Coding Theory and Applications

Solved Exercises and Problems of Cyclic Codes

Enes Pasalic
University of Primorska
Koper, 2013

Contents

1 Preface

This is a collection of solved exercises and problems of cyclic codes for students who have a working knowledge of coding theory. Its aim is to achieve a balance among the computational skills, theory, and applications of cyclic codes, while keeping the level suitable for beginning students. The contents are arranged to permit enough flexibility to allow the presentation of a traditional introduction to the subject, or to allow a more applied course.

Enes Pasalic
enes.pasalic@upr.si

2 Problems

1. (Decoding RM codes) A RM code $(1, 3)$ is a (8,4,4) linear code that can correct any single error. Construct a generator matrix for this code and decode the received codeword $r = (01010111)$

   The corresponding generator matrix is,

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

   Note that the generator matrix is in proper order, that is the columns of the last 3 rows of G are binary representation of integers $0, 1, \ldots, 7$. Least significant bit on the left, that is 3=(110). The decoding procedure is as follows:

   (a) Construct vector $\mathbf{R} = (-1)^{\mathbf{r}} = (1, -1, 1, -1, 1, -1, -1, -1)$.
   (b) Construct the Hadamard matrix of size 8×8
   (c) Compute $\hat{\mathbf{R}} = \mathbf{R}H$
   (d) Find the maximum absolute value in $\hat{\mathbf{R}}$
   (e) The binary representation of the entry in $\hat{\mathbf{R}}$ specifies the linear combination of the basis vectors of G to be used (apart from $\mathbf{1}$).

   We compute:

   $$\hat{\mathbf{R}} = \mathbf{R}H_8 = \begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \\ 1 \\ -1 \\ -1 \\ -1 \end{bmatrix}^T \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix} = \begin{bmatrix} -2 \\ 6 \\ 2 \\ 2 \\ 2 \\ 2 \\ -2 \\ -2 \end{bmatrix}^T$$

   Thus $\max \hat{\mathbf{R}} = 6$, and the corresponding vector is $\mathbf{u} = (100)$. Since the sign is positive we get that the codeword is $\mathbf{u} \cdot \mathbf{v} = \mathbf{v}_1$ where $\mathbf{v}_1$ is the second row of G. That is, $\mathbf{c} = (01010101)$ which agrees with the received vector.

2. (Constructing fields) Discuss the construction of finite fields of eight elements.

   Sometimes we define finite fields by means of a primitive element being a primitive root of the polynomial used to construct the field.
   Exponents of the primitive element α of the finite field $GF(2^m)$ generate all nonzero elements of that field:

   $$\alpha^0 = 1, \alpha, \alpha^2, \alpha^{2^m-2}, \alpha^{2^m-1} = 1.$$

Additionally, every element of the field $GF(2^m)$ can be represented as a polynomial

$$a(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 \ldots + a_{m-1}\alpha^{m-1}$$

where polynomial coefficients are binary, $a_i \in \{0, 1\}$. If we collect coefficients into a vector

$$a = (a_0, a_1, \ldots, a_{m-1})$$

we obtain equivalent binary representation of the field elements, using m bits. To obtain these representations and establish a connection between them, we use primitive polynomial $p(x)$ of degree m, which generates the field $GF(2^m)$.
In the case of $GF(2^3)$, there are two primitive polynomials that can be used to generate the field: $p_0(x) = 1 + x + x^3$ and $p'(x) = 1 + x^2 + x^3$. How do we know these are primitive polynomials ?
Simply check that

$$p(0) = 1; \quad p(1) = 1$$

that is no zeros and no reducibility over GF(2).
Let us use $p(x) = 1 + x + x^3$. By setting $p(\alpha) = 0$ (primitive element is a zero of the primitive polynomial) we obtain the following relation,

$$p(\alpha) = 1 + \alpha + \alpha^3 = 0 \Rightarrow \alpha^3 = \alpha + 1$$

From this relation we obtain the polynomial representation of all field elements:

$$\begin{aligned}
\alpha^0 &= 1 \\
\alpha^1 &= \alpha \\
\alpha^2 &= \alpha^2 \\
\alpha^3 &= \alpha + 1 \\
\alpha^4 &= \alpha \cdot \alpha^3 = \alpha \cdot (\alpha + 1) = \alpha^2 + \alpha \\
\alpha^5 &= \alpha^2 + \alpha + 1 \\
\alpha^6 &= \alpha^2 + 1 \\
\alpha^7 &= 1
\end{aligned}$$

Verify that for e.g. $\alpha^5 = (\alpha^2 + 1)(\alpha^3 + \alpha + 1) + \alpha^2 + \alpha + 1 = \alpha^2 + \alpha + 1$. Table 1 lists the elements of $GF(2^3)$, with 4 equivalent representations.

3. (Arithmetic in GF(25)). Let GF(25) be represented by polynomials of degree < 2 with arithmetic modulo the polynomial $p(x) = x^2 + x + 2$, which is prime over GF(5). Perform the following calculations in GF(25).

   (a) Find $(2x + 3) \cdot (3x + 4)$.

   Arithmetic modulo $x^2 + x + 2$ is based on the equation $x^2 = -x - 2 = 4x + 3$. Thus,

   $(2x+3)\cdot(3x+4) = 6x^2+17x+12 \pmod 5 = x^2+2x+2 = (4x+3)+(2x+2) = 6x+5.$

   Note arithmetic on polynomial coefficients is performed modulo 5.

α^i	polynomial	binary $(a_0\ a_1\ a_2)$	decimal	order
0	0	000	0	–
α^0	1	100	1	1
α^1	α	010	2	7
α^2	α^2	001	4	7
α^3	$\alpha+1$	110	3	7
α^4	$\alpha^2+\alpha$	011	6	7
α^5	$\alpha^2+\alpha+1$	111	7	7
α^6	α^2+1	101	5	7

Table 1: Four different representations

(b) Find $(3x+1)^{-1}$.

Reciprocals in fields of dimension 2 can be found by several methods. First we use the extended Euclidean algorithm with inputs $3x+1$ and $p(x)$, which requires only one polynomial division.

$$x^2+x+2 = (2x+3)(3x+1)+4.$$

Therefore modulo x^2+x+2 over GF(5),

$$(2x+3)(3x+1)+4 = 0 \Rightarrow (2x+3)(3x+1) = 4 = 1.$$

We conclude that $(3x+1)^{-1} = 2x+3$.

Another method is to use direct substitution. Because the defining polynomial is of degree 2, all elements can be represented as polynomials over GF(5) of degree ≤ 1. Let $(3x+1)^{-1} = ax+b$, where a and b must be determined. Then,

$$\begin{aligned} 1 &= (3x+1)(ax+b) = 3ax+(a+3b)x+b \\ &= 3a(4x+3)+(a+3b)x+b \\ &= 12ax+9a+(a+3b)x+b \\ &= (13a+3b)x+(9a+b) = (3a+3b)x+(4a+b). \end{aligned}$$

By equating coecients on both sides of the expression, we obtain a system of linear equations.

$$\begin{aligned} 3a+3b &= 0 \\ 4a+b &= 1 \end{aligned}$$

Solving this system of equations yields $a=2$ and $b=3$. Thus $(3x+1)^{-1} = 2x+3$.

(c) Find the multiplicative order of $x+1$.

The order of $x+1$ is a divisor of 24, the order of the multiplicative group of GF(25). Therefore we need consider only powers that are proper divisors of 24, namely, 2, 3, 4, 6, 8, and 12.

$$\begin{aligned}
(x+1)^2 &= x^2+2x+1 = (4x+3)+(2x+1) = x+4 \\
(x+1)^3 &= (x+1)(x+4) = x^2+5x+4 \\
&= (4x+3)+4 = 4x+2 \\
(x+1)^4 &= ((x+1)^2)^2 = (x+4)^2 2 = x^2+8x+16 \\
&= (4x+3)+(3x+1) = 2x+4 \\
(x+1)^6 &= ((x+1)^3)^2 = (4x+2)^2 \\
&= 16x^2+16x+4 = (4x+3)+(x+4) = 2 \\
(x+1)^8 &= ((x+1)^4)^2 = (2x+4)^2 = 4x^2+16x+16 \\
&= (16x+12)+(x+1) = 2x+3 \\
(x+1)^{12} &= ((x+1)^6)^2 = 2^2 = 4
\end{aligned}$$

Since $(x+1)^d \neq 1$ for every proper divisor d of 24, we conclude that the order of $x+1$ is 24, that is, $x+1$ is a primitive element of GF(25).

4. (Fields and subfields)

(a) For the integers with the subtraction operator, which group axiom(s) are not satised ?

Subtraction is not associative. For example, $(1-1)-1 = -1 \neq 1 = 1-(1-1)$. Also, subtraction does not have a left identity element, since $e-a = a$ only when $a = e/2$.

(b) The number of vectors in a vector space V is 125. What is the dimension of V ?

Every finite-dimensional vector space is isomorphic to the n-tuples over the field of scalars. A finite vector space has a finite field of scalars, GF(q), and therefore q^n elements. Since V has $125 = 5^3$ elements, the scalar field is GF(5) and the dimension of V is 3.
Remark : A less satisfying but technically correct answer: scalars are GF(5^3) and the dimension of V is 1.)

(c) What is the smallest field that contains both GF(27) and GF(81) as subfields ?

Since GF(27) = GF(3^3) and GF(81) = GF(3^4), these are fields of characteristic 3. Any extension field GF(3^m) of GF(3^3) has an exponent m that is a multiple of 3, and any extension field GF(3^m) of GF(3^4) has an exponent m that is a multiple of 4. If GF(3^m) contains both GF(3^3) and GF(3^4) then m is a multiple of both 3 and 4. The least common multiple is 12, so the smallest common extension field is GF(3^{12}) = GF(531 441).

(d) List the subfields of GF(4^6).

The trick is to realize that GF(4^6) = GF(2^{12}). The subfields of GF(2^{12}) are GF(2^m) where m is a divisor of 12, namely, GF(2^{12}), GF(2^6), GF(2^4), GF(2^3), GF(2^2), and GF(2). Note that not every subfield of GF(4^6) is of the form GF(4^m); for example, GF(2^3).

5. (Computation in GF(2^m)) Describe how to evaluate the square root of an arbitrary element of the field GF(2^m) using only multiplications.

