Solutions for Homeworks

Exercise 1.

Consider a communication channel, which takes as input a vector of length $n = 5$, and erases exactly one out of the 5 coefficients, but we do not know which one. Design two linear codes over $\mathbb{F}_3$ that make sure any message of length $k = 4$ can always be received perfectly at the receiver.

Solution 1. Since $k = 4$ and $n = 5$, we will add one coefficient, a linear combination of the 4 data symbols x_1, x_2, x_3, x_4. Since we are over $\mathbb{F}_3$, non-zero elements are 1 and 2, so we could choose $a_1x_1 + a_2x_2 + a_3x_4 + a_4x_4$, with a_i being 1 or 2. It is important that all 4 data symbols are present, because if the erasure affects any of the x_i, a copy must be contained in the 5th coefficient.

Exercise 2.

Consider G to be the generator matrix of a linear code over $\mathbb{F}_5$:

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

Write G in systematic form.

Solution 2. Basis vectors are rows of G. We are allowed to do a change of basis, that is do linear operations on the rows of G. We start by obtaining zeroes in the first column (this is the first step of Gaussian elimination), and then multiply the second row by 2 to have a 1 on the diagonal:

$$G \to \begin{bmatrix} 1 & 2 & 4 & 0 & 1 \\ 0 & -2 & -3 & 2 & 0 \\ 0 & -2 & -4 & 3 & 0 \end{bmatrix} \to \begin{bmatrix} 1 & 2 & 4 & 0 & 1 \\ 0 & 1 & -1 & 4 & 0 \\ 0 & -2 & -4 & 3 & 0 \end{bmatrix}$$

Then use the second row to have zeroes on the first and third rows, and multiply the last row by -1 to have a 1 on the diagonal:

$$G \to \begin{bmatrix} 1 & 0 & 1 & -3 & 1 \\ 0 & 1 & -1 & 4 & 0 \\ 0 & 0 & -1 & 1 & 0 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 1 & -3 & 1 \\ 0 & 1 & -1 & 4 & 0 \\ 0 & 0 & 1 & -1 & 0 \end{bmatrix}.$$

Finally the last row is used to obtain the systematic form:

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

Exercise 3.

Consider G to be the generator matrix of a linear code $\mathcal{C}$ over $\mathbb{F}_q$:

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

1. For $q = 2$, give the cardinality of $\mathcal{C}$ and list all codewords.
2. For $q = 4$, give the cardinality of $\mathcal{C}$ and list all codewords.

Solution 3.

1. For $q = 2$, $|\mathcal{C}| = 2^2$ and the codewords are $(0,0,0)$, $(1,0,1)$, $(0,1,1)$, $(1,1,0)$.
2. For $q = 4$, $|\mathcal{C}| = 4^2$ and for ω such that $\omega^2 = \omega + 1$, the codewords are $(0,0,0)$, $(0,1,1)$, $(0,\omega,\omega)$, $(0,\omega^2,\omega^2)$, $(1,0,1)$, $(1,1,0)$, $(1,\omega,\omega^2)$, $(1,\omega^2,\omega)$, $(\omega,0,\omega)$, $(\omega,1,\omega^2)$, $(\omega,\omega,0)$, $(\omega,\omega^2,1)$, $(\omega^2,0,\omega^2)$, $(\omega^2,1,\omega)$, $(\omega^2,\omega,1)$, $(\omega^2,\omega^2,0)$.

Exercise 4.

Compute a parity check matrix in systematic form for the code given by the following generator matrix:

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

Solution 4. Since the field is not specified, the parity check matrix is:

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

Exercise 5.

Consider the linear $(8,4)$ code over $\mathbb{F}_2$ given by the generator matrix:

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

Decide whether this code is self-orthogonal and/or self-dual. Does your answer change if you replace $\mathbb{F}_2$ by $\mathbb{F}_p$ for p an odd prime?

Solution 5. The parity check matrix of this code is

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

Flip row 1 and row 2 and then add (the new) row 1 to row 3 and 4:

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

Then add row 2 to rows 3 and 4, and permute the newly obtained rows 3 and 4:

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

and we already see that the last 2 rows are the same as that of G. We add row 3 to row 1 and row 2, and then we add row 4 to the newly obtained row 1 and row 2:

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

This shows that the code is self-dual and thus self-orthogonal in particular.

Note that this works over $\mathbb{F}_2$, but not necessarily otherwise. For example, take the codeword $(1, 0, 0, 0, 0, 1, 1, 1)$. Then the inner product of this codeword with itself is 4. This is also 0 modulo 2, but this is not 0 modulo another prime. This shows that the code is not included into its dual, and in thus not self-dual over $\mathbb{F}_p$ for p an odd prime.

Exercise 6.

Show that if a code is self-dual, then its length n must be even, and its dimension must be $n/2$.

Solution 6. A linear (n, k) code $\mathcal{C}$ has dimension k, its dual $C^\perp$ has dimension $n - k$. If we want $\mathcal{C} = \mathcal{C}^\perp$, we need $n - k = k$, that is $n = 2k$ and therefore n is even. That $n = 2k$ also tells us that $k = n/2$.

Exercise 7. (*)

1. Consider the code $\mathcal{C}_1$ over $\mathbb{F}_3$ given by the following parity check matrix:

$$H_1 = \begin{bmatrix} 2 & 2 & 1 & 0 \\ 0 & 1 & 1 & 2 \end{bmatrix}.$$

   Is the code self-orthogonal? self-dual? Justify your answer.

2. Consider the code $\mathcal{C}_2$ given by the following generator matrix over $\mathbb{F}_4$:

$$G_2 = \begin{bmatrix} 1 & 0 & 0 & 1 & w & w \\ 0 & 1 & 0 & w & 1 & w \\ 0 & 0 & 1 & w & w & 1 \end{bmatrix}.$$

   Is this code self-orthogonal? self-dual? Justify your answer.

Solution 7. 1. Since we have a parity check matrix, we first put it into a familiar form, namely add minus row 1 to row 2 and then multiply row 2 by 2 to get

$$H_1 \to \begin{bmatrix} 2 & 2 & 1 & 0 \\ -2 & -1 & 0 & 2 \end{bmatrix} \to \begin{bmatrix} 2 & 2 & 1 & 0 \\ -1 & 1 & 0 & 1 \end{bmatrix}.$$

Then a generator matrix is

$$G_1 = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & -1 \end{bmatrix}.$$

From H_1, we can put it in systematic form by adding row 2 to row 1 and then multiply row 1 by 2:

$$H_1 \to \begin{bmatrix} 2 & 0 & 2 & 2 \\ 0 & 1 & 1 & 2 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{bmatrix}.$$

So the code is self-dual and so in particular it is self-orthogonal (it is the tetracode).

