb{Z}/p^r\mathbb{Z}$ can be extended to an element of $\mathbb{Z}_p$ by taking the sequence

$$(c_1, c_2, \ldots, c_{r-1}, c, c, c, \ldots),$$

where $c_i = c \bmod p^i$, for $i = 1, \ldots r-1$. Therefore, the coefficients of $h_r(X)$ can be viewed as elements of $\mathbb{Z}_p$ and therefore as elements of $\mathbb{Q}_p$.

Since $n$ is not a multiple of $p$, the roots of $h_1(X)$ in $\overline{\mathbb{Q}}_p$ are distinct. By induction, we can assume that the roots of $h_r(X)$ are distinct.

For each root $\alpha$ of $h_r(X)$ (in $\overline{\mathbb{Q}}_p$),

$$\alpha^n \equiv 1 \pmod{p^r}.$$

Let

$$f(X) = h_r(X) + p^r g(X),$$

for some polynomial $g(X) \in \mathbb{Z}_p[X]$.

For each root $\beta$ of $f$, there is a root $\alpha$ of $h_r(X)$ such that

$$\beta \equiv \alpha \pmod{p^r}.$$

Then, by Lemma 10.1,

$$\beta^p \equiv \alpha^p \pmod{p^{r+1}}.$$

Lemma 10.1 also implies that

$$\alpha^{np} \equiv 1 \pmod{p^{r+1}}$$

from which we deduce that

$$\beta^{np} \equiv 1 \pmod{p^{r+1}}.$$

Let

$$h_{r+1}(X) = \prod (X - \beta^p),$$

where the product runs over the roots $\beta$ of $f$.

Then $h_{r+1}$ divides $X^n - 1$ modulo $p^{r+1}$. Since

$$\beta^p \equiv \alpha^p \equiv \alpha \pmod{p},$$

$h_{r+1}$ and $h_r$ have the same roots modulo $p$.

Thus, the roots of $h_{r+1}$ are distinct and

$$h_{r+1} \equiv h_r \pmod{p}.$$

□

## 10.3 $p$-Adic Codes

Let $R$ be a commutative ring with multiplicative identity 1. An **$R$-module** $M$ is a commutative group with a left multiplication from $R \times M \to M$ satisfying $\lambda(u+v) = \lambda u + \lambda v$, $(\lambda+\mu)u = \lambda u + \mu u$, $(\lambda\mu)u = \lambda(\mu u)$ and $1u = u$, for all $u, v \in M$ and all $\lambda, \mu \in R$.

The set $\mathbb{Z}_p^n$ of $n$-tuples over the $p$-adic integers is a commutative group with respect to addition. We define left multiplication of an element $(u_1, \ldots, u_n) \in \mathbb{Z}_p^n$ by an element $\lambda \in \mathbb{Z}_p$ as

$$\lambda(u_1, \ldots, u_n) = (\lambda u_1, \ldots, \lambda u_n).$$

This scalar multiplication satisfies $\lambda(u+v) = \lambda u + \lambda v$, $(\lambda+\mu)u = \lambda u + \mu u$, $(\lambda\mu)u = \lambda(\mu u)$ and $1u = u$, for all $u, v \in \mathbb{Z}_p^n$ and all $\lambda, \mu \in \mathbb{Z}_p$. Thus, with this scalar multiplication $\mathbb{Z}_p^n$ is a $\mathbb{Z}_p$-module.

A **submodule** $C$ of $\mathbb{Z}_p^n$ is a non-empty subset of $\mathbb{Z}_p^n$ which is closed under linear combinations. In other words,

$$\lambda u + \mu v \in C,$$

for all $u, v \in C$ and all $\lambda, \mu \in \mathbb{Z}_p$.

We now re-define the analogous objects that we saw for linear codes over a field for codes over $\mathbb{Z}_p$. A **$p$-adic code** of length $n$ is a subset of $\mathbb{Z}_p^n$. A **linear code** over $\mathbb{Z}_p$ is a submodule of $\mathbb{Z}_p^n$.