   In GF(2^m) every element β satisfies $\beta^{2^m} = \beta$. Therefore $\sqrt{\beta} = \beta^{2^{m-1}}$, and so the square root of any element can be found by squaring $m-1$ times. For example, the square root of x in GF(2^7) is $x^{64} \pmod{x^7 + x^3 + 1}$, which we can compute as follows:

$$\begin{aligned} x^8 &= x + x^4 \\ x^{16} &= x^2 + x^8 = x + x^2 + x^4 \\ x^{32} &= x^2 + x^4 + x^8 = x + x^2 \\ x^{64} &= x^2 + x^4 \end{aligned}$$

6. (Computations in GF(1009)). In this exercise we compute the inverse in the group and perform exponentiation using the group structure. We use the fact that 1009 is prime.

   (a) In GF(1009) find 999^{1012}. Hint: calculator not needed.

   Since $\beta^{1008} = 1$ for every nonzero element β of GF(1009),

$$999^{1012} = (-10)^{1012-1008} = (10)^4 = 1000 \cdot 10 = -9 \cdot 10 = -90 = 919.$$

   (b) Let us consider the construction of $GF(4)$ by adjoining the root of irreducible polynomial $x^2 + x + 1 \in \mathbb{F}_2[x]$.

   Thus we start with $GF(2) = \{0, 1\}$ and consider

$$f(x) = x^2 + x + 1$$

   of degree 2. Let α be a root of $f(\alpha) = 0$, i.e.,

$$\alpha^2 + \alpha + 1 = 0$$

   so that $\alpha^2 = \alpha + 1$. Then we extend $GF(2)$ and consider $\mathbb{F}_2(\alpha)$ which now have 3 elements $0, 1, \alpha$. Clearly, we must have the element $\alpha + 1$ as an element of $\mathbb{F}_2(\alpha)$ since $\mathbb{F}_2(\alpha)$is closed under addition. Then it can be easily checked that

$$\{0, 1, \alpha, \alpha^2 = \alpha + 1\}$$

   is a finite field of $2^m = 4$ elements.

7. The error trapping algorithm will only correct error patterns $e(x)$ where, for some i, $x^i e(x) \pmod{1 + x^n}$ has degree at most $n - k$. It is quite possible that there are error patterns of weight at most t that do not satisfy this property. Such error patterns are correctable by the code, but the closest codeword is not found with this algorithm.

   Let $n = 7$, let $g(x) = 1 + x + x^3$ be the generator polynomial for the 1-error-correcting (so $t = 1$) linear cyclic code. If $w(x) = x^2 + x^3$ is received then

$$s(x) = w(x) \pmod{g(x)} = x^2 + x^3 \pmod{1 + x + x^3} = 1 + x + x^2$$

is the syndrome polynomial. We next compute

$$s_1(x) = xs(x) \pmod{g(x)} = x(1 + x + x^2) \pmod{g(x)} = 1 + x^2$$

$s_2(x) = x^2 s(x) \pmod{g(x)} = x(1 + x^2) \pmod{g(x)} = 1$; which has weight $1 \leq t$. That is what we want; the algorithm stops and corrects the error. So $j = 2$ and therefore

$$e(x) = x^{7-2} s_2(x) \pmod{1 + x^7} = x^5$$

Thus

$$c(x) = w(x) + e(x) = (x^2 + x^3) + x^5$$

is the most likely codeword.

8. (Factoring polynomials - counting cyclic codes) In this exercise we use some shortcuts to find out the factorization of polynomials of the form $x^n - 1$. This then allows for counting the number of cyclic codes over some finite field.
Factor $x^8 - 1$ over GF(3) and find the number of cyclic codes over GF(3) of blocklength 8. The following hint is proved useful: all factors are linear or quadratic.

   The following obvious partial factorization holds over any ring with identity:

$$\begin{aligned} x^8 - 1 &= (x^4 - 1)(x^4 + 1) = (x^2 - 1)(x^2 + 1))(x^4 + 1) = \\ &= (x - 1)(x + 1)(x^2 + 1)(x^4 + 1) \end{aligned}$$

   The polynomial $x^2 + 1$ is irreducible, as can be verified by trying all possible linear factors $(x, x + 1, x + 2)$ or, equivalently, by checking that neither 0, 1, nor 2 is a zero. We know that $x^4 + 1$ must factor into two irreducible quadratic factors, since the zeroes of $x^8 - 1$ are the nonzero elements of GF(9). This comes from the fact that any nonzero element $a \in GF(9)$ satisfies $a^8 = 1$ (the order of multiplicative group is 8 and order of any element divides the order of the group (Lagrange)). By checking a few quadratic polynomials, we find that

$$x^4 + 1 = (x^2 + x + 2)(x^2 + 2x + 2).$$

   Therefore the complete factorization is,

$$x^8 - 1 = (x - 1)(x + 1)(x^2 + 1)(x^2 + x + 2)(x^2 + 2x + 2).$$

   Remark that these irreducible quadratic polynomials are used to construct $GF(9)$, and the roots of $x^8 - 1$ are also the roots of $(x^2 + x + 2)$ or $(x^2 + 2x + 2)$.

   There are five distinct prime factors, so there are $2^5 = 32$ divisors of $x^8 - 1$ and therefore 32 cyclic codes of blocklength 8 over GF(3), including the trivial codes of rate 0 ($g(x) = x^8 - 1$) and rate 1 ($g(x) = 1$).

Each nonzero element of GF(9) is a zero of one of the prime factors of $x^8 - 1$, so each cyclic code over GF(3) of blocklength 8 is characterized by a set of elements of GF(9) that are the zeroes of all codewords. These elements correspond to the choice of $g(x)|x^n - 1$.

9. (Burst error detecting): Show that cyclic codes are "optimal" for burst error detecting. That is, every (shortened) cyclic code with generator polynomial of degree r can detect all burst errors of length r.

We must show that no burst of length $\leq r$ is a codeword. See the lecture notes (Implementation of cyclic codes) for the reasoning. Simply if $c(x) = m(x)g(x)$ and we add an error polynomial $e(x)$ to get a codeword $c'(x) = c(x) + e(x)$ we must have that $c'(x) \equiv 0 \pmod{g(x)}$ then we must have $e(x) \equiv 0 \pmod{g(x)}$.

Such a burst is of the form

$$e(x) = x^i + x^{i+1} + \cdots + x^{i+r-1} = x^i(1 + x + \cdots + x^{r-1}) = x^i b(x)$$

where $b(x) \neq 0$ and $\deg b(x) < r$. Now since the constant coefficient of $g(x)$ is nonzero $g(x)$ and x^i are relatively prime.

Thus if $g(x)|x^i b(x)$ then $g(x)|b(x)$. This is not possible since $\deg b(x) < \deg g(x)$. The burst error detecting ability is exactly r because $g(x)$ is a codeword that is a burst of length $r+1$. Otherwise $g(x)$ would be detected as a burst error.

Optional Most burst errors of length $> r$ can be detected. For binary alphabets we have:

$$\text{P(burst of length l is detected)} = \begin{cases} 1 - 2^{-r+1} & l = r+1 \\ 1 - 2^{-r} & l > r+1 \end{cases}$$

10. (Subfields of GF(2^6) The following primitive polynomials over GF(2),

$$x^3 + x + 1, \;\; x^2 + x + 1, \;\; x^6 + x + 1,$$

have zeroes α, β, and γ, respectively. That is, $\alpha^3 + \alpha + 1 = 0$, $\beta^2 + \beta + 1 = 0$, and $\gamma^6 + \gamma + 1 = 0$.

(a) What is the smallest field that contains α ?

The minimal polynomial of α has degree 3, so α is primitive in GF(2^3) = GF(8).

(b) What is the smallest field that contains β, repeat for γ ?

The minimal polynomial of β has degree 2, so β is primitive in GF(2^2)) = GF(4). Similarly, GF(2^6) is the smallest field than contains γ.

(c) Express α as a power of γ.

Note that GF(8)$\subset$ GF(64) so the question has sense. The order of α is 7. The elements of GF(64) of order 7 are $\gamma^{(63/7)i}$ for $i = 1, \ldots, 6$. Thus, $\alpha = \gamma^{9i}$ for some value of i in the range $1, \ldots, 6$.

(d) What is the smallest field that contains $\alpha + \beta$?

The only elements common to GF(4) and GF(8) are 0 and 1. Thus α is not in GF(4) and β is not in GF(8). It follows that $\alpha + \beta$ does not belong to either GF(4) or GF(8), since

$$\alpha + \beta \in GF(4) \Rightarrow (\alpha + \beta) - \beta = \alpha \in GF(4) \Rightarrow \text{ contradiction,}$$
$$\alpha + \beta \in GF(8) \Rightarrow (\alpha + \beta) - \alpha = \beta \in GF(8) \Rightarrow \text{ contradiction,}$$

Thus the smallest field that contains $\alpha + \beta$ must be the smallest field that contains GF(4) and GF(8), which is GF(64).

(e) Find the multiplicative order of $\alpha\beta$.

The multiplicative order n of $\alpha\beta$ is the least common multiple of 7 and 3, the multiplicative orders of α and β. Thus $n = 21$. We can check this easily.

$$(\alpha\beta)^{21} = \alpha^{21}\beta^{21} = \alpha^{7\cdot 3}\beta^{3\cdot 7} = 1^3 1^7 = 1.$$

How do we know that the order is not smaller than 21? From the previous equation we know that the order must be a divisor of 21, and neither 1, 3, nor 7 works,

$$\begin{aligned}(\alpha\beta)^1 &= \alpha\beta \neq 1 \ \ (since \ \ \alpha\beta \notin GF(4)) \\ (\alpha\beta)^3 &= \alpha^3\beta^3 = \alpha^3 \neq 1 \\ (\alpha\beta)^7 &= \alpha^7\beta^7 = \beta^7 = \beta^{7 \bmod 3} = \beta \neq 1\end{aligned}$$

11. If f is an irreducible polynomial in $\mathbb{F}_q[x]$ of degree m, then f has a root α in $\mathbb{F}_{q^m}$. Furthermore, all the roots of f are simple and given by the m distinct elements $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ of $\mathbb{F}_{q^m}$.