2. Consider the code $\mathcal{C}_2$ given by the following generator matrix over $\mathbb{F}_4$:

$$G_2 = \begin{bmatrix} 1 & 0 & 0 & 1 & w & w \\ 0 & 1 & 0 & w & 1 & w \\ 0 & 0 & 1 & w & w & 1 \end{bmatrix}.$$

This code cannot be self-orthogonal since the inner product of row 1 and row 2 is w^2 which is not 0. Thus the code is not self-dual either.

Exercise 8.

For both

1. the $(n, n-1)$ single parity check code,
2. and the $(4, 2)$ tetracode over $\mathbb{F}_3$,

compute their minimum Hamming distance based on their parity check matrix.

Solution 8. 1. For the $(n, n-1)$ single parity check code, its parity check matrix is the matrix $[1, \ldots, 1]$ (it is the dual of the repetition code, whose generator matrix is $[1, \ldots, 1]$). We need d linearly dependent columns (they are all linearly dependent), but such that no $d-1$ columns are linearly dependent. So $d = 2$, which is consistent with what we know.

2. For the $(4, 2)$ tetracode over $\mathbb{F}_3$, it is self-dual so its systematic parity check matrix is the same as its generator matrix, namely

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

We need d linearly dependent columns, we have that the first 3 columns for example are linearly dependent, and any two columns are linearly independent (for two vectors to be linearly dependent, we need $\lambda_1 \mathbf{x}_1 + \lambda_2 \mathbf{x}_2 = 0$, for λ_1, λ_2 non-zero, that is $\mathbf{x}_1$ and $\mathbf{x}_2$ are multiples of each others). So $d = 3$, which is also consistent with what we know.

Exercise 9. (*)

For $\mathbf{x} \in \mathbb{F}_3^n$, prove that $wt(\mathbf{x}) \equiv \mathbf{x} \cdot \mathbf{x}^T \pmod 3$.

Solution 9. A vector $\mathbf{x} \in \mathbb{F}_3^n$ has non-coefficients which are either 1 or 2, thus $\mathbf{x} \cdot \mathbf{x}$ will contain $0^2 \equiv 0$, $1^2 \equiv 1$ and $2^2 \equiv 1$ so it counts 1 for every non-zero coefficients, which is the weight modulo 3.

Exercise 10.

Consider the $(4, 2)$ tetracode $\mathcal{C}$ over $\mathbb{F}_3$. For every codework $\mathbf{c}$ of $\mathcal{C}$, construct a Hamming sphere $S_t(\mathbf{c})$ of radius t such that no sphere intersects.

Solution 10. First we recall that the tetracode is given by

$$\mathcal{C} = \{(x_1, x_2, x_1 + x_2, x_1 - x_2),\ x_1, x_2 \in \mathbb{F}_3\}$$

and that by definition a Hamming sphere $S_t(\mathbf{c})$ is

$$S_t(\mathbf{c}) = \{\mathbf{v} \in \mathbb{F}_3^4,\ d_H(\mathbf{c}, \mathbf{v}) \leq t\}.$$

We know from a result seen in class that if the minimum Hamming distance $d_H(\mathcal{C})$ is d, then spheres of radius $t = \lfloor \frac{d-1}{2} \rfloor$ around distinct codewords are disjoint, so we will use here $t = 1$ (make sure you remember why $d_H(\mathcal{C}) = 3$). We next have to compute $S_1(\mathbf{c})$ for $\mathbf{c} \in \mathcal{C}$, in the computations below, a_1, a_2, a_3 are always element of $\mathbb{F}_3$:

$$\begin{aligned}
S_1((0,0,0,0)) &= \{(0,0,0,0), (a_1,0,0,0), (0,a_1,0,0), (0,0,a_1,0), (0,0,0,a_1),\ a_1 \neq 0\} \\
S_1((1,0,1,1)) &= \{(1,0,1,1), (a_1,0,1,1), (1,a_2,1,1), (1,0,a_1,1), (1,0,1,a_1),\ a_1 \neq 1,\ a_2 \neq 0\} \\
S_1((2,0,2,2)) &= \{(2,0,2,2), (a_1,0,2,2), (2,a_2,2,2), (2,0,a_1,2), (2,0,2,a_1),\ a_1 \neq 2,\ a_2 \neq 0\} \\
S_1((0,1,1,2)) &= \{(0,1,1,2), (a_1,1,1,2), (0,a_2,1,2), (0,1,a_2,2), (0,1,1,a_3),\ a_1 \neq 0,\ a_2 \neq 1,\ a_3 \neq 2\} \\
S_1((1,1,2,0)) &= \{(1,1,2,0), (a_1,1,2,0), (1,a_1,2,0), (1,1,a_2,0), (1,1,2,a_3),\ a_1 \neq 1,\ a_2 \neq 2,\ a_3 \neq 0\} \\
S_1((2,1,0,1)) &= \{(2,1,0,1), (a_1,1,0,1), (2,a_2,0,1), (2,1,a_3,1), (2,1,0,a_2),\ a_1 \neq 2,\ a_2 \neq 1,\ a_3 \neq 0\} \\
S_1((0,2,2,1)) &= \{(0,2,2,1), (a_1,2,2,1), (0,a_2,2,1), (0,2,a_2,1), (0,2,2,a_3),\ a_1 \neq 0,\ a_2 \neq 2,\ a_3 \neq 1\} \\
S_1((1,2,0,2)) &= \{(1,2,0,2), (a_1,2,0,2), (1,a_2,0,2), (1,2,a_3,2), (1,2,0,a_2),\ a_1 \neq 1,\ a_2 \neq 2,\ a_3 \neq 3\} \\
S_1((2,2,1,0)) &= \{(2,2,1,0), (a_1,2,1,0), (2,a_1,1,0), (2,2,a_2,0), (2,2,1,a_3),\ a_1 \neq 2,\ a_2 \neq 1,\ a_3 \neq 0\}
\end{aligned}$$

Exercise 11. (*)

Let $\mathcal{C}$ be the code over $\mathbb{F}_2$ given by the generator matrix

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

Do the codewords of $\mathcal{C}$ whose weights are divisible by 4 form a linear code? Justify your answer.

Solution 11. It is not a linear code. Take for example the sum of row 1 and row 3, given by $(0,0,1,1,1,1)$, and the sum of row 2 and row 3, given by $(1,0,0,1,1,1)$. The sum of these two codewords is

$$(0,0,1,1,1,1) + (1,0,0,1,1,1) = (1,0,1,0,0,0).$$

This codeword has weight 2, which is not divisible by 4, therefore the code cannot be linear.

Exercise 12.