A **generator matrix** for a linear code $C$ over $\mathbb{Z}_p$ is a $k \times n$ matrix G with the property that

$$C = \{(u_1, \ldots, u_k)\mathrm{G} |\ (u_1, \ldots, u_k) \in \mathbb{Z}_p^k\}.$$

We define the **scalar product** on $\mathbb{Z}_p^n$ as the standard inner product

$$u \cdot v = u_1 v_1 + \cdots + u_n v_n.$$

The **dual code** of a linear code $C$ is defined, as in the case of a linear code over a finite field, as

$$C^{\perp} = \{v \in \mathbb{Z}_p^n \mid u \cdot v = 0 \text{ for all } u \in C\}.$$

A linear code $C$ is **cyclic** if

$$(c_1, c_2, \ldots, c_n) \in C$$

implies

$$(c_n, c_1, \ldots, c_{n-1}) \in C.$$

A codeword of the cyclic code corresponds to a polynomial in the ring $\mathbb{Z}_p[X]/(X^n - 1)$ under the correspondence

$$(c_1, c_2, \ldots, c_n) \mapsto c_1 + c_2X + \cdots + c_nX^{n-1}.$$

As in the case of finite fields, under this correspondence, a cyclic code is an ideal $\langle g \rangle$, where $g$ is some divisor of $X^n - 1$.

**Example 10.3**
The polynomial $X^3+X+1$ divides $X^7-1$ in $(\mathbb{Z}/2\mathbb{Z})[X]$. Theorem 10.2 implies the existence of a polynomial in $\mathbb{Z}_2[X]$ which divides $X^7 - 1$. One can verify that

$$g(X) = X^3 + \lambda X^2 + (\lambda - 1)X - 1$$

divides $X^7 - 1$ in $\mathbb{Z}_2[X]$ if and only if $\lambda^2 - \lambda + 2 = 0$ by observing that

$$X^7 - 1 = (X^3 + \lambda X^2 + (\lambda - 1)X - 1)(X^3 + (1 - \lambda)X^2 - \lambda X - 1)(X - 1).$$

To calculate $\lambda$, suppose

$$\lambda = (a_1, a_2, a_3, \ldots).$$

Since $a_1 \in \mathbb{Z}/2\mathbb{Z}$, we have $a_1 = 0$ or 1.

If $a_1 = 0$, then substituting $\lambda \equiv 0 + 2a_2 \pmod 4$ in

$$\lambda^2 - \lambda + 2 \equiv 0 \pmod 4$$

implies

$$-2a_2 + 2 \equiv 0 \pmod 4,$$

so $a_2 = 1$ and $\lambda \equiv 2 \pmod 4$.

Substituting $\lambda \equiv 2 + 4a_3 \pmod 8$ in

$$\lambda^2 - \lambda + 2 \equiv 0 \pmod 8$$

implies

$$4 - 2 - 4a_3 + 2 \equiv 0 \pmod 8,$$

so $a_3 = 1$ and $\lambda \equiv 6 \pmod 8$.

Continuing in this way we deduce that one of the roots of $\lambda^2 - \lambda + 2$ is

$$\lambda = (0, 2, 6, 6, 6, 38, 38, 166, 422, \ldots).$$

The cyclic code $\langle g \rangle$ is a 2-adic linear code of length 7 with generator matrix

$$\mathrm{G} = \begin{pmatrix} -1 & \lambda - 1 & \lambda & 1 & 0 & 0 & 0 \\ 0 & -1 & \lambda - 1 & \lambda & 1 & 0 & 0 \\ 0 & 0 & -1 & \lambda - 1 & \lambda & 1 & 0 \\ 0 & 0 & 0 & -1 & \lambda - 1 & \lambda & 1 \end{pmatrix}.$$

■

To make use of these $p$-adic codes, we will now consider the coordinates of the codewords of a $p$-adic code modulo $p^h$ for some $h$. The resulting code will be a code defined over the finite alphabet $\mathbb{Z}/p^h\mathbb{Z}$. We will use the matrix G from Example 10.3 in Example 10.9.

## 10.4 Codes over $\mathbb{Z}/p^h\mathbb{Z}$

A **linear code** over $\mathbb{Z}/p^h\mathbb{Z}$ is a $(\mathbb{Z}/p^h\mathbb{Z})$-submodule of $(\mathbb{Z}/p^h\mathbb{Z})^n$. As in the case for a linear code over $\mathbb{F}_q$, we define a **generator matrix** for a linear code $C$ over $(\mathbb{Z}/p^h\mathbb{Z})^n$ as a $r \times n$ matrix G with the property that

$$C = \{(u_1, \ldots, u_r)\mathrm{G} |\ (u_1, \ldots, u_r) \in (\mathbb{Z}/p^h\mathbb{Z})^r\}.$$

If all the elements in the $i$-th row of G are divisible by $p^j$, then we can restrict $u_i$ to $\mathbb{Z}/p^{h-j}\mathbb{Z}$.