Let α be a root of f in the splitting field of f over $\mathbb{F}_q$. Then, since $deg(f) = m$ we have that the field $\mathbb{F}_q(\alpha)$ (which is an extension field of $\mathbb{F}_q$ obtained by adjoining α to $\mathbb{F}_q$) satisfies $[\mathbb{F}_q(\alpha) : F_q] = m$ (dimension of the vector space over $\mathbb{F}_q$) and therefore $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$. In particular $\alpha \in \mathbb{F}_{q^m}$.

We already had one such example when we constructed the field $\mathbb{F}_{2^2}$ using the irreducible polynomial $p(x) = x^2 + x + 1$, that is $m = 2$. Adjoining α as a root of $x^2 + x + 1$ (meaning $p(\alpha) = 0$) implies that we extend our prime field $\mathbb{F}_2 = \{0, 1\}$ to contain the element α,

$$\mathbb{F}_2 \cup \alpha = \{0, 1, \alpha\}$$

But then for the closure property of the field we have to include the element $1 + \alpha$ so that,

$$\mathbb{F}_{2^2} = \{0, 1, \alpha, 1 + \alpha\}.$$

Next we show that if $\beta \in \mathbb{F}_{q^m}$ is a root of f then also $f(\beta^q) = 0$. Write,

$$f(x) = a_m x^m + a_{m-1}x^{m-1} + \ldots + a_1 x + a_0; a_i \in \mathbb{F}_q.$$

Then,

$$\begin{aligned} f(\beta^q) &= a_m\beta^{qm} + \ldots + a_1\beta^q + a_0 = a_m^q\beta^{qm} + \ldots + a_1^q\beta^q + a_0 = \\ &\quad (a_m\beta^m + \ldots + a_1\beta + a_0)^q = f(\beta)^q = 0. \end{aligned}$$

The second equality comes from the Lemma 2.7 !

12. (Euler's ϕ function) In this exercise we use the Euler's ϕ function to count the number of integers that are coprime to n. Let $n = \prod_{i=1}^{k} p_i^{e_i}$ be a factorization of positive integer n. Then,

$$\phi(n) = \prod_{i=1} n(p_i^{e_i} - p_i^{e_i - 1})$$

. Then we can compute the following cardinalities of the numbers coprime to n.

$$\begin{aligned} \phi(193) &= 192 \\ \phi(284) &= \phi(2^2 \cdot 71) = (2^2 - 2^1)(71 - 1) = 140 \\ \phi(440) &= \phi(2^3 \cdot 5 \cdot 11) = (2^3 - 2^2)(5 - 1)(11 - 1) = 160 \end{aligned}$$

13. (Prime quadratic polynomials.) In this exercise we investigate the number of prime quadratic polynomial over extension fields of prime order $p = 2$. We know that over GF(2) the choice of prime quadratic polynomial is unique i.e. $p(x) = x^2 + x + 1$.
a) How many distinct second-degree monic polynomials of the form $x^2 + ax + b(b \neq 0)$ are there over GF(16)?

    There are 16 choices for a and 15 choices for $b = 0$. Therefore the number of monic polynomials of degree 2 over GF(16) is $16 \cdot 15 = 240$.

    b) How many distinct polynomials of the form $(x - \beta)(x - \gamma)$ are there over GF(16)?

    There are 15 choices for $\beta \neq 0$ and 15 choices for $\gamma \neq 0$. However, since order is not important, the number of ways to form $(x - \beta)(x - \gamma)$ is the number of ways to pick two different elements from a set of 15 plus the number of ways to pick a pair of identical elements, that is,

$$\binom{15}{2} + 15 = 120.$$

    c) Does this prove that an irreducible second-degree polynomial exists ? How many second-degree prime polynomials over GF(16) are there ?

    Every reducible monic polynomial of degree 2 with nonzero constant term can be factored as $(x - \beta)(x - \gamma)$ with $\beta, \gamma \neq 0$. Since the number of ways of factoring is smaller than the number of polynomials of degree 2, the difference consists of prime polynomials.
    Hence there are $240120 = 120$ irreducible monic (i.e., prime) quadratic polynomials over GF(16).
    Each such polynomial has two zeroes that belong to GF(256)GF(16). Since the number of primitive elements in GF(256) equals to $\phi(255) = \phi(3{\cdot}5{\cdot}17) = 2{\cdot}4{\cdot}16 = 128$ there are 128 primitive elements and therefore 64 primitive polynomials of degree 2 over GF(16). The remaining 56 prime polynomials are not primitive.

14. Find the number of cyclic codes over GF(3) of blocklength 80. Idea is that it is not necessary to actually factor $x^{80}-1$ to do this.

    The prime factors of $x^{80}-1$ over GF(3) are the minimal polynomials over GF(3) of all nonzero elements of GF(81). There are two nonzero elements in GF(3) and six elements of GF(9)-GF(3). Therefore $x^{80}-1$ has two prime factors of degree 1 ($x-1$ and $x-2$ corresponding to the nonzero elements of GF(3)).

    In addition there are three prime factors of degree 2 that correspond to these six elements.

    Here it is important to notice that for an $\alpha \in GF(3^2) - GF(3)$ the algebraic extension over GF(3) is of order 2 and this must be the degree of the minimal polynomials. These elements clearly cannot have a minimal polynomial of degree 1 as $x - \alpha = 0$ has no solution in GF(3) for $\alpha \in GF(9) - GF(3)$. Also note that the the conjugates of α are

    $$\alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$$

    and since in our case $\alpha \in GF(3^2) - GF(3)$ we have $m = 2$. Let us assume that α is a primitive element of $GF(3^2)$ and α^3 is a conjugate over $GF(3)$. But then taking α^3 as another element of $\alpha \in GF(3^2) - GF(3)$ we see that its conjugate is $(\alpha^3)^3 = \alpha^9 = \alpha$ hence the two elements have the same minimal polynomial.

    Reasoning in the same way there are $(81-9)/4 = 18$ prime factors of degree 4. In all, $x^{80}-1$ has $2+3+18 = 23$ distinct prime factors. Thus there are $2^{23} = 8388608$ generator polynomials of cyclic codes over GF(3) of blocklength 80.

15. (Cyclic codes I): Let C_1 and C_2 be cyclic codes of blocklength n generated by $g_1(x)$ and $g_2(x)$, respectively.

    (a) Find the the generator polynomial of the smallest cyclic code that contains $C_1 \cup C_2$, that is, all the codewords of C_1 and C_2.

    (b) The intersection of cyclic codes is cyclic. Find the generator polynomial of $C_1 \cap C_2$.

    (a) The generator polynomial of C, the smallest cyclic code that contains the union $C_1 \cup C_2$, is

    $$g(x) = \gcd(g_1(x), g_2(x)).$$

    Both $g_1(x)$ and $g_2(x)$ are codewords of C, so $g(x)$ is a divisor of $g_1(x)$ and $g_2(x)$, and the codewords of C_1 and C_2 are multiples of $g_1(x)$, respectively $g_2(x)$. Therefore $g(x)$ generates a code that contains $C_1 \cup C_2$ and therefore contains C.

    Conversely, since (Extended Euclidean Algorithm)

    $$\begin{aligned} \gcd(g_1(x), g_2(x)) &= a(x)g_1(x) + b(x)g_2(x) \\ &= (a(x)g_1(x) + b(x)g_2(x)) \pmod{x^n - 1}, \end{aligned}$$

we see that $g(x)$ is a linear combination of cyclic shifts of vectors from $C_1 \cup C_2$. Hence any cyclic code containing $C_1 \cup C_2$ in particular, C must include $g(x)$ and all of its polynomial multiples; that is, C contains the code generated by $g(x)$.

(b) The generator polynomial of $C_1 \cap C_2$ is

$$g(x) = lcm(g_1(x), g_2(x)).$$

Every codeword in the intersection of two cyclic codes is divisible by both generator polynomials and therefore by their least common multiple.

Conversely, every multiple of the least common multiple belongs to both codes, hence to their intersection. When $g_1(x)$ and $g_2(x)$ are relatively prime, their least common multiple is their product. In this case, the generator polynomial of the intersection of two cyclic codes is $g_1(x)g_2(x)$.

16. (Cyclic codes II): In this problem we consider using other generator polynomials than the lowest degree monic polynomial $g(x)$. Recall that for a cyclic code of length n we can write,

$$g(x) = \prod_{i \in K} (x - \alpha^i),$$

as $g(x)$ is a divisor of $x^n - 1$, and K is a union of some cyclotomic cosets. For instance let $n = 9$ and then we have,

$$\begin{aligned} C_0 &= \{0\} \\ C_3 &= \{3, 6\} \\ C_1 &= \{1, 2, 4, 8, 7, 5\} \end{aligned}$$

Then taking $K = C_0 \cup C_3$ means that $g(x) = (x + 1)m_3(x)$ where $m_3(x)$ is the minimal polynomial of α^3. Now a codeword $c(x) \in C$ if and only if $c(\alpha^i) = 0$ for all $i \in K$.
Next we show that if $p(x) \in \mathbb{F}[x]/(x^n - 1)$ does not introduce any new zeros, i.e. $p(\alpha^i) \neq 0$ for all $i \notin K$, then $g(x)$ and $p(x)g(x)$ generates the same code.

Obviously the ideal generated by $p(x)g(x)$ is a subideal of the $< g(x) >$, i.e.,

$$< g(x) \supseteq p(x)g(x).$$

The n-th roots of unity

$$\{\alpha^i : i \in K\}$$

are called the zeros of the code. The other n-th roots of unity for which

$$g(\alpha^i) \neq 0$$

($i \notin K$) are then the roots of $h(x) = (x^n - 1)/g(x)$. Therefore, $h(x)$ and $p(x)$ are relatively prime (as $p(\alpha^i) \neq 0$ for $i \notin K$), i.e., $gcd(p(x), h(x)) = 1$. Thus, by Extended Euclidean Algorithm,

$$\begin{aligned} 1 &= a(x)p(x) + b(x)h(x) && \text{in } F[x] \\ g(x) &= a(x)p(x)g(x) + b(x)h(x)g(x) && \text{in } F[x] \\ &= a(x)p(x)g(x) && \text{in } F[x]/(x^n - 1) \end{aligned}$$

This implies that $< g(x) > \subseteq < p(x)g(x) >$ and therefore $< g(x) > = < p(x)g(x) >$. As a special case the codes generated by $g(x)$ and $g^2(x)$ are the same.

item (Shuffled codewords): Prove the following statement: A binary cyclic code of odd blocklength n is invariant under the permutation $c(x) \rightarrow c(x^2) \pmod{x^n - 1}$. Discuss the effect of this permutation on the codewords.