[Exercise 66 from Huffman and Pless] The weight of a coset is the smallest weight of a vector in the coset. Find a non-zero linear $(4,k)$ code over $\mathbb{F}_2$ of minimum Hamming distance d such that all cosets contain a unique vector whose weight is the coset weight, and some coset has weight greater than $t = \lfloor \frac{d-1}{2} \rfloor$.

Solution 12. We consider a code $\mathcal{C}$ which is of length $n = 4$ over $\mathbb{F}_2$, which means the code comprises codewords of the form $(x_1, x_2, x_3, x_4) \in \mathbb{F}_2^4$.

- The code itself is a coset, and it necessarily contains $(0,0,0,0)$ since the code is linear. This codeword has Hamming weight 0, therefore the weight of this coset is 0 (and there is no other vector in it with weight 0).
- We know cosets partition $\mathbb{F}_2^4$, so every vector must appear in one coset. In particular, the vectors $(1,0,0,0)$, $(0,1,0,0)$, $(0,0,1,0)$ and $(0,0,0,1)$ (which are all vectors of weight 1) must belong to some coset.
- As a consequence that cosets partition $\mathbb{F}_2^4$, $|\mathbb{F}_2^4| = 2^4 = |\mathcal{C}| \cdot$(number of cosets) $= 2^k 2^{n-k}$. So the number of cosets is a power of 2: it cannot be 1 (this is when $n = k$), so it could be 2, 4 or 8 (it cannot be 16, this is when $k = 0$).

Suppose we have 4 cosets, then we also have 4 vectors of weight 1, and we cannot put two vectors of weight 1 in the same coset, since this would violate the rule that we want only one vector of smallest weight, except if the coset is the code itself, since then we have a vector of weight 0 (which cannot happen with other cosets). So we could try to build a code that has 4 cosets, each coset contains 4 codewords, and the coset which is the code will contain one vector of weight 1, say $(1,0,0,0)$.

coset 1 $= \mathcal{C}$	coset 2	coset 3	coset 4
$(0,0,0,0)$	$(0,1,0,0)$	$(0,0,1,0)$	$(0,0,0,1)$
$(1,0,0,0)$			

Since we want the code to be a linear code, we must have $k = 2$, therefore we will have codewords of the form (x_1, x_2, x_3, x_4) with $(x_1, x_2) \in \mathbb{F}_2^2$. Then x_3 gives 0 both with $(x_1, x_2) = (0,0), (1,0)$, so $x_3 = x_2$. But by the same

reasoning, we should have $x_4 = x_2$. It is a strange code which basically sends two information bits, yet protects only the second one, but as per our definition of code, it is a subspace of dimension 2, so it is valid:

coset $1 = \mathcal{C}$	coset 2	coset 3	coset 4
$(0,0,0,0)$	$(0,1,0,0)$	$(0,0,1,0)$	$(0,0,0,1)$
$(1,0,0,0)$			
$(0,1,1,1)$			
$(1,1,1,1)$			

So let us now compute the cosets.

coset $1 = \mathcal{C}$	coset 2	coset 3	coset 4
$(0,0,0,0)$	$(0,1,0,0)$	$(0,0,1,0)$	$(0,0,0,1)$
$(1,0,0,0)$	$(1,1,0,0)$	$(1,0,1,0)$	$(1,0,0,1)$
$(0,1,1,1)$	$(0,0,1,1)$	$(0,1,0,1)$	$(0,1,1,0)$
$(1,1,1,1)$	$(1,0,1,1)$	$(1,1,0,1)$	$(1,1,1,0)$

If we look at the weight of each coset, coset 1 has weight 0, all the others have weight 1, and they also have a single vector of smallest weight, as requested. We are left to check the condition that some coset has weight greater than $\lfloor \frac{d-1}{2} \rfloor$. Here $d = 1$ (namely, the Hamming distance is 1), so $t = 0$ and indeed we have 3 cosets of weight 1.

Exercise 13. (*)

For $\mathcal{C}_1, \mathcal{C}_2$ two linear codes of length n over $\mathbb{F}_q$, consider the set

$$\mathcal{C}_1 + \mathcal{C}_2 = \{\mathbf{c}_1 + \mathbf{c}_2,\ \mathbf{c}_1 \in \mathcal{C}_1,\ \mathbf{c}_2 \in \mathcal{C}_2\}.$$

Show that $(\mathcal{C}_1 + \mathcal{C}_2)^\perp = \mathcal{C}_1^\perp \cap \mathcal{C}_2^\perp$.

Solution 13. By definition, $(\mathcal{C}_1 + \mathcal{C}_2)^\perp = \{\mathbf{y} \in \mathbb{F}_q^n,\ \mathbf{y} \cdot \mathbf{c} = 0 \text{ for all } \mathbf{c} \in \mathcal{C}_1 + \mathcal{C}_2\} = \{\mathbf{y} \in \mathbb{F}_q^n,\ \mathbf{y} \cdot \mathbf{c}_1 + \mathbf{y} \cdot \mathbf{c}_2 = 0 \text{ for all } \mathbf{c}_1 \in \mathcal{C}_1, \mathbf{c}_2 \in \mathcal{C}_2\}$. Since this holds for all $\mathbf{c}_1, \mathbf{c}_2$ and both belong to linear codes, they can take the value $\mathbf{0}$, and so $\mathbf{y}$ must be both orthogonal to $\mathbf{c}_1$ and to $\mathbf{c}_2$.

Exercise 14.

Suppose the $(4, 2)$ tetracode over $\mathbb{F}_3$ was used and the following vectors were received:

1. $(1, 1, 1, 1)$
2. $(1, -1, 0, -1)$

Decode these vectors.

Solution 14. The tetracode is self-dual, so its generator matrix in systematic form is also a parity check matrix:

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

Note that

$$\begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & -1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = x_1 \begin{bmatrix} 1 \\ 0 \end{bmatrix} + x_2 \begin{bmatrix} 0 \\ 1 \end{bmatrix} + x_3 \begin{bmatrix} 1 \\ 1 \end{bmatrix} + x_4 \begin{bmatrix} 1 \\ -1 \end{bmatrix}.$$

When computing the table with syndromes $H\mathbf{x}^T$ and coset leaders, we first consider $\mathbf{x}$ with weight 0 or less, and thus we know that computing $H\mathbf{x}^T$ will give the column i of H if $\mathbf{x}$ has a one in coordinate i and zeros elsewhere, and similarly it will give twice the column i of H if $\mathbf{x}$ has a two in coordinate i and zeros elsewhere. Also since $|\mathbb{F}_3^4| = 3^4 = 3^2 3^2$, there are 9 cosets.