**Example 10.4**

Let

$$\mathrm{G} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 2 & 2 & 3 & 3 & 4 & 4 & 5 & 5 & 6 & 6 & 7 & 7 & 8 & 8 \\ 0 & 0 & 3 & 6 & 3 & 6 & 3 & 6 & 3 & 6 & 3 & 6 & 3 & 6 & 3 & 6 & 3 & 6 & 3 & 6 \end{pmatrix},$$

where the elements of G are from $\mathbb{Z}/9\mathbb{Z}$.

The code generated by the matrix G is

$$C = \{(u_1, u_2, u_3)\mathrm{G} \mid u_1, u_2 \in \mathbb{Z}/9\mathbb{Z},\ u_3 \in \mathbb{Z}/3\mathbb{Z}\}.$$

Thus, the code $C$ is a 9-ary code of length 20 of size 243.

The codeword

$$(3, 0, 1)\mathrm{G} = (3, 0, 3, 6, 6, 0, 6, 0, 6, 0, 6, 0, 6, 0, 6, 0, 6, 0, 6, 0)$$

and the all-zero codeword differ in 11 coordinates, so the minimum distance is at most 11. It is Exercise 10.3 to verify that the minimum distance is 11. ■

**Theorem 10.5**

*After a suitable permutation of the coordinates, a linear code $C$ over $(\mathbb{Z}/p^h\mathbb{Z})^n$ has a generator matrix of the form*

$$\mathrm{G} = \begin{pmatrix} \mathrm{I} & \mathrm{A}_{01} & \mathrm{A}_{02} & \mathrm{A}_{03} & \cdots & \mathrm{A}_{0,h-1} & \mathrm{A}_{0,h} \\ 0 & p\mathrm{I} & p\mathrm{A}_{12} & p\mathrm{A}_{13} & \cdots & p\mathrm{A}_{1,h-1} & p\mathrm{A}_{1,h} \\ 0 & 0 & p^2\mathrm{I} & p^2\mathrm{A}_{23} & \cdots & p^2\mathrm{A}_{2,h-1} & p^2\mathrm{A}_{2,h} \\ \vdots & \ddots & \ddots & \ddots & \ddots & \cdots & \vdots \\ \vdots & \cdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & . & \cdots & 0 & 0 & p^{h-1}\mathrm{I} & p^{h-1}\mathrm{A}_{h-1,h} \end{pmatrix}.$$

*If the block sizes of the columns are $k_0, k_1, \ldots, k_h$ (necessarily summing to $n$), then*

$$|C| = p^k,$$

*where*

$$k = \sum_{i=0}^{h-1} (h - i)k_i.$$

**Proof**

Applying elementary row operations to the matrix does not change the code $C$ generated by the matrix. Since we are also allowed to permute the columns the only impediment to obtaining a generator matrix of the form

$$\begin{pmatrix} \mathrm{I} & \mathrm{B}_{01} \end{pmatrix},$$

is rows in which all elements are divisible by $p$. Thus, we obtain a generator matrix of the form

$$\mathrm{G} = \begin{pmatrix} \mathrm{I} & \mathrm{B}_{01} \\ 0 & p\mathrm{B}_{02} \end{pmatrix},$$

for some matrices $\mathrm{B}_{01}$ and $\mathrm{B}_{02}$. We continue applying row operations and column permutations. Again, the only impediment to obtaining a generator matrix of the form

$$\begin{pmatrix} \mathrm{I} & \mathrm{B}_{01} & \mathrm{B}_{02} \\ 0 & p\mathrm{I} & p\mathrm{B}_{12} \end{pmatrix},$$

is rows in which all elements are divisible by $p^2$.

Therefore, there is a generator matrix for $C$ of the form

$$\mathrm{G} = \begin{pmatrix} \mathrm{I} & \mathrm{B}_{01} & \mathrm{B}_{02} \\ 0 & p\mathrm{I} & p\mathrm{B}_{12} \\ 0 & 0 & p^2\mathrm{B}_{22} \end{pmatrix}.$$

The form of G follows by continuing applying row operations and column permutations.