Solution: There is a simple algebraic proof. Over GF(2) squaring is linear, so $c(x^2) = c(x)^2$. Let $h(x)$ be the check polynomial of this cyclic code. Then since

$$c(x)h(x) \pmod{x^n - 1} = 0,$$

$$c(x^2) \pmod{x^n - 1}h(x)) \pmod{x^n - 1} =$$
$$c(x)^2 h(x) \pmod{x^n - 1} = 0,$$

which confirms that

$$c(x^2) \pmod{x^n - 1}$$

is also a codeword.

To analyse the effect of this permutation let us investigate what happens to the components of the codewords. The transformation

$$c(x) \rightarrow c(x^2) \pmod{x^n - 1}$$

is linear, so we first study its effect on unit vectors, i.e., monomials x_i , where $0 \leq i < n$. If $i \leq (n1)/2$ then $2i \leq n1$, hence

$$x^i \rightarrow x^{2i} \pmod{x^n - 1} = x^{2i}$$

If $i > (n-1)/2$ then $i \geq (n+1)/2$, hence $i = (n+k)/2$ for an odd integer k where $1 \leq k \leq n$. There are

$$n - (n-1)/2 - 1 = (n-1)/2$$

such numbers. For $k = 1$,

$$x^i \rightarrow x^{2i} \pmod{x^n - 1} = x^{n+1} \pmod{x^n - 1} = x.$$

In general, for odd k,

$$x^{(n+k)/2} \rightarrow x^{n+k} \pmod{x^n - 1}$$
$$= (x^k \cdot x^n) \pmod{x^n - 1} = x^k.$$

The result of the transformation is the vector,

$$(c_0, c_{\frac{n+1}{2}}, c_1, c_{\frac{n+3}{2}}, \ldots, c_i, c_{\frac{n+1+2i}{2}}, \ldots, c_{n-2}, c_{\frac{n-3}{2}}, c_{n-1}, c_{\frac{n-1}{2}}).$$

This vector is obtained by splitting the original vector into two parts, the first $(n+1)/2$ components and the last $(n-1)/2$, then shuffling the two parts, starting with the first original component.

17. Weights of the codewords in a cyclic code Let $g(X)$ be the generator polynomial of a binary cyclic code of length n.

a) Show that if $g(X)$ has $X+1$ as a factor then the code contains no codewords of odd weight.

A polynomial $v(X) \in GF(2)[X]$ is a code polynomial **iff** it is of degree at most $n-1$ and can be written as $v(X) = u(X)g(X)$ for some polynomial $u(X) \in GF(2)[X]$. Since $X+1$ divides $g(X)$ by assumption, it follows that $X+1$ divides $v(X)$. Hence $v(1) = 0$. This means precisely that the weight of the corresponding codeword $(v_0, \ldots, v_{n-1})$ is even.

b) Show that if n is odd and $X+1$ is not a factor of $g(X)$ then the code contains the codeword consisting of all 1's.

The claim of this part of the problem is true whether n is odd or even

$$X^n + 1 = (X+1)(1 + X + X^2 + \ldots + X^{n-1})$$

Since $g(X)$ divides $X^n + 1$ and does not have $X+1$ as a factor, it must divide $1 + X + X^2 + \ldots + X^{n-1})$. In other words, the length n word consisting of all 1's is a codeword.

c) Show that if n is the smallest integer such that $g(X)$ divides $X^n + 1$ then the code has minimum weight at least 3.

If there is a codeword of weight 1, the associated code polynomial is X^m, for some $0 \leq m \leq n-1$. Since the code is cyclic, it follows that 1 is also a code polynomial. But then the code is trivial (every word is a codeword), and $g(X) = 1$, contradicting the hypothesis.
If there is a codeword of weight 2, the associated code polynomial is $X^m + X^l$ for some $0 \leq m < l \leq n-1$. Since the code is cyclic, it follows that $1 + X^{l-m}$ is also a code polynomial. Hence $g(X)$ divides $1 + X^{l-m}$, which contradicts the hypothesis since $l - m < n$.
Thus under the hypothesis the smallest weight of a nonzero codeword must be at least 3.

d) Suppose $g(X)$ is such that the corresponding code C of length n contains both even-weight and odd-weight codewords. Show that the polynomial $(X+1)g(X)$ also generates a binary cyclic code C_1 of length n, and that this code contains the even weight codewords of C.

Let C denote the binary cyclic code (n, k) with generator polynomial $g(X)$. We know that $g(X)$ divides $X^n + 1$. Since C contains both even and odd weight codewords, $X+1$ does not divide $g(X)$ (see part a)). Thus $(X+1)g(X)$ divides $X^n + 1$. Hence it is the generator polynomial of a binary cyclic $(n, k-1)$ code. Let C_1 denote this code. We claim that C_1 is comprised of the even weight codewords of C.

Consider a codeword of C. The corresponding code polynomial can be uniquely

written in the form $a(X)g(X)$, where $a(X) \in GF(2)[X]$ is of degree at most $k-1$. The codeword has even weight iff its code polynomial is divisible by $X+1$ (see again part a)).

Since $X+1$ does not divide $g(X)$, it follows that the codeword has even weight iff $X+1$ divides $a(X)$, i.e. $a(X) = b(X)(X+1)$ for some $b(X) \in GF(2)[X]$. But this means the code polynomial has the form $b(X)((X+1)g(X))$, so the corresponding codeword is in C_1.
For the converse, consider a codeword in C_1. Its code polynomial is of the form $b(X)(X+1)g(X)$ for a unique $b(X) \in GF(2)[X]$ of degree at most $k-2$. Writing this as $(b(X)(X+1))g(X)$ we see that the codeword is in C and has even weight.

18. (Subfields and conjugates): Let α be a primitive element of GF(1024).

    (a) List the elements in the subelds GF(4) and GF(32) as powers of α.

    (b) Find the conjugates of α with respect to the subelds GF(2), GF(4), and GF(32).

    (a) In general, the subfield $GF(q)$ of $GF(Q)$ consists of the q elements of $GF(Q)$ that are zeroes of $x^q - x$. If α is a primitive element of $GF(Q)$, then the nonzero elements of $GF(q)$ are powers of $\alpha^{(Q-1)/(q-1)}$, which is a primitive element of $GF(q)$. Indeed, $(\alpha^{(Q-1)/(q-1)})^{q-1} = 1$ and there is no integer $< q-1$ satisfying this. In particular, the subfields GF(4) and GF(32) of GF(2^{10}) are generated by primitive elements $\alpha^{1023/3} = \alpha^{341}$ and $\alpha^{1023/31} = \alpha^{33}$, respectively. The elements of these subfields can be represented as powers of α^{341} and α^{33}:

$$\begin{aligned} GF(4) &= \{0, 1, \alpha^{341}, \alpha^{682}\} \\ GF(32) &= \{0, 1, \alpha^{33}, \alpha^{66}, \alpha^{99}, \alpha^{132}, \ldots, \alpha^{924}, \alpha^{957}, \alpha^{990}\} \end{aligned}$$

    (b) Over GF(2), GF(4), and GF(32), the primitive element α of GF(1024) has 10, 5, and 2 conjugates, respectively:

$$\begin{aligned} GF(2) &= \{\alpha, \alpha^2, \alpha^4, \ldots, \alpha^{256}, \alpha^{512}\} \\ GF(4) &= \{\alpha, \alpha^4, \alpha^{16}, \alpha^{64}, \alpha^{256}\} \\ GF(32) &= \alpha, \alpha^{32} \end{aligned}$$

19. (BCH codes): The polynomial $p(y) = y^3 + 2y + 1$ is primitive over GF(3). Minimal polynomials for selected elements of GF(27) are listed below.

$$\begin{array}{cc} m_{\alpha^0}(x) = x - 1 & m_{\alpha^4}(x) = x^3 + x^2 - 1 \\ m_{\alpha^1}(x) = x^3 - x + 1 & m_{\alpha^5}(x) = x^3 - x^2 + x + 1 \\ m_{\alpha^2}(x) = x^3 + x^2 + x - 1 & m_{\alpha^6}(x) = x^3 + x^2 + x - 1 \\ m_{\alpha^3}(x) = x^3 - x + 1 & \end{array}$$

    (a) Without completing this list, state how many distinct minimal polynomials there are for elements of GF(27).

    (b) Find the generator polynomial for a (26, 19) double-error correcting BCH code over GF(3).

(c) Determine the rate, dimension and minimum distance of this code?

(a) First note that the polynomial $p(y) = y^3+2y+1$ is primitive, which means that taking the powers of y we get all the nonzero elements of $GF(3^3)$. Of course the arithmetic is performed mod y^3+2y+1, i.e. using $y^3 = -2y-1 = y+2$. Therefore $y^4 = y \cdot y^3 = y^2 + 2y$ etc. For the computation below we use $y^9 = y + 1$. This element y is denoted as α and called a primitive element in $GF(3^3)$ since $\alpha^{26} = 1$ and $\alpha^j \neq 1$ for $1 \leq j < 26$.
The only proper subfield of GF(27) is GF(3). The minimal polynomials for the elements in $GF(3)$ are trivially $x - a$ for $a \in \{0, 1, 2\}$. The minimal polynomial associated with element $a = 0$ is never used as a factor for generator polynomials.
Therefore there are 27 - 3 = 24 elements in GF(27)-GF(3), and each of these elements has a minimal polynomial of degree 3. To see this we note that these 24 elements are divided into conjugacy classes, each class containing 3 elements, e.g.

$$C(\alpha) = \{\alpha, \alpha^3, \alpha^{3^2} = \alpha^9, \alpha^{3^3} = \alpha\},$$

. Of course, the repetition of α in $C(\alpha)$ is just for the purpose of demonstration and $C(\alpha) = \{\alpha, \alpha^3, \alpha^{3^2} = \alpha^9\}$. The elements in the same class have the same minimal polynomial, $C(\alpha) = C(\alpha^3) = C(\alpha^9)$. For instance,

$$C(\alpha^3) = \{\alpha^3, \alpha^{3^2} = \alpha^9, \alpha^{3^3} = \alpha\}.$$

The minimal polynomial is defined as

$$\begin{aligned} m_\alpha(x) &= \prod_{\beta \in C(\alpha)} = (x-\alpha)(x-\alpha^3)(x-\alpha^9) = \\ &= x^3 + x^2(-\alpha - \alpha^3 - \alpha^9) + x(\alpha^{12} + \alpha^4 + \alpha^{10}) - \alpha^{13} = \\ &= x^3 + x^2[2\alpha + 2(\alpha+2) + 2(\alpha+2)^3] + \\ &\quad x(\alpha^2 + 2 + \alpha^2 + 2\alpha + \alpha^2 + \alpha) - 2 = \\ &= x^3 + x^2[\alpha + 1 + 2(\alpha+1)] + 2x - 2 = \\ &= x^3 + 2x - 2. \end{aligned}$$

Taking α^2 we get the conjugacy class

$$C(\alpha^2) = \{\alpha^2, (\alpha^2)^3 = \alpha^6, (\alpha^2)^{3^2} = \alpha^{18}, \alpha^{54} = \alpha^2\}.$$

Thus there are 8 minimal polynomials of degree 3 and 3 minimal polynomials of degree 1 for the ground field GF(3).