	$H\mathbf{x}^T$	coset leader
$(0,0)$	$H(0,0,0,0)^T$	$(0,0,0,0)$
$(1,0)$	$H(1,0,0,0)^T$	$(1,0,0,0)$
$(0,1)$	$H(0,1,0,0)^T$	$(0,1,0,0)$
$(1,1)$	$H(0,0,1,0)^T$	$(0,0,1,0)$
$(1,2)$	$H(0,0,0,1)^T$	$(0,0,0,1)$
$(2,0)$	$H(2,0,0,0)^T$	$(2,0,0,0)$
$(0,2)$	$H(0,2,0,0)^T$	$(0,2,0,0)$
$(2,2)$	$H(0,0,2,0)^T$	$(0,0,2,0)$
$(2,1)$	$H(0,0,0,2)^T$	$(0,0,0,2)$

For the received vectors $(1,1,1,1)$ and $(1,-1,0,-1)$, we compute their respective syndromes:

$$H(1,1,1,1)^T = (0,1),\ H(1,-1,0,-1)^T = (0,0).$$

Then we decode them as:

$$\mathbf{y} = (1,1,1,1) \to \hat{\mathbf{c}} = (1,1,1,1) - (0,1,0,0) = (1,0,1,1),$$

this would mean recovering from one error, and

$$\mathbf{y} = (1,-1,0,-1) \to \hat{\mathbf{c}} = (1,-1,0,-1) - (0,0,0,0) = (1,-1,0,-1),$$

that is there was no error (or there were enough errors to send one codeword to another).

Exercise 15. (*)

Let $\mathcal{C}$ be the code over $\mathbb{F}_2$ given by the generator matrix

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

1. How many cosets of $\mathcal{C}$ are there?
2. What is the minimum distance of $\mathcal{C}$?

3. Construct a table of all syndromes. If possible, decode the following:

   - $(1,1,0,1,0,1,0)$,
   - $(0,0,1,0,0,0,0)$.

Solution 15. 1. The number of cosets is $2^{n-k} = 2^3 = 8$.

2. The minimum distance of $\mathcal{C}$ is 3, because there is a word of weight 3, e.g. $(1,0,0,0,1,0,1)$. It is not possible to find a codeword of weight 1 or 2, since having a single information symbol to be non-zero creates at least two parities which are not zero. Alternatively, compute a parity check matrix:

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

   H has a set of 3 linearly dependent columns, e.g., column 7,6 and 3. It has no set of 2 columns linearly dependent, since no column is repeated.

3. A table of all syndromes is given by

$(0,0,0)$	$H(0,0,0,0,0,0,0)^T$
$(1,0,1)$	$H(1,0,0,0,0,0,0)^T$
$(1,1,0)$	$H(0,1,0,0,0,0,0)^T$
$(0,1,1)$	$H(0,0,1,0,0,0,0)^T$
$(1,1,1)$	$H(0,0,0,1,0,0,0)^T$
$(1,0,0)$	$H(0,0,0,0,1,0,0)^T$
$(0,1,0)$	$H(0,0,0,0,0,1,0)^T$
$(0,0,1)$	$H(0,0,0,0,0,0,1)^T$

   If possible, decode the following:

   - $(1,1,0,1,0,1,0)$, the syndrome is $(1,1,0)$ and so the decoded codeword is $(1,0,0,1,0,1,0)$.
   - $(0,0,1,0,0,0,0)$, the sydnrome is $(0,1,1)$ and the decoded codeword is $(0,0,0,0,0,0,0)$.

   Since $t = 1$, there are unique coset leaders and decoding can be done.

Exercise 16.

Consider the following generator matrix over $\mathbb{F}_2$:

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

Justify all your answers.

1. Write the matrix G in systematic form.
2. What are the dimension k and the length n of the corresponding code $\mathcal{C}$?

3. Compute a parity check matrix for this code $\mathcal{C}$.
4. Is this code $\mathcal{C}$ self-dual? self-orthogonal?
5. Compute the minimum distance of $\mathcal{C}$.
6. Does $\mathcal{C}$ contain a codeword of weight 4?
7. Suppose the decoder receives $(1, 0, 0, 0, *, 1)$ where $*$ is an erased symbol. What is the codeword being sent?
8. How many cosets of $\mathcal{C}$ are there?
9. Construct a table of coset leaders and associated syndromes.
10. One coset has weight 2, which coset is it and what are its coset leaders?
11. If possible, decode the following received vectors:
    (a) $(1, 1, 0, 1, 1, 0)$
    (b) $(1, 1, 0, 1, 1, 1)$
    (c) $(1, 1, 0, 0, 0, 1)$.

    If decoding is not possible, explain why.

Solution 16. 1. To write

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

in systematic form, we first add row 1 to row 3

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

and then add row 2 to row 1:

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

2. The length n is 6, it is just the number of columns of G. Now for k, it is 3 because we have three rows that are linearly independent.
3. Since we have G in systematic form, we will use it to compute H:

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

4. If we wanted the code to be self-orthogonal, we would need $\mathcal{C}$ to be inside its dual $\mathcal{C}^\perp$, and since $\mathcal{C}^\perp$ is the set of vectors orthogonal to every vector in the code, this means that every $\mathbf{c} \in \mathcal{C}$ must be orthogonal to every codeword, in particular to itself, so $\mathbf{c} = (0,1,1,1,0,0)$ is not orthogonal to itself, so it cannot be in $\mathcal{C}^\perp$ and thus the code is not self-orthogonal, thus not self-dual either.

5. A generic codeword is of the form $(x_1, x_2, x_3, x_2+x_3, x_1+x_3, x_1+x_2)$. When $x_1 = 1$ and $x_2 = x_3 = 0$, we get $(1,0,0,0,1,1)$, which has weight 3. To have a weight less than 3 is not possible: if only one data symbol is not zero, there are two parities which are not zero, and if two data symbols are not zero, there will at least be one parity symbol which is not zero. Therefore the Hamming distance is 3.

6. Again a generic codeword is of the form $(x_1, x_2, x_3, x_2+x_3, x_1+x_3, x_1+x_2)$. We just showed above that a single data symbol which is not zero means a weight of 3. So let us try two data symbols which are not zero, say $x_1 = 0$, $x_2 = x_3 = 1$, this gives the codeword $(0,1,1,0,1,1)$ which has weight 4.

7. Suppose the decoder receives $(1,0,0,0,*,1)$ where $*$ is an erased symbol. Since the Hamming distance of the code is 3, we can recover the codeword $(1,0,0,0,1,1)$.

8. To count the number of cosets of $\mathcal{C}$, we recall that $|\mathbb{F}_2^6| = 2^6 = |\mathcal{C}|$(number of cosets). Thus $2^6 = 2^3 \cdot 2^3$ and there are 8 cosets.