The code generated by G is

$$C = \{(u_1, \ldots, u_r)\mathrm{G} \mid u_i \in \mathbb{Z}/p^h\mathbb{Z}\}.$$

If all the entries in the $\ell$-th row of G are divisible by $p^j$, then we can restrict $u_\ell$ to $\mathbb{Z}/p^{h-j}\mathbb{Z}$, which implies that the size of the code is as claimed. □

**Example 10.6**

Consider the code over $\mathbb{Z}/8\mathbb{Z}$ generated by the matrix

$$\begin{pmatrix} 0 & 2 & 1 & 4 & 1 & 1 \\ 4 & 6 & 7 & 4 & 7 & 1 \end{pmatrix}.$$

By shifting the coordinates one coordinate to the right, we obtain an equivalent code with generator matrix

$$\begin{pmatrix} 1 & 0 & 2 & 1 & 4 & 1 \\ 1 & 4 & 6 & 7 & 4 & 7 \end{pmatrix}.$$

Subtracting the first row from the second, we obtain a generator matrix for the same code

$$\begin{pmatrix} 1 & 0 & 2 & 1 & 4 & 1 \\ 0 & 4 & 4 & 6 & 0 & 6 \end{pmatrix}.$$

Multiplying the second row by 3 we obtain another generator matrix for the code

$$\begin{pmatrix} 1\,0\,2\,1\,4\,1 \\ 0\,4\,4\,2\,0\,2 \end{pmatrix}.$$

Finally, interchanging the second and sixth column we obtain an equivalent code with generator matrix

$$\begin{pmatrix} 1\,1\,2\,1\,4\,0 \\ 0\,2\,4\,2\,0\,4 \end{pmatrix}.$$

Comparing this to the claim of Theorem 10.5, the matrix $A_{01} = (1)$, the matrix $A_{02} = (2\,1\,4\,0)$ and the matrix $A_{12} = (2\,1\,0\,2)$.

Note that the code has size 32 and not 64, which is not immediately apparent from the initial generator matrix. ■

## 10.5 Codes over $\mathbb{Z}/4\mathbb{Z}$

10

The **Gray map** is a map $\gamma$ from $\mathbb{Z}/4\mathbb{Z}$ to $\{0, 1\}^2$ defined by

| $x$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| $\gamma(x)$ | (0, 0) | (0, 1) | (1, 1) | (1, 0) |

.

We extend the Gray map to a map from $(\mathbb{Z}/4\mathbb{Z})^n$ to $\{0, 1\}^{2n}$ by applying $\gamma$ to each coordinate.

If $C$ is a block code of length $n$ over $\mathbb{Z}/4\mathbb{Z}$, then $\gamma(C)$, defined by

$$\gamma(C) = \{\gamma(v) \mid v \in C\},$$

is a binary code of length $2n$. It is immediate that if $C$ has minimum distance $d$, then $\gamma(C)$ has minimum distance at least $d$.

However, there is a possibility that the minimum distance of $\gamma(C)$ is larger than $d$.

**Example 10.7**

Let $C$ be the code over $\mathbb{Z}/4\mathbb{Z}$ generated by the matrix

$$\begin{pmatrix} 1\,0\,2\,1\,1\,1 \\ 0\,2\,2\,2\,0\,0 \end{pmatrix}.$$

The 8 codewords of $C$ and the code $\gamma(C)$ are

| C | $\gamma(C)$ |
|---|---|
| (0,0,0,0,0,0) | (0,0,0,0,0,0,0,0,0,0,0,0) |
| (1,0,2,1,1,1) | (0,1,0,0,1,1,0,1,0,1,0,1) |
| (0,2,2,2,0,0) | (0,0,1,1,1,1,1,1,0,0,0,0) |
| (1,2,0,3,1,1) | (0,1,1,1,0,0,1,0,0,1,0,1) |
| (2,0,0,2,2,2) | (1,1,0,0,0,0,1,1,1,1,1,1) |
| (2,2,2,0,2,2) | (1,1,1,1,1,1,0,0,1,1,1,1) |
| (3,0,2,3,3,3) | (1,0,0,0,1,1,1,0,1,0,1,0) |
| (3,2,0,1,3,3) | (1,0,1,1,0,0,0,1,1,0,1,0) |

One readily checks that the minimum distance of $C$ is 3 and the minimum distance of $\gamma(C)$ is 6. ■

The **Lee distance** between two elements $u$ and $v$ of $(\mathbb{Z}/4\mathbb{Z})^n$ is defined as the Hamming distance between $\gamma(u)$ and $\gamma(v)$. The **Lee weight** of an element $u$ of $(\mathbb{Z}/4\mathbb{Z})^n$ is the Lee distance between $u$ and the all zero $n$-tuple.