(b) The generator polynomial for a (26, 19) cyclic code is the product of minimal polynomials and since $k = 19$ we need $\deg(g) = 7$. To get the designed distance $\delta = 5$ we need to choose 4 consecutive roots (consecutive powers of α) as a subset of the roots of $m_i(x)$. If we choose 0 as the first power, then since α^3 is a conjugate over GF(3) of α, only three minimal polynomials are needed.

$$g(x) = LCM(m_{\alpha^0}(x), m_{\alpha^1}(x), m_{\alpha^2}(x), m_{\alpha^3}(x))$$

$$
\begin{aligned}
&= m_{\alpha^0}(x) m_{\alpha^1}(x) m_{\alpha^2}(x) \\
&= (x-1)(x^3 - x + 1)(x^3 + x^2 + x - 1) \\
&= x^7 - x^5 - x^4 + x^3 - x^2 + 1 \\
&= x^7 + 2x^5 + 2x^4 + x^3 + 2x^2 + 1.
\end{aligned}
$$

The set of the roots of these minimal polynomials is,

$$R = \{1, \alpha, \alpha^3, \alpha^9, \alpha^2, \alpha^6, \alpha^{18}\}.$$

Thus we have 4 consecutive powers of α in the set of roots of $g(x)$, i.e., $\alpha^0, \alpha^1, \alpha^2, \alpha^3$. Therefore $d \geq 5$.

(c) The rate of the code is $k/n = 19/26 = 0.731$. There are 3^{19} codewords. The minimum distance is at least 5 by design, using the BCH bound. The generator polynomial is a codeword of Haming weight 6, so the minimum distance is at most 6.
But if we check `www.codetables.de` then the upper and lower bound for a linear code over GF(3) equals to $d = 5$, i.e. (26,19,5) is the best possible linear code for fixed $n = 26$ and $k = 19$.

20. (Hamming codes over extension fields): Find the generator polynomial of a (9, 7) Hamming code over GF(8). (The purpose of this exercise is to demonstrate the construction over extension fields.)

Solution: The blocklength of a Hamming code over $GF(8)$ is of the form $n = (8^m - 1)/(8 - 1)$, where $m \geq 2$. Blocklength 9 corresponds to $m = 2$. The parity check matrix is of the form (per definition of Hamming codes),

$$H = [1 \ \beta \ \beta^2 \ \ldots \ \beta^8]$$

where β is an element of multiplicative order 9 in some extension field of GF(8). The suitable extension field is clearly GF(64) since $m = 2$.

There are $\phi(9) = 6$ elements of order 9, each of which has a minimal polynomial of degree 2. Thus there are $6/2 = 3$ possible generator polynomials.
Let β be an element of GF(64) of order 9. The conjugate of β over GF(8) is β^8. But $\beta^8 = \beta^1$ since $\beta^9 = 1$. Thus the minimal polynomial of β is,

$$(x + \beta)(x + \beta^8) = x^2 + (\beta + \beta^8)x + \beta \cdot \beta^8 = x^2 + ax + 1,$$

where $a = \beta + \beta^8$ is an element of GF(8) (check for the definition of minimal polynomials).
To determine which values of a correspond to prime polynomials, we must choose a representation for GF(8). We use the representation based on the primitive polynomial $x^3 + x + 1$, which can be summarized in the following table. The binary representations of the powers of the primitive element α that is a zero of the primitive polynomial $x^3 + x + 1$ are given so that the least significant bit comes first. (For example, $\alpha^4 = \alpha + \alpha^2 = 011$.)

i	0	1	2	3	4	5	6	7
α^i	100	010	001	110	011	111	101	100

To determine which polynomials of the form $x^2 + ax + 1$ are prime over GF(8), we first find the polynomials that are not prime, that is, have two linear factors. The coefficient of the linear term in the product

$$(x + \alpha^i)(x + \alpha^i)$$

is

$$\alpha^i + \alpha^{7-i}.$$

These coefficients are listed in the following table.

i	$\alpha^i + \alpha^{7-i}$
0	$100 + 100 = 000 = 0$
1	$010 + 101 = 111 = 7 = \alpha^5$
2	$001 + 111 = 110 = 3 = \alpha^3$
3	$110 + 011 = 101 = 5 = \alpha^6$
4	$011 + 110 = 101 = 5 = \alpha^6$
5	$111 + 001 = 110 = 3 = \alpha^3$
6	$101 + 010 = 111 = 7 = \alpha^5$

Therefore, the coefficient $a \notin \{1, \alpha^3, \alpha^5, \alpha^6\}$ if the polynomial $x^2 + ax + 1$ is to be prime. In other words the prime polynomials are,

$$x^2 + \alpha x + 1$$
$$x^2 + \alpha^2 x + 1$$
$$x^2 + \alpha^4 x + 1$$

Note that the coefficients of x in these three polynomials are conjugates over GF(2). This is consistent with the principle that conjugates are indistinguishable when viewed from the subfield.

21. (Ternary Golay code) a) Find the generator polynomial of a cyclic $(11, 6, d)$ ternary code. If $d = 5$ this code corresponds to a so-called ternary Golay code.

Solution: We first discuss the possible choices for the generator polynomial form the blocklength n and the dimension of the code k.

The generator polynomial $g(x)$ is a divisor over GF(3) of $x^{11} - 1$ of degree $n - k = 11 - 6 = 5$. Therefore the zeroes of $g(x)$ are five of the ten elements of $GF(3^5)$ that are of multiplicative order 11.
Let β be one of the zeros of $x^{11}-1$. Then its conjugates over GF(3) are $\beta^3, \beta^9, \beta^{27} = \beta^5, \beta^{15} = \beta^4$. The remaining five elements of order 11 are reciprocals of these conjugates and are zeroes of the reciprocal polynomial of $g(x)$. Thus there are two $(11, 6, d)$ cyclic codes over GF(3), and their generator polynomials have the following factorizations,

$$\begin{aligned} g_1(x) &= (x - \beta)(x - \beta^3)(x - \beta^4)(x - \beta^5)(x - \beta^9) \\ g_2(x) &= (x - \beta^2)(x - \beta^6)(x - \beta^7)(x - \beta^8)(x - \beta^{10}) \end{aligned}$$

Since both generator polynomials are divisors of $x^{11}-1$,

$$x^{11}-1=(x-1)g_1(x)g_2(x)\Rightarrow g_1(x)g_2(x)=x^{10}+x^9+\cdots+x^2+x+1.$$

Let us assume that $g_1(x)$ is the generator polynomial of our code. We can find the coefficients of $g_1(x)$ by several methods:

- Multiply the linear factors over $GF(3^5)$. This requires a representation of $GF(3^5)$, e.g., as polynomials modulo a primitive polynomial over GF(3) of degree 5.
- Factor $x^{11}-1$ by checking polynomials of degree 5 (tedious).
- Use the fact that $g_1(x)$ and $g_2(x)$ are divisors of $x^{10}+x^9+x8+\ldots+x^2+x+1$ and are reciprocal polynomials to find conditions that determine their coefficients.

The first two methods are not easily done by hand, so we choose the third method. The constant coefficient of $g_1(x)$ is $(-1)^5\beta\beta^3\beta^4\beta^5\beta^9=-\beta^{22}=-1=2$. In the same way, we find that the constant coefficient of $g_2(x)$ is 2. Since $g_2(x)$ is the reciprocal polynomial of $g_1(x)$, the coefficients of $g_2(x)$ are the reverse of the coefficients of $g_1(x)$ scaled by the factor $2^1=2$. That is, if

$$g_1(x)=2+a_1x+a_2x^2+a_3x^3+a_4x^4+x^5,$$

then

$$g_2(x)=2+2a_4x+2a_3x^2+2a_2x^3+2a_1x^4+x^5.$$

Now we use the fact that all coefficients of the product $g_1(x)g_2(x)$ are 1.

The coefficients of x,x^2,x^3,x^4 are

$$\begin{aligned}
&2\cdot 2a_4+2a_1=1\Rightarrow a_4+2a_1=1\\
&\Rightarrow a_4=1+a_1\\
&2\cdot 2a_3+2a_1a_4+2a_2=1\Rightarrow a_3+2a_1a_4+2a_2=1\\
&\Rightarrow a_3=1+a_1a_4+a_2\\
&2\cdot 2a_2+2a_1a_3+2a_2a_4=1\\
&\Rightarrow a_2=1+a_1a_3+a_2a_4+a_3\\
&2\cdot 2a_1+2a_1a_2+2a_2a_3+2a_3a_4+2a_4=1\\
&\Rightarrow g_1=1+a_1a_2+a_2a_3+a_3a_4+a_4
\end{aligned}$$

By the first two of the above equations, a_3 and a_4 are determined by a_1 and a_2. Let us denote by $a_2'=1+a_1a_3+a_2a_4+a_3$. The following table lists the possible

combinations of values.

a_1	a_2	a_3	a_4	a_2'
0	0	1	1	2
0	1	2	1	1
0	2	0	1	0
1	0	0	2	0
1	1	1	2	2
1	2	2	2	0
2	0	1	0	1
2	1	2	0	1
2	2	0	0	1

The second and eighth rows in the above table have consistent values for a_2 and a_2'. (The fourth row corresponds to a generator polynomial of weight 4, which cannot be a codeword.) The corresponding generator polynomials are,

$$x^5 + x^4 + 2x^3 + x^2 + 1$$
$$x^5 + 2x^3 + x^2 + x + 2$$

22. (BCH codes of blocklength 31). The design minimum distance of a t-error-correcting binary BCH code is $2t + 1$, where t is the number of factors in the generator polynomial

$$g(x) = lcm(m_1(x), m_3(x), \ldots, m_{2t-1}(x)).$$

The factors $m_i(x)$ of $g(x)$ are minimal polynomials over GF(2) of α^i , where α is primitive.