9. To construct a table of coset leaders and associated syndromes, we first construct the syndromes. We know that there 8 syndromes of the form $H\mathbf{x}^T$, we first choose $\mathbf{x}$ to be a vector of weight either 0 or 1, this gives the following table:

$H\mathbf{x}^T$	coset leader
$H(0,0,0,0,0,0)^T$	$(0,0,0,0,0,0)$
$H(1,0,0,0,0,0)^T$	$(1,0,0,0,0,0)$
$H(0,1,0,0,0,0)^T$	$(0,1,0,0,0,0)$
$H(0,0,1,0,0,0)^T$	$(0,0,1,0,0,0)$
$H(0,0,0,1,0,0)^T$	$(0,0,0,1,0,0)$
$H(0,0,0,0,1,0)^T$	$(0,0,0,0,1,0)$
$H(0,0,0,0,0,1)^T$	$(0,0,0,0,0,1)$
$H(?,?,?,?,?,?)^T$	$?$

We note that since

$$H = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{bmatrix} = x_1 \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} + \ldots + x_6 \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix},$$

$H\mathbf{x}^T$ where $\mathbf{x}^T$ is non-zero only in its ith coordinate means the syndrome is the ith column of H. Thus the missing syndrome in the table is $(1,1,1)$ which could be obtained for example using $x_1 = 1$ and $x_4 = 1$ (the other x_i are zero). We note that the corresponding coset necessarily has weight 2, since all vectors of weight less than 2 are already in the other cosets.

$H\mathbf{x}^T$	coset leader
$(0,0,0)$	$(0,0,0,0,0,0)$
$(0,1,1)$	$(1,0,0,0,0,0)$
$(1,0,1)$	$(0,1,0,0,0,0)$
$(1,1,0)$	$(0,0,1,0,0,0)$
$(1,0,0)$	$(0,0,0,1,0,0)$
$(0,1,0)$	$(0,0,0,0,1,0)$
$(0,0,1)$	$(0,0,0,0,0,1)$
$(1,1,1)$	$(1,0,0,1,0,0)$

10. One coset has weight 2, it is the coset $(1,0,0,1,0,0)+\mathcal{C}$. Its coset leaders are vectors of weight 2. We already know that $(1,0,0,1,0,0)$ has weight 2, and generic vectors in this coset are of the form $(x_1+1, x_2, x_3, x_2+x_3+1, x_1+x_3, x_1+x_2)$:

(x_1,x_2,x_3)	$(x_1+1, x_2, x_3, x_2+x_3+1, x_1+x_3, x_1+x_2)$
$(0,0,0)$	$(1,0,0,1,0,0)$
$(1,0,0)$	$(0,0,0,1,1,1)$
$(0,1,0)$	$(1,1,0,0,0,1)$
$(1,1,0)$	$(0,1,0,0,1,0)$
$(0,0,1)$	$(1,0,1,0,1,0)$
$(1,0,1)$	$(0,0,1,0,0,1)$
$(0,1,1)$	$(1,1,1,1,1,1)$
$(1,1,1)$	$(0,1,1,1,0,0)$

We see two other vectors of weight 2, namely $(0,1,0,0,1,0)$ and $(0,0,1,0,0,1)$.

11. We received the following vectors:

    (a) $(1,1,0,1,1,0)$
    (b) $(1,1,0,1,1,1)$
    (c) $(1,1,0,0,0,1)$.

    We start by computing their syndromes:

    $$H(1,1,0,1,1,0)^T = (0,0,0)^T,\ H(1,1,0,1,1,1)^T = (0,0,1)^T,\ H(1,1,0,0,0,1)^T = (1,1,1)^T.$$

    Then the decoded codeword is the received vector minus the coset leader, that is

    $$(1,1,0,1,1,0) - (0,0,0,0,0,0),\ (1,1,0,1,1,1) - (0,0,0,0,0,1),$$

    for $(1,1,0,0,0,1)$, we actually have several coset leaders, so the decoder cannot make a direct decision. For the other two cases:

    $$\mathbf{y} = (1,1,0,1,1,0) \to \hat{\mathbf{c}} = (1,1,0,1,1,0),$$

this would correspond to a transmission with no error (or there are enough errors to actually swap a codeword with another), and

$$\mathbf{y} = (1,1,0,1,1,1) \to \hat{\mathbf{c}} = (1,1,0,1,1,0),$$

this would correspond to a transmission with one error.

Exercise 17.

Let $\mathcal{C}$ be an $(n,1)$ repetition code over $\mathbb{F}_2$. Find the parameters n for which $\mathcal{C}$ is perfect.

Solution 17. For $\mathcal{C}$ to be perfect, it needs to have parameters that match the Sphere Packing Bound:

$$SPB = \frac{q^n}{\sum_{i=0}^{t} \binom{n}{i}(q-1)^i}.$$

Recall that $d_H(\mathcal{C}) = n$. For $q = 2$ and n odd, that is $n = 2t+1$ ($\iff$ $t = \lfloor \frac{n-1}{2} \rfloor = \frac{n-1}{2}$), we have, recalling that $\binom{n}{i} = \binom{n}{n-i}$:

$$\begin{aligned}
\sum_{i=0}^{t} \binom{n}{i}(q-1)^i &= \frac{1}{2}\left(\sum_{i=0}^{t}\binom{n}{i} + \sum_{i=0}^{t}\binom{n}{n-i}\right) \\
&= \frac{1}{2}\left(\sum_{i=0}^{t}\binom{n}{i} + \sum_{s=t+1}^{n}\binom{n}{s}\right) \\
&= \frac{1}{2}\sum_{i=0}^{n}\binom{n}{i} = 2^{n-1}
\end{aligned}$$

using the change of variable $s = n - i$ in the second equality, and noticing that after this change of variables, the second sum contains all the terms between $s = n$ and $s = n - t = (2t+1) - t = t + 1$. In this case, the repetition code is thus perfect. The code is not perfect for $q = 2$ and n even, which can be seen from the formulas (we would have $\sum_{s=t}^{n}\binom{n}{s}$ and thus the term in $s = t$ would repeat the term in $i = t$).

Exercise 18.

Provide an example of two codes $\mathcal{C}_1$ and $\mathcal{C}_2$ such that

$$\mathcal{C}_1 M = \mathcal{C}_2,\ \mathcal{C}_1^{\perp} M \neq \mathcal{C}_2^{\perp},$$

for M a monomial matrix.