**Lemma 10.8** *Let $C$ be a linear code over $\mathbb{Z}/4\mathbb{Z}$. The minimum Lee weight of a non-zero codeword of $C$ is equal to the minimum distance of $\gamma(C)$.*

**Proof**

Let $u = (u_1, \ldots, u_n)$ and $v = (v_1, \ldots, v_n)$ be two codewords of $C$.

By checking all possibilities for $u_i, v_i \in \mathbb{Z}/4\mathbb{Z}$, one can verify that the distance between $\gamma(u_i)$ and $\gamma(v_i)$ is equal to the distance between $(0, 0)$ and $\gamma(u_i - v_i)$.

Thus,

$$d(\gamma(u), \gamma(v)) = \sum_{i=1}^{n} d(\gamma(u_i), \gamma(v_i)) = \sum_{i=1}^{n} d(\gamma(u_i - v_i), (0, 0))$$

which is equal to the Lee weight of $u - v$. □

In the following example, we return to Example 10.3 and consider the entries in the matrix modulo 4. This matrix will then generate a code over $\mathbb{Z}/4\mathbb{Z}$.

**Example 10.9**

By Example 10.3, we have that $X^3 + 2X^2 + X + 3$ divides $X^7 - 1$ in $(\mathbb{Z}/4\mathbb{Z})[X]$. This polynomial generates a cyclic code of length 7 which extends to a code of length 8 with generator matrix

$$\mathrm{G} = \begin{pmatrix} 3\,1\,2\,1\,0\,0\,0\,1 \\ 0\,3\,1\,2\,1\,0\,0\,1 \\ 0\,0\,3\,1\,2\,1\,0\,1 \\ 0\,0\,0\,3\,1\,2\,1\,1 \end{pmatrix}.$$

Let $C$ be the $\mathbb{Z}/4\mathbb{Z}$-linear code of length 8 with 256 codewords defined by

$$C = \{uG \mid u \in (\mathbb{Z}/4\mathbb{Z})^4\}.$$

The code $\gamma(C)$ is a binary code of length 16 with 256 codewords. By Exercise 10.7, the minimum distance of $\gamma(C)$ is 6. This code is equivalent to the code constructed in Example 9.12. As mentioned there, an important observation is that there is no binary linear code with these parameters, which we proved in Example 4.20. ■

Example 10.9 suggests that codes over rings may be a good place to look for non-linear codes which have better parameter sets than linear codes. It may be the case that we need to consider non-linear codes to disprove Conjecture 3.18.

## 10.6 Comments

This chapter leans somewhat on the enlightening article by Calderbank and Sloane on $p$-adic codes [14]. Carlet [19] has generalised the Gray map to a bijection from $\mathbb{Z}/2^k\mathbb{Z}$ to $R(1, k-1)$. This can be extended to $(\mathbb{Z}/2^k\mathbb{Z})^n$ and can therefore be used to construct (non-linear) binary codes from $\mathbb{Z}/2^k\mathbb{Z}$-linear codes.

Theorem 10.2 is a special case of Hensel's lifting lemma. For more on $p$-adic numbers, including the lifting lemma, see [30].

## 10.7 Exercises

**10.1** *Let*

$$\lambda = (1, b_2, b_3, b_4, \ldots)$$

*be the* 2*-adic integer which is a root of* $X^2 - X + 2$*. Calculate the numbers* $b_2, b_3, b_4$ *in the sequence of* $\lambda$*.*

**10.2** *Prove that the code generated by the* $4 \times 8$ *matrix obtained by extending the generator matrix in Example 10.3 with the all-one vector is a self-dual code.*

**10.3** *Check, with the aid of a computer or not, that the code in Example 10.4 has minimum distance* 11*.*

**10.4** *i. Prove that the dual code* $C^{\perp}$*, to the code* $C$ *generated by the matrix in Theorem 10.5, has a generator matrix of the form*

$$\mathrm{G} = \begin{pmatrix} \mathrm{B}_{0,h} & \mathrm{B}_{0,h-1} & \cdots & \mathrm{B}_{03} & \mathrm{B}_{02} & \mathrm{B}_{01} & \mathrm{I} \\ p\mathrm{B}_{1,h} & p\mathrm{B}_{1,h-1} & \cdots & p\mathrm{B}_{13} & p\mathrm{B}_{12} & p\mathrm{I} & 0 \\ p^2\mathrm{B}_{2,h} & p^2\mathrm{B}_{2,h-1} & \cdots & p^2\mathrm{B}_{23} & p^2\mathrm{I} & 0 & 0 \\ . & . & . & .^{.^{.}} & .^{.^{.}} & . & . \\ . & . & .^{.^{.}} & .^{.^{.}} & . & . & . \\ p^{h-1}\mathrm{B}_{h-1,h} & p^{h-1}\mathrm{I} & 0 & \dots & \dots & \dots & 0 \end{pmatrix},$$