(a) List the conjugacy classes of the powers of α, represented by exponents. For example, the conjugacy class of $1 = \alpha^0$ is $\{0\}$ and the conjugacy class of α is $\{1, 2, 4, 8, 16\}$.

The conjugacy class of $1 = \alpha^0$ is represented by $\{0\}$. The exponents of the elements of conjugacy classes of the positive powers of α are listed below:

$$\{1, 2, 4, 8, 16\} \quad \{7, 14, 28, 25, 19\}$$
$$\{3, 6, 12, 24, 17\} \quad \{11, 22, 13, 26, 21\}$$
$$\{5, 10, 20, 9, 18\} \quad \{15, 30, 29, 27, 23\}$$

All conjugacy classes have five elements because GF(32) has no nontrivial subeld. All ele- ments of GF(32)-GF(2) are primitive because the multiplicative group has order 31, which is prime. In general, if p is prime then GF(2^p) has no subfield except GF(2). However, not every element of GF(2^p) - GF(2) need to be primitive; e.g., GF(2^{11}) has elements of orders 23 and 89.

(b) Find the number of check bits used by the narrow-sense binary primitive BCH codes of blocklength 31 and design minimum distance $2t + 1$ for $t = 1, \ldots, 8$.

Using the conjugacy classes found in part (a), we list the exponents of the zeroes of the factors of the generator polynomials of narrow-sense t-error-

correcting codes for $t = 1, \ldots, 8$.

t	Conjugacy class	$n-k$
1	$\{1, 2, 4, 8, 16\}$	5
2	$\{3, 6, 12, 24, 17\}$	10
3	$\{5, 10, 20, 9, 18\}$	15
4	$\{7, 14, 28, 25, 19\}$	20
5	–	20
6	$\{11, 22, 13, 26, 21\}$	25
7	–	25
8	$\{15, 30, 29, 27, 23\}$	30

Rows 5 and 7 are empty because the corresponding conjugacy classes were listed in rows 3 and 4. For $t = 1, \ldots, 4$, the BCH bound guarantees that $5t$ check bits are sufficient to correct t errors. But for $t = 5$, no additional check bits are needed because the α^9 and α^{10} are conjugates of α^5. Similarly, α^{13} is a conjugate of α^{11} , so the narrow-sense BCH code for $t = 6$ is guaranteed to correct 7 errors.

(c) The generator polynomials of these BCH codes have zeroes other than $\alpha, \ldots, \alpha^{2t}$. List the minimum distances guaranteed by the BCH bound for these six codes.

The BCH bound says that the minimum distance of a BCH code is at least one more than the number of consecutive powers of α that are zeroes of the generator polynomial $g(x) = lcm(f_1(x), \ldots, f_{2t-1}(x))$. The following table lists the conjugacy classes of odd powers of α, from which we can determine the number of consecutive powers of α that are zeroes of $g(x)$.

t	Conjugacy class	Consecutive powers	Min. dist.
1	$\{1, 2, 4, 8, 16\}$	2	3
2	$\{3, 6, 12, 24, 17\}$	4	5
3	$\{5, 10, 20, 9, 18\}$	6	7
4	$\{7, 14, 28, 25, 19\}$	10	11
5	–	10	11
6	$\{11, 22, 13, 26, 21\}$	14	15
7	–	14	15
8	$\{15, 30, 29, 27, 23\}$	30	31

The Hamming bound can be used to show that the error correcting ability is t for $t = 1, 2, 3$. It can also be shown that the codes with $t = 6$ and $t = 8$ have minimum distances equal to the BCH bound.

23. (BHC decoding): Let $GF(2^4) = GF(2)[x]/(p(x))$, where p(x) is the primitive polynomial $p(x) = x^4 + x + 1$, and let α be the primitive root $\alpha = x \pmod{p(x)}$. We let $g(x)$ be the monic polynomial of smallest degree having the following zeroes:

$$\alpha, \alpha^2, \alpha^3 \alpha^4$$

and let $n = 15$ be the length of the code. Hence, since $g(x)$ has four consecutive roots, the corresponding cyclic code C is a BCH code with design distance $\delta = 4 + 1 = 5$.

Hence, the minimum distance $d \geq 5 = 2t + 1$. This implies that the the BCH code C is capable of correcting $t = 2$ errors. Since $\alpha, \alpha^2, \alpha^4$ are all conjugate to each other (have the same minimum polynomial), and since α and α^3 are not conjugates, $g(x)$ is simply the polynomial of smallest degree having α and α^3 as roots.

Thus, the parity matrix is given by (check the lecture notes),

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{13} & \alpha^{14} \\ 1 & (\alpha^3)^1 & (\alpha^3)^2 & \cdots & (\alpha^3)^{13} & (\alpha^3)^{14} \end{pmatrix}$$

which simplifies to (using $\alpha^{15} = 1$),

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{13} & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & \cdots & \alpha^9 & \alpha^{12} \end{pmatrix}$$

Let us assume that a code vector $\mathbf{c}$ is sent over a BSC, and that the received vector is $\mathbf{r} = \mathbf{c} + \mathbf{e}$, where $\mathbf{e}$ denotes the error vector. Let us further assume that exactly two errors have occured, i.e.,

$$\mathbf{e} = \mathbf{e}_i + \mathbf{e}_j$$

where $\mathbf{e}_i$ and $\mathbf{e}_j$ are nonzero at positions i and j respectively. Remark that nonzero means $\mathbf{r}_i = \mathbf{r}_j = 1$ as our code is binary, but the decoder alphabet is GF(16) !!!

Now we compute the syndrome of $\mathbf{r}$ as usual,

$$S = H\mathbf{r}^T = (\alpha^i + \alpha^j, (\alpha^i)^3 + (\alpha^j)^3) = (s_0, s_1).$$

We will call the field elements α^i and α^j error locators, since their logs are the locations of the two respective errors. Knowing the error locators is equivalent to knowing the error locations.

We construct the **error location polynomial** $S(x)$ from the components s_0 and s_1 of the syndrome. The error location polynomial $S(x)$ is the polynomial over GF(16) whose roots are the error locator. In other words,

$$S(x) = (x + \alpha^i)(x + \alpha^j) = x^2 + (\alpha^i + \alpha^j)x + \alpha^{i+j}.$$

Then since, $\alpha^i + \alpha^j = s_0$ and $(\alpha^i)^3 + (\alpha^j)^3 = s_1$ we have,

$$s_1 = (\alpha^i + \alpha^j)[(\alpha^i)^2 + \alpha^{i+j} + (\alpha^j)^2] = s_0(s_0^2 + \alpha^{i+j}).$$

Then

$$\alpha^{i+j} = \frac{s_1}{s_0} + s_0^2$$

Furthermore we have,

$$S(x) = x^2 + (\alpha^i + \alpha^j)x + \alpha^{i+j} = x^2 + s_0 x + \frac{s_1}{s_0} + s_0^2$$

and we need to find the roots of this polynomial to get α^i and α^j ! Note that s_0, s_1 are known as it is a syndrome of the received vector. Given the syndrome $S = (s_0, s_1)$ of the received vector $\mathbf{r}$ our error correcting scheme is as follows:

- If $s_0 = s_1 = 0$, then we decide that no error has occurred.
- If $s_0 \neq 0$ and $s_1 = s_0^3$, then we decide that a single error has occurred at the error locator $z = \alpha^i$.
- If $s_0 \neq 0$ and $s_1 \neq s_0^3$, then we decide that two errors have occurred, and we find the two error locators α^i and α^j by finding the two roots of the error locator polynomial $S(x)$.

24. Block code over GF(16). The parity-check matrix of a (15,13) linear block code over GF(16) is,

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & \dots & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \dots & \alpha^{14} \end{bmatrix}$$

where α is a primitive element of GF(16) satisfying $\alpha^4 + \alpha + 1 = 0$.

(a) Calculate the syndrome of r = (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1).

The components of the syndrome (s_0, s_1) are the inner products of r with the rows of H. The first component is $s_0 = 1 + 1 + \ldots + 1 = 1$, since the sum of an odd number of ones in a field of characteristic 2 is 1.
The second component is $1 + \alpha + \alpha^2 + \alpha^3 + \ldots + \alpha^{14}$. . Since α is a zero of

$$x^{15} - 1 = (x - 1)(1 + x + x^2 + + \ldots + x^{14})$$

but not a zero of $x - 1$, it is a zero of the second factor, which evaluated at α is the second syndrome component. Therefore $s_1 = 0$.

(b) Suppose that the syndrome of a received 15-tuple is $s = (\alpha^8, \alpha^4)$. Assuming that there is a single symbol error, find the error location and error pattern.

If the error is $e = e_i x^i$, that is, a nonzero error pattern e_i in location i, then

$$\begin{aligned} s_0 &= \sum_{j=0}^{14} r_j = \sum_{j=0}^{14} (c_j + e_j) = \sum_{j=0}^{14} c_j + \sum_{j=0}^{14} e_j = 0 + e_i = e_i \ \ (Hc^T = 0) \\ s_1 &= \sum_{j=0}^{14} r_j \alpha^j = \sum_{j=0}^{14} (c_j + e_j)\alpha^j = \sum_{j=0}^{14} c_j \alpha^j + \sum_{j=0}^{14} e_j \alpha^j = 0 + e_i \alpha^i = e_i \alpha^i \end{aligned}$$

The error location is found from,

$$\frac{s_1}{s_0} = \frac{\alpha^4}{\alpha^8} = \alpha^{-4} = \alpha^{11}.$$

The error pattern is simply s_0, i.e. the error is α^8.

(c) If only single symbol errors are corrected, which syndromes result in decoder failure ?