Solution 18. Suppose $\mathcal{C}_1$ has generator matrix $[1,1]$ and $\mathcal{C}_2$ has generator matrix $[1,w]$ both over $\mathbb{F}_4$. We build a monomial matrix

$$M = \begin{bmatrix} 1 & 0 \\ 0 & w \end{bmatrix}$$

and check the condition $\mathcal{C}_1 M = \mathcal{C}_2$:

$$[1,1]\begin{bmatrix}1 & 0\\ 0 & w\end{bmatrix} = [1,w].$$

Then $\mathcal{C}_1^\perp$ has generator matrix $[1,1]$ and $\mathcal{C}_2^\perp$ has generator matrix $[w,1]$, or equivalently, multiply the basis by w^2, $[1,w^2]$. We have

$$[1,1]\begin{bmatrix}1 & 0\\ 0 & w\end{bmatrix} = [1,w] \neq [1,w^2].$$

Exercise 19.

If $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$, prove that

$$wt(\mathbf{x}+\mathbf{y}) = wt(\mathbf{x}) + wt(\mathbf{y}) - 2wt(\mathbf{x} \cap \mathbf{y})$$

where $\mathbf{x} \cap \mathbf{y}$ is the vector in $\mathbb{F}_2^n$ which has 1s precisely in the positions where both $\mathbf{x}$ and $\mathbf{x}$ have 1s.

Solution 19. It is enough to look at a single coordinate. If $\mathbf{x}$ and $\mathbf{y}$ disagree on this coordinate, this means one has a zero and the other a one, thus summing these two coordinates will give one, which is indeed $wt(\mathbf{x}) + wt(\mathbf{y})$ ($wt(\mathbf{x} \cap \mathbf{y})$ has a zero in this coordinate). Then if $\mathbf{x}$ and $\mathbf{y}$ agree on this coordinate, either they agree on zero, and both sides of the equality are zero, or they agree on one: then the left hand-side contains a zero ($1 + 1 \equiv 0$), while $wt(\mathbf{x}) + wt(\mathbf{y})$ counts two, which is cancelled out by $-2wt(\mathbf{x} \cap \mathbf{y})$.

Exercise 20.

Let $\mathcal{C}$ be a binary linear code. Show that if $\mathcal{C}$ is self-orthogonal and has a generator matrix such that each row has a weight divisible by 4, then every codeword of $\mathcal{C}$ has a weight divisible by 4.

Solution 20. Consider two rows $\mathbf{x}$ and $\mathbf{y}$ of the generator matrix. Using Exercise 19, we know that $wt(\mathbf{x}+\mathbf{y}) = wt(\mathbf{x}) + wt(\mathbf{y}) - 2wt(\mathbf{x} \cap \mathbf{y})$, and $wt(\mathbf{x}) \equiv wt(\mathbf{y}) \equiv 0 \pmod 4$ since each weight is divisible by 4. Furthemore, the code is contained in its dual. This means that the inner product of $\mathbf{x}$ and $\mathbf{y}$ must be zero, therefore $\mathbf{x}$ and $\mathbf{y}$ need to agree on an even number of coordinates, which shows that $2wt(\mathbf{x} \cap \mathbf{y}) \equiv 0 \pmod 4$. We just showed that the sum of two rows of the generator matrix has a weight divisible by 4. Now every codeword is obtained as a linear combination (that is for the binary case as a sum) of rows of the generator matrix. We can complete the proof by induction. Suppose it is true for l rows of the matrix, and we want to prove it is true for $l+1$. We know that codewords obtained as the sum of l rows have a weight divisible by 4, let us call $\mathbf{c}$ such a codeword. Then suppose $\mathbf{x}$ is a new row of the generator matrix. Then $wt(\mathbf{x}+\mathbf{c}) \equiv 0$ using the same arguments as above.

Exercise 21.

Show that the Golay code $\mathcal{G}_{12}$ is a $(12, 6, 6)$ self-dual code and that the Golay code $\mathcal{G}_{11}$ has minimum distance 5.

Solution 21. We recall that a generator matrix for $\mathcal{G}_{12}$ is $G = [\mathbf{I}_6, A]$ with

$$A = \left[\begin{array}{c|ccccc} 0 & 1 & 1 & 1 & 1 & 1 \\ \hline 1 & 0 & 1 & 2 & 2 & 1 \\ 1 & 1 & 0 & 1 & 2 & 2 \\ 1 & 2 & 1 & 0 & 1 & 2 \\ 1 & 2 & 2 & 1 & 0 & 1 \\ 1 & 1 & 2 & 2 & 1 & 0 \end{array}\right].$$

The code has length 12 since there are 12 columns in G, it has dimension 6 because G contains 6 rows that are linearly independent. We next show that $\mathcal{G}_{12}$ is self-orthogonal:

- Every row is orthogonal to each other since: (1) row 1 contains 6 ones, and $6 \equiv 0 \pmod 3$, (2) for row 2, $(1,0,1,2,2,1) \cdot (1,0,1,2,2,1) = 11 \equiv 2 \pmod 3$ so row 2 is orthogonal to itself, (3) other rows are shift of row 2.
- The inner product between row 1 and row i for $i \geq 2$ is $1+2+2+1 \equiv 0 \pmod 3$.
- The inner product between row 2 and row i for $i \geq 2$ is 0 by inspection.
- The inner product between row i and row j, $i \geq 3$, $j \geq 4$ is also 0, by shifing row i so as to obtain row 2, and use the same shift on row j.

Since every row of G is orthogonal to all rows of G, $\mathcal{G}_{12} \subseteq \mathcal{G}_{12}^{\perp}$ and since they have both dimensions 6, they are equal.

We next look at the Hamming distance. We mimic the arguments done for the binary case. First we notice that the Hamming weight of every codeword $\mathbf{c}$ is divisible by 3, this is because $wt(\mathbf{c}) = \mathbf{c} \cdot \mathbf{c} \pmod 3$, but $\mathbf{c} \cdot \mathbf{c} \equiv 0 \pmod 3$ since the code is self-dual. So the Hamming distance of the code is either 3 or 6 (we have codewords of weight 6). We are thus left to rule out 3. Write $\mathbf{c} = (\mathbf{c}_1, \mathbf{c}_2)$ with $\mathbf{c}_1, \mathbf{c}_2 \in \mathbb{F}_3^6$.

- $wt(\mathbf{c}_1) = 0$, $wt(\mathbf{c}_2) = 3$: impossible since $wt(\mathbf{c}_1) = 0$ implies $\mathbf{c} = \mathbf{0}$.
- $wt(\mathbf{c}_1) = 1$, $wt(\mathbf{c}_2) = 2$: impossible since $wt(\mathbf{c}_1) = 1$ implies $\mathbf{c}$ is one row of G, and none have weight 2.
- $wt(\mathbf{c}_1) = 2$, $wt(\mathbf{c}_2) = 1$: impossible since $wt(\mathbf{c}_1) = 2$ implies $\mathbf{c}$ is a linear combination of two rows of G, but then this linear combination should cancel all coefficients but one in $\mathbf{c}_2$, which cannot happen.
- $wt(\mathbf{c}_1) = 3$, $wt(\mathbf{c}_2) = 0$: impossible since $wt(\mathbf{c}_2) = 0$ implies that there is a linear combination of 3 rows that cancel all coefficients in $\mathbf{c}_2$.