*for some matrices* $\mathrm{B}_{ij}$*, where the blocks of columns have the same size as in Theorem 10.5.*

*ii. Prove that* $|C^{\perp}| = p^{k_{\perp}}$*, where*

$$k_{\perp} = \sum_{i=1}^{h} i k_i.$$

**10.5** *Let* $C$ *be a linear code over* $\mathbb{Z}/p^h\mathbb{Z}$*. Prove that* $(C^{\perp})^{\perp} = C$*.*

**10.6** *Let* $C$ *be the linear code over* $\mathbb{Z}/4\mathbb{Z}$ *from Example 10.7.*

*i. Check that the minimum Lee weight of a non-zero codeword of* $C$ *is* 6 *and verify that the minimum Hamming distance between any two codewords of* $\gamma(C)$ *is* 6*.*

*ii. The code* $\gamma(C)$ *is a non-linear binary code of length* 12*, minimum distance* 6 *and size* 8*. Construct a linear code with the same parameters.*

*iii. The code*

$$C = \{\lambda u + 2\mu v \mid \lambda \in \mathbb{Z}/4\mathbb{Z},\ \mu \in \mathbb{Z}/2\mathbb{Z}\}$$

*for some* $u \in (\mathbb{Z}/4\mathbb{Z})^6$ *and* $v \in (\mathbb{Z}/2\mathbb{Z})^6$*, where the weight of* $v$ *is* 3*. Construct a code with the same parameters as* $C$ *in which the weight of* $v$ *is* 4*.*

**10.7**

*i. Prove, using row operations, that the code* $C$ *in Example 10.9 has a generator matrix*

$$\mathrm{G} = \mathrm{G}_1 + 2\mathrm{G}_2,$$

*where*

$$\mathrm{G}_1 = \begin{pmatrix} 1&0&0&0&0&1&1&1 \\ 0&1&0&0&1&0&1&1 \\ 0&0&1&0&1&1&0&1 \\ 0&0&0&1&1&1&1&0 \end{pmatrix}$$

*and*

$$G_2 = \begin{pmatrix} 0\,0\,0\,0\,1\,1\,0\,0 \\ 0\,0\,0\,0\,0\,1\,1\,0 \\ 0\,0\,0\,0\,0\,0\,1\,1 \\ 0\,0\,0\,0\,1\,0\,0\,1 \end{pmatrix}.$$

*ii. Prove, using Lemma 10.8, that the code $\gamma(C)$ in Example 10.9 has minimum distance 6.*

**10.8**

*i. Prove that $X^2 + \lambda X - 1$ divides $X^8 - 1$ in $\mathbb{Z}_p[X]$, where $\lambda$ is a $p$-adic integer satisfying $\lambda^2 = -2$.*

*ii. Calculate the next few numbers in the sequences $(1, 4, \ldots)$ and $(2, 5, \ldots)$ which are both solutions of $\lambda^2 = -2$ in $\mathbb{Z}_3$.*

**10.9**

*i. Prove that $X^5 + \lambda X^4 - X^3 + X^2 + (\lambda - 1)X - 1$ divides $X^{11} - 1$ in $\mathbb{Z}_p[X]$, where $\lambda$ is a $p$-adic integer satisfying $\lambda^2 = \lambda - 3$.*

*ii. Calculate the first few numbers in the sequences which are solutions of $\lambda^2 = \lambda - 3$ in $\mathbb{Z}_3$.*

**10.10**

*i. Prove that $X^{11} + \lambda X^{10} + (\lambda - 3)X^9 - 4X^8 - (\lambda + 3)X^7 - (2\lambda + 1)X^6 - (2\lambda - 3)X^5 - (\lambda - 4)X^4 + 4X^3 + (\lambda + 2)X^2 + (\lambda - 1)X - 1$ divides $X^{23} - 1$ in $\mathbb{Z}_p[X]$, where $\lambda$ is a $p$-adic integer satisfying $\lambda^2 = \lambda - 6$.*

*ii. Calculate the first few numbers in the sequences which are solutions of $\lambda^2 = \lambda - 6$ in $\mathbb{Z}_2$.*