Single errors always result in syndromes in which both components are nonzero. The decoding procedure used in part (b) fails if exactly one syndrome component is 0. There are 30 uncorrectable syndromes, namely $(s_0, 0)$ and $(0, s_1)$ where $s_0 \neq 0$ and $s_1 \neq 0$.

25. (Fire codes): Fire codes are cyclic codes that are designed for efficient correction of burst errors and efficient encoding/decoding. The generator polynomial is of the form,

$$g(x) = (x^{2t-1} + 1)p(x)$$

where $p(x)$ is a primitive polynomial over $GF(2)$ (for binary case), thus if degree of p is m then the order of p is $2^m - 1$. To be a cyclic code we know that $g(x)$ must divide $x^n - 1$ and therefore the block length is then the least common multiples of the orders of $p(x)$ and $x^{2t-1} + 1$. One can show that the Fire code can correct the bursts of length $\leq m$. The burst error efficiency is defined as ,

$$\frac{2t}{2t - 1 + m}$$

and its maximum is for $t = m$ which is approximately 2/3.

(a) What are the blocklength n, dimension k, and burst correction performance of the binary Fire code with generator polynomial $g(x) = (x^{15} + 1)(x^8 + x^4 + x^3 + x^2 + 1)$?

(b) Construct the generator polynomial for a cyclic Fire code of blocklength $n = 1143$ over GF(256) that will correct all burst errors of length 5 or less. Use the fact that $x^8 + x^4 + x^3 + x^2 + 1$ is a primitive polynomial over GF(2).

(a) To analyze the binary Fire code with generator polynomial

$$g(x) = (x^{15} + 1)(x^8 + x^4 + x^3 + x^2 + 1)$$

we first consider the factor $x^8+x^4+x^3+x^2+1$. This is a primitive polynomial of degree 8 so it has order $2^8 - 1 = 255$. The order of the factor $x^{15} + 1$ is obviously 15. Therefore the order of $g(x)$ the least common multiple of its factors and is therefore $n = 255$.

The number of check symbols is $n - k = \deg g(x) = 15 + 8 = 23$. Thus the dimension of the code is $k = n - (n - k) = 255 - 23 = 232$, and its rate is $232/255 = 0.910$. By properties of Fire codes, the burst correction performance of this code with $t = 8$ and $m = 8$ is at least 8. It can be shown that it is exactly 8. This is because the generator polynomial,

$$g(x) = x^8 + x^4 + x^3 + x^2 + 1 + x^{15}(x^8 + x^4 + x^3 + x^2 + 1)$$

is a codeword that is a sum of two bursts of length 9 (one starts at position 0 and the other at position 15) , which shows that not all bursts (combinations of bursts) of length 9 can be corrected. These two bursts transform the zero codeword into the codeword $c(x) = g(x)$.

(b) By definition, the generator polynomial of a cyclic Fire code of blocklength $n = 1143$ over GF(256) that can correct all burst errors of length 5 or less is

$$g(x) = (x^{2\cdot 5-1} - 1)p(x) = (x^9 - 1)p(x),$$

where $p(x)$ is prime of degree ≥ 5 (condition for correcting bursts of length up to 5). The blocklength $n = 1143 = 9 \cdot 127$ is the order of $g(x)$, which is the least common multiple of the orders of the factors of $g(x)$. The order of

any prime polynomial over GF(256) of degree 5 is a divisor of $256^5 - 1$. Since 127 is not a divisor of $256^5 - 1$, there is no degree 5 prime polynomial over GF(256) of order 127. Similarly, since 127 is not a divisor of $256^6 - 1$, there is no degree 6 prime polynomial over GF(256) of order 127!

Therefore we must use a polynomial of degree 7, and the simplest choice is a primitive polynomial over GF(2) of degree 7. We choose $p(x) = x^7 + x^3 + 1$. The corresponding generator polynomial is,

$$g(x) = (x^9 + 1)(x^7 + x^3 + 1) = 1 + x^3 + x^7 + x^9 + x^{12} + x^{16}.$$

The burst error correction efficiency of this code is $2t/(n-k) = 10/16 = 5/8$.

26. (Erasure correction): Consider the (7,4) binary Hamming code with parity-check matrix,

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

a) Find a codeword of weight 3.

Need to find three columns of H that adds to zero (recall $Hc^T = 0$). One such codeword is $\mathbf{c}$=(1000110).

b) Decode $\mathbf{r}_1 = (100?01?)$ a codeword with two erasures.

Let x and y be the unknown bits in the transmitted codeword $\mathbf{c}_1$. Then $H\mathbf{c}_1^T = 0$ yields three linear equations for the two unknowns x and y:

$$\begin{aligned} 0 &= 1 + x + 1 + y = x + y \\ 0 &= x + 1 \\ 0 &= 1 + y \end{aligned}$$

From the last two equations, we see that $x = 1$ and $y = 1$, which is conrmed by the first equation. Thus $\mathbf{c}_1 = (1001011)$.

c) Decode $\mathbf{r}_2 = (100???)$ a codeword with 3 erasures.

Let x, y, z be the unknown bits in the transmitted codeword $\mathbf{c}_2$. Then $H\mathbf{c}_1^T = 0$ yields:

$$\begin{aligned} 0 &= 1 + x + z \\ 0 &= x + y + z \\ 0 &= y + z \end{aligned}$$

Adding the last two equations yields $x = 0$. Substituting $x = 0$ into the first equation yields $z = 1$. The third equation implies $y = z = 1$. Thus $\mathbf{c}_2 = (1000110)$.

d) Explain why part (c) does not contradict the fact that a code with minimum distance 3 has erasure correction ability 2.

The erasure correction ability $d - 1 = 2$ is the maximum number of erasures that are guaranteed to be correctable because any two columns of H are linearly independent. Some sets of three columns are linearly independent, such as columns 4, 5, and 6, and so erasures in those bit positions can be corrected. Other sets of three columns are linearly dependent, such as columns 1, 2, and 4, and so erasures in those bit positions cannot be corrected.

27. (Reed-Solomon code over GF(11)) Let C be the (10,7) narrow-sense Reed-Solomon code over GF(11) based on the primitive element $\alpha = 6$.

i	0	1	2	3	4	5	6	7	8	9
6^i	1	6	3	7	9	10	5	8	4	2

(a) Find the generator polynomial of C.

The generator polynomial can be calculated by multiplying its factors over GF(11).

$$\begin{aligned} g(x) &= (x-6)(x-6^2)(x-6^3) = (x-6)(x-3)(x-7) \\ &= (x+5)(x+8)(x+4) = (x^2+2x+7)(x+4) = x^3+6x^2+4x+6. \end{aligned}$$

(b) Find the syndrome of $r(x) = x^5$.

First note that the parity check matrix is 3×10 and consequently there are three syndromes computed as $s = Hr$. The polynomial syndrome is $s(x) = x^5 \pmod{g(x)} = 2x^2 + 7x + 6$. Home exercise to check this !

28. (Reed-Solomon code over GF(16)). A (15,11) double error correcting Reed-Solomon code over GF(16) has the following generator polynomial:

$$g(x) = (x+\alpha)(x+\alpha^2)(x+\alpha^3)(x+\alpha^4) = x^4 + \alpha^{13}x^3 + \alpha^6 x^2 + \alpha^3 + \alpha^{10}.$$

(a) A received vector has partial syndromes $S_1 = \alpha^1, S_2 = \alpha^{13}, S_3 = {}^1, S_4 = \alpha^{11}$. Find the error-locator polynomial $\Lambda(x)$.

Since $S_1 \neq 0$, there is at least one error. To determine whether there are two or more errors, we consider the coefficient matrix M_2 in the following system of linear equations.

$$M_2 = \begin{bmatrix} S_1 & S_2 \\ S_2 & S_3 \end{bmatrix} \begin{bmatrix} \Lambda_1 \\ \Lambda_2 \end{bmatrix} = \begin{bmatrix} \alpha^2 \\ \alpha^{11} \end{bmatrix}$$

Thus,

$$\Lambda(x) = 1 + \alpha^{11}x + \alpha^2 x^2.$$

For small $t = 2$ there is no need to use Extended Euclidean algorithm for the same purpose.

(b) Assume that a received vector has error-locator polynomial $\Lambda(x) = 1 + \alpha^9 x + \alpha^{11}x^2$. Find the error locators X_1, X_2.

To find the zeros of the we solve the quadratic equation by using a change of variables. Let $u = \alpha^2 x$. Then

$$\Lambda(x) = 1 + \alpha^7 u + \alpha^7 u^2 = \alpha^7(\alpha^8 + u + u^2) = f(u)$$

Clearly, the zeros of this polynomial $f(u)$ occur when $u + u^2 = \alpha^8$.
To calculate this one can construct the field table (based on the primitive polynomial $x^4 + x + 1$ and compute $u + u^2$ for $u = 0, 1, \alpha, \alpha^2, \ldots, \alpha^{14}$ and compare for which α^i we have

$$\alpha^i + \alpha^{2i} = \alpha^8$$

The zeros are found to be α^{11} and α^{12}. E.g. consider α^{11}. Then,

$$\alpha^{11} + \alpha^{22} = \alpha^{11} + \alpha^7 = \alpha^7 \underbrace{(1 + \alpha^4)}_{=\alpha} = \alpha^8.$$

Now to get the zeros of $\Lambda(x)$ we substitute back and get $\alpha^{-2}u_1 = \alpha^{10}$ and $\alpha^{-2}u_2 = \alpha^9$. Finally, the error locators are zeros of the reciprocal polynomial, therefore $X_1 = \alpha^{-10}$ and $X_2 = \alpha^{-9}$.

29. (MDS codes : Let C be a code over the field $GF(4) = \{0, 1, \alpha, \alpha^2\}$ g (where α is a root of the irreducible polynomial $1 + x + x^2 \in \mathbb{F}_2[x]$, i.e. $\alpha^2 = \alpha + 1$) with the generator matrix,

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

Show that C is an MDS code.

An MDS code is a linear (n, k, d) code for which $d = n - k + 1$ (the min. distance meets the Singelton bound). In our case, $n = 4$, $k = 2$ so we must have $d = 3$. It is enough to show that any $k = 2$ columns of G are linearly independent. This is obviously true by inspecting the generator matrix as

$$\beta G_i + \gamma G_j \neq (0, 0)^T$$

for any $i \neq j$ and $\beta, \gamma \in GF(4)$. Here G_i denotes a the i-th column of G.