Finally, to show that the Golay code $\mathcal{G}_{11}$ has minimum distance 5, it is enough to notice that $\mathcal{G}_{12}$ has minimum distance 6, and that a codeword of minimum distance 6 is punctured in a non-zero coordinate.

Exercise 22.

1. Let $\mathcal{C}$ be a code over $\mathbb{F}_q$. Let $\mathcal{C}_1$ be the code obtained from $\mathcal{C}$ by puncturing on the right-most coordinate and then extending this punctured code on the right. Prove that $\mathcal{C} = \mathcal{C}_1$ if and only if all codewords of $\mathcal{C}$ have the property that the sum of their coordinates is 0 (these codewords are sometimes called even-like).

2. With $\mathcal{C}_1$ as above, prove that if $\mathcal{C}$ is self-orthogonal and contains the all-one codeword $(1, \ldots, 1)$ then $\mathcal{C} = \mathcal{C}_1$.

Solution 22. 1. If $\mathcal{C} = \mathcal{C}_1$, then it means that the set of codewords obtained by (1) removing the last coordinate (codewords are now of the form $(c_1, \ldots, c_{n-1})$), and (2) adding as last coordinate minus the sum of the $n-1$ coordinates (codewords are now of the form $(c_1, \ldots, c_{n-1}, -c_1 - \ldots - c_{n-1})$), is the set $\mathcal{C}$. So it must have been that codewords were already of the form $(c_1, \ldots, c_{n-1}, -c_1 - \ldots - c_{n-1})$). Conversely, if codewords are of the form $(c_1, \ldots, c_{n-1}, -c_1 - \ldots - c_{n-1})$, then we will have $\mathcal{C} = \mathcal{C}_1$.

2. If $\mathcal{C}$ is self-orthogonal, and $(1, \ldots, 1) \in \mathcal{C}$, then it must be that $(1, \ldots, 1) \in \mathcal{C}^\perp$, which means that $(1, \ldots, 1) \cdot \mathbf{c} \equiv 0$ for all $\mathbf{c} \in \mathcal{C}$. But then this means that $c_1 + \ldots + c_{n-1} + c_n = 0$ thus $c_1 + \ldots, c_{n-1} = -c_n$. We then use the previous point to conclude.

Exercise 23. (*)

Does puncturing a binary $(24, 12, 8)$ code (in any position) yield a perfect code? Justify your answer.

Solution 23. If we puncture a $(24, 12, 8)$ code, we are removing a column of the generator matrix, so the resulting code has dimenion 23. Since $d_H = 8$, the dimension $k = 12$ does not change, and the new minimum distance is either 8 or 7.

Now for a code to be perfect, its parameters need to meet the Sphere Packing Bound, which, for a binary code is

$$\frac{2^{23}}{\sum_{i=0}^{t} \binom{23}{i}}, \; t = \lfloor \frac{8-1}{2} \rfloor = 3 \text{ or } \; t = \lfloor \frac{7-1}{2} \rfloor = 3.$$

We then compute

$$\begin{aligned} & \frac{2^{23}}{\sum_{i=0}^{3} \binom{23}{i}} \\ = & \frac{2^{23}}{1 + 23 + 23 \cdot 11 + 23 \cdot 11 \cdot 7} \\ = & \frac{2^{23}}{24 + 23 \cdot 11 \cdot 8} \\ = & \frac{2^{20}}{3 + 23 \cdot 11} = \frac{2^{20}}{256} = 2^{12}. \end{aligned}$$

Thus the punctured code is perfect.

Exercise 24.

1. Does extending a binary $(5, 3, 3)$ code yield a perfect code? Justify your answer.

2. What is the geometric interpretation of a perfect code?

Solution 24. 1. Extending a binary $(5, 3, 3)$ code means that the resulting code will have a length of 6, and the minimum distance could remain 3 or go to 4. To check whether the code is perfect, one uses the Sphere Packing Bound:

$$\frac{2^6}{\sum_{i=0}^{t} \binom{6}{i}}, \ t = \lfloor \frac{d-1}{2} \rfloor.$$

Whether $d = 3, 4$, we have

$$\lfloor \frac{4-1}{2} \rfloor = 1, \ \lfloor \frac{3-1}{2} \rfloor = 1$$

so the bound becomes

$$\frac{2^6}{\binom{6}{0} + \binom{6}{1}} = \frac{2^6}{1+6}$$

so we do not get a perfect code.

2. A perfect code reaches the Sphere Packing Bound. This means that the whole space containing q^n elements is partitioned into q^k (if the code is linear, or into the number of codewords in general) disjoint Hamming spheres, with as their centers codewords, and as their radius t.

Exercise 25. (*)

Construct, if possible, an $(8, 4, 4)$ binary code using the $(\mathbf{u}|\mathbf{u}+\mathbf{v})$ construction.

Solution 25. Reed-Mueller codes are built using this construction, and they yield codes of length 2^m, so we look at $m = 3$. They have minimum distance $2^{m-r} = 2^{3-r}$, so take $r = 1$ to give a minimum Hamming distance of 4. We are left to check that we get the right dimension:

$$\binom{3}{0} + \binom{3}{1} = 1 + 3 = 4$$

so an example is the Reed-Mueller code $\mathcal{R}(1, 3)$.

Exercise 26.

Prove that the $(\mathbf{u}|\mathbf{u}+\mathbf{v})$ construction has minimum Hamming distance $\min\{2d_1, d_2\}$ if d_1, d_2 are the minimum Hamming distances of $\mathcal{C}_1$ and $\mathcal{C}_2$.

Solution 26. We look at generic codewords, of the form $(\mathbf{u}, \mathbf{u}+\mathbf{v})$, $\mathbf{u} \in \mathcal{C}_1$, $\mathbf{v} \in \mathcal{C}_2$. Since both $\mathcal{C}_1, \mathcal{C}_2$ are linear codes, they each contain the zero codeword.