On contrary, if $k = 2$ columns of G are linearly dependent then there exists coefficients $\beta_1, \beta_2 \in GF(4)$ such that $\mathbf{c_1} = \beta_1 g_1$ and $\beta_2 g_2$ (g_i is the i-th row of G) agrees at k positions implying that $d = n - k$, a contradiction.

30. (Convolutional code): A simple convolutional code with rate 1/2 has encoding equations,

$$c_i^1 = m_i, \;\; c_i^2 = m_i \oplus m_{i-1},$$

where m_i is an information bit and c_i^i , c_i^2 are the corresponding codeword bits. For example, $m_1 m_2 m_3 = 101$ is encoded to $c_1^1 c_1^2 c_2^1 c_2^2 c_3^1 c_3^2 = 1\ 1\ 0\ 1\ 1\ 1$. This code can correct single bit errors that are sufficiently far apart. a) Each information bit mi aects three codeword bits. Use these three equations to obtain a majority-logic decoder for this convolutional code.

Solution : The encoding equations provide two equations that include the information bit m_i:

$$c_i^1 = m_i,$$
$$c_i^2 = m_i \oplus m_{i-1}.$$

A third equation arises from the effect of m_i on the next codeword block:

$$c_{i+1}^2 = m_{i+1} + m_i$$

Using $c_{i-1}^i = m_{i-1}$ and $c_{i+1} = m_{i+1}$ we can rewrite these three equations as follows:

$$\begin{aligned} m_i &= c_i^1 \\ m_i &= c_{i-1}^1 \oplus c_i^2 \\ m_i &= c_{i+1}^1 \oplus c_{i+1}^2 \end{aligned}$$

Each equation provides one vote for the value of m_i, leading to the decoding equation,

$$\hat{m}_i = \text{majority}(c_i^1, c_{i-1}^1 \oplus c_i^2, c_{i+1}^1 \oplus c_{i+1}^2).$$

b) Find the minimum separation between errors that guarantees that errors can be corrected by the decoder of part (a). (Encoded bits are transmitted in the order c_i^1, c_i^2)

Solution : If the information bit c_i^1 is incorrect, but the nearby received bits are correct, the last two equations will outvote the incorrect first equation. Similarly, any single error in the 6 consecutive bits

$$\ldots c_{i-1}^1, c_{i-1}^2, c_i^1, c_i^2, c_{i+1}^1, c_{i+1}^2 \ldots$$

will be corrected because each bit appears in at most one of the three equations. Thus errors that are 6 or more bit positions apart can always be corrected, because the decoding window of 6 bits will include at most one wrong bit. On the other hand, errors in c_{i-1}^1 and c_{i+1}^2 will result in miscorrecting m_i. The distance between these two incorrect bits is 5. Therefore 6 is the minimum distance between bit errors that guarantees that the errors will be corrected using the decoder of part (a).

c) Describe a decoding method that is more powerful than the method of part (a)

Solution : The decoder can be improved by using the previously decoded estimate $\hat{m}_{i-1}$ instead of c_{i-1}^i in the second equation:

$$\hat{m}_i = \text{majority}(c_i^1, \hat{m}_{i-1} \oplus c_i^2, c_{i+1}^1 \oplus c_{i+1}^2).$$

This majority logic decoder with feedback operates successfully as long as there is at most one error in any two consecutive 2-bit received blocks, which is guaranteed by a distance of at least 4 between bit errors.

31. This question considers cyclic codes.

(a) Define the term cyclic code.

In words any cyclic shift of a codeword in the code must be in the code as well.

(b) Determine whether the following codes are cyclic. Briefly explain your answers.

(i) The binary code $C = \{0000, 1010, 0101, 1110, 1101, 1011, 0111\}$.

Not cyclic since not linear (e.g. $1010 + 0101 = 1111$ is not in the code).

(ii) The ternary code $C = \{000, 011, 101, 110\}$.

Not cyclic since not linear (e.g. $2 \times 011 = 022$ is not in the code).

(iii) The 7-ary code

$$C = \{\mathbf{x} \in \mathbb{Z}_7^5 \mid \sum_{i=1}^{5} ix_i \equiv 0 \bmod 7\}.$$

Not cyclic since not closed under cyclic shift (e.g. 02100 is in the code but 21000 is not).

(iv) $E_n \subset \mathbb{Z}_2^n$, the set of even weight binary words of length n.

E_n is linear, and cyclic shift leaves the weight of a vector unchanged, so it's closed under cyclic shift. Hence E_n is cyclic.

(v) $O_n \subset \mathbb{Z}_2^n$, the set of odd weight binary words of length n. O_n is not cyclic since it isn't linear (e.g. it doesn't contain the zero vector).

(c) (i) Factorize $p(x) = x^5 - 1$ over $\mathbb{Z}_{31}$ into irreducible factors. (Hint: what is $p(2^n)$?)

Note that $p(2^n) = 2^{5n} - 1 = 32^n - 1 = 1^n - 1 = 0$ for all n. Hence $p(1) = p(2) = p(4) = p(8) = p(16) = 0$ and we deduce that there are 5 associated linear factors. But since $degp(x) = 5$, this completely determines the factorization:

$$x^5 - 1 = (x-1)(x-2)(x-4)(x-8)(x-16)$$

over $\mathbb{Z}_{31}$.

(ii) For each $k = \{0, 1, 2, \ldots, 5\}$ let N_k denote the number of distinct 31-ary cyclic codes of length 5 and dimension k. Determine these numbers as $N_0, N_1, \ldots, N_5$.

It follows that there are $2^5 = 32$ distinct cyclic codes of length 5 over $\mathbb{Z}_{31}$, determined by the generator polynomials

$$g(x) = (x-1)^{m_1}(x-2)^{m_2}(x-4)^{m_3}(x-8)^{m_4}(x-16)^{m_5}.$$

where each $m_i \in \{0, 1\}$. The code $< g(x) >$ has dimension $k = 5 - m_1 - m_2 - \ldots - m_5$, so the number of codes of dimension k is the number of ways of choosing $5 - k$ nonzero exponents out of 5. Hence,

$$N_k = \binom{5}{5-k} = \binom{5}{k}.$$

(iii) Choose the cyclic code of dimension 3 with minimal root values, C say. Write down the generator polynomial $g(x)$, the check polynomial $h(x)$, a generator matrix G and a parity check matrix H for C. Determine $d(C)$.

There are $N_3 = 10$ different dimension 3 codes, but we choose one with minimal root values,

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

This has check polynomial

$$h(x) = (x-4)(x-8)(x-16) = 16 + 6x - 28x^2 + x^3 = 15 + 6x + 3x^2 + x^3.$$

The generator matrix is,

$$G = \begin{pmatrix} 2 & -3 & 1 & 0 & 0 \\ 0 & 2 & -3 & 1 & 0 \\ 0 & 0 & 2 & -3 & 1 \end{pmatrix}$$

and the parity check matrix

$$H = \begin{pmatrix} 1 & 3 & 6 & 15 & 0 \\ 0 & 1 & 3 & 6 & 15 \end{pmatrix}$$

Since no pair of columns of H is lin. dependent, and every triple of columns is linearly dependent, we deduce that $d = 3$.

32. A ternary channel transmits one of three symbols at each symbol time: sinusoidal pulses at phase angles $0°, 120°$, or $240°$. Represent the channel symbols with $\{0, 1, 2\}$.

(a) Design a triple-error-correcting BCH code of blocklength 80 for this channel. You are not supposed to construct the extension field, only need to identify a suitable element used in the construction. Also, you need to specify minimal polynomials that are factors of the generator polynomial, without computing either these polynomials or $g(x)$ explicitly.

We are given that $x^4 + x + 2$ is primitive over GF(3). Every BCH code over GF(3) of blocklength 80 is defined by an element of $GF(3^m)$ of order 80. The smallest field of characteristic 3 that contains an element of order 80 is $GF(3^4) = GF(81)$. Since we can use any primitive element, we can choose a zero of the primitive polynomial $x^4 + x + 2$.
A narrow-sense ternary primitive 3EC BCH code has codewords whose common zeroes are the first 6 powers of α, for $p(\alpha) = 0$. Since α^3 is a conjugate of α and α^6 is a conjugate of α^2 over GF(3), these 6 powers belong to only 4 distinct conjugacy classes:

$$\{\alpha, \alpha^3, \alpha^9, \alpha^{27}\}, \{\alpha^2, \alpha^6, \alpha^{18}, \alpha^{54}\}, \{\alpha^4, \alpha^{12}, \alpha^{36}, \alpha^{28}\}, \{\alpha^5, \alpha^{15}, \alpha^{45}, \alpha^{55}\}.$$

The check matrix has 16 linearly independent rows over GF(3), and the generator polynomial has degree 16. The generator polynomial is the product of the distinct minimal polynomials over GF(3) of $\alpha, \alpha^2, \ldots, \alpha^6$:

$$g(x) = f_1(x) f_2(x) f_4(x) f_5(x).$$

It remains to find the minimal polynomials. Computing in GF(81) we have:

$$f_1(x) = (x-\alpha)(x-\alpha^3)(x-\alpha^9)(x-\alpha^{27}) = x^4 + x + 2.$$

In the similar manner,

$$\begin{aligned} f_2(x) &= (x-\alpha^2)(x-\alpha^6)(x-\alpha^{18})(x-\alpha^{54}) = x^4+x^2+2x+1 \\ f_4(x) &= (x-\alpha^4)(x-\alpha^{12})(x-\alpha^{36})(x-\alpha^{28}) = x^4+2x^3+x+1 \\ f_5(x) &= (x-\alpha^5)(x-\alpha^{15})(x-\alpha^{45})(x-\alpha^{55}) = x^4+x^2+2 \end{aligned}$$

Note that an explicit computation of the minimal polynomials was not required.

(b) What is the rate of the code ?

Since the generator polynomial has 4 prime factors of degree 4, its degree is 16. Therefore $k = n(nk) = 8016 = 64$. The rate of the code is $64/80 = 4/5$.

(c) How might this code be used to transmit binary data ?

Blocks of binary data can be encoded into blocks of ternary data. For example, 3 binary bits can be represented by 8 of the 9 possible combinations of ternary 2-tuple. Other transformation schemes are of course possible.