When $\mathbf{v} = \mathbf{0}$, we get the codeword $(\mathbf{u}, \mathbf{u})$, for $\mathbf{u} \in \mathcal{C}_1$, in which case the minimum Hamming distance is twice that of $\mathcal{C}_1$, namely $2d_1$:

$$wt((\mathbf{u}, \mathbf{u})) \geq 2d_1 \geq \min(2d_1, d_2).$$

When $\mathbf{u} = \mathbf{0}$, we get the codeword $(\mathbf{0}, \mathbf{v})$, for $\mathbf{v} \in \mathcal{C}_2$, in which case the minimum Hamming distance is that of $\mathcal{C}_2$, namely d_2:

$$wt((\mathbf{0}, \mathbf{v})) \geq d_2 \geq \min(2d_1, d_2).$$

This already gives us a minimum Hamming distance of $\min\{2d_1, d_2\}$, though we still need to argue that when $\mathbf{u}, \mathbf{v}$ are both not zero, we cannot decrease the found minimum distance. Then

$$wt((\mathbf{u}, \mathbf{u}+\mathbf{v})) = wt(\mathbf{u})+wt(\mathbf{u}+\mathbf{v}) \geq wt(\mathbf{u})+(wt(\mathbf{v})-wt(\mathbf{u})) \geq wt(\mathbf{v}) \geq \min(2d_1, d_2).$$

The inequality holds true since: in $\mathbf{u}+\mathbf{v}$, we look at $\mathbf{v}$, it has some weight $wt(\mathbf{v})$, now when we add $\mathbf{u}$, whenever $u_i = -v_i$, the weight drops by 1, whenever $u_i \neq 0$ and $v_i = 0$, the weight increases by 1, in all other cases, there is no change. So a bound is obtained by subtracting $wt(\mathbf{u})$: when $u_i = -v_i$, the weight drops by 1, when $u_i \neq 0$ and $v_i = 0$, the weight also drops by 1, in all other cases, either there is no change (when the coefficients of u is zero), or the weight drops by 1.

Exercise 27.

1. Construct an extended binary Hamming code of length 8.
2. Show that the binary Reed-Muller code $\mathcal{R}(1, 3)$ is equivalent to the extended binary Hamming of length 8.

Solution 27. To construct an extended binary Hamming code of length 8, we start with a Hamming code of length 7. So we start with a parity check matrix (in systematic form or not):

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

and we compute the parity check matrix of the extended code:

$$\hat{H} = \left[\begin{array}{ccccccc|c} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \end{array}\right].$$

The code $\mathcal{R}(1, 3)$ has for generator matrix:

$$\left[\begin{array}{cccc|cccc} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ \hline 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right].$$

We add row 3 and 4 to row 1, and permute column 4 and 5:

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

The corresponding parity check matrix is:

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

To see whether we get $\hat{H}$, we sum row 1,2 and 3 and add the result to row 4:

$$\left[\begin{array}{cccccccc} 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ \hline 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}\right]$$

and we notice that above the row of ones, we get as columns every possible binary representation between 0 and 7.

Exercise 28.

Let r be an integer with $0 \leq r \leq m$. Prove that

$$\mathcal{R}(i,m) \subseteq \mathcal{R}(j,m),\ 0 \leq i \leq j \leq m.$$

Solution 28. We do a proof by induction on m. If $m = 1$, we need to prove that

$$\mathcal{R}(i,1) \subseteq \mathcal{R}(j,1),\ 0 \leq i \leq j \leq 1.$$

For $j = 1$, $\mathcal{R}(1,1)$ is the whole space so $\mathcal{R}(i,1)$ is included in $\mathcal{R}(1,1)$. For $j = 0$, $i = 0$ and we have equality.

Assume by induction that $\mathcal{R}(i,m-1) \subseteq \mathcal{R}(j,m-1),\ 0 < i \leq j < m$. Then

$$\begin{aligned} \mathcal{R}(i,m) &= \{(\mathbf{u}, \mathbf{u}+\mathbf{v}),\ \mathbf{u} \in \mathcal{R}(i,m-1),\ \mathbf{v} \in \mathcal{R}(i-1,m-1)\} \\ &\subseteq \{(\mathbf{u}, \mathbf{u}+\mathbf{v}),\ \mathbf{u} \in \mathcal{R}(j,m-1),\ \mathbf{v} \in \mathcal{R}(j-1,m-1)\} \\ &= \mathcal{R}(j,m). \end{aligned}$$

This concludes the proof by induction for $0 < i$. If $i = 0$, we only need to show that the all-one vector is in $\mathcal{R}(j,m)$ for $j < m$. Inductively, we assume that the all-one vector of length 2^{m-1} is in $\mathcal{R}(j,m-1)$. Then the all-one vector of length 2^m is in $\mathcal{R}(j,m)$ as one choice for $\mathbf{u}$ is to take the all-one vector, with $\mathbf{v} = \mathbf{0}$.

Exercise 29.

Show that the covering radius of a linear $(n,k)_q$ code $\mathcal{C}$ is at most $n-k$.

Solution 29. Since $\mathcal{C}$ is a linear code, take G the generator matrix of $\mathcal{C}$ in systematic form. This shows that the first k coordinates of any codeword can be any vector in $\mathbb{F}_q^k$. An arbitrary vector in $\mathbb{F}_q^n$ will thus necessarily match a codeword on its first k coordinates, and it can differ in at most $n-k$, this means this vector is at distance at most $n-k$ from a codeword, thus the covering radius of $\mathcal{C}$ is at most $n-k$.

Exercise 30.

Is there a binary code with parameters $(5, 3, 3)$?

Solution 30. Using the Sphere Packing bound, we have that

$$B_2(5, 3) \leq 5$$

thus it is not possible to have $k = 3$, which would imply $B_2(5, 3) = 2^3 = 8$.

Exercise 31.

Are there binary Hamming codes which are MDS?

Solution 31. Given $r \geq 2$, binary Hamming codes have parameters $n = 2^r - 1$, $k = 2^r - r - 1$ and minimum Hamming distance $d = 3$. For a code to be MDS, we need $d = n - k + 1$, that is

$$3 = 2^r - 1 - (2^r - r - 1) + 1 = r + 1$$

so the only case is $r = 2$, but when $r = 2$, $k = 1$, $n = 3$ and $d = 3$ so it is a repetition code.

Exercise 32.

Find a polynomial of degree 4 which is irreducible over $\mathbb{F}_2$. List elements of the finite field $\mathbb{F}_{16}$.

Solution 32. We know there is a single polynomial of degree 2 which is irreducible over $\mathbb{F}_2$, namely X^2+X+1. We compute $(X^2+X+1)^2 = X^4+X^2+1$. Next we look for a generic polynomial of the form $X^4+p_3X^3+p_2X^2+p_1X+1$. Consider $X^4 + X^3 + 1$, evaluated in $X = 0$ and $X = 1$, the polynomial is not zero, so we cannot factor out a term of degree 1, but we cannot factor out a term of degree 2 either, so the polynomial is irreducible. We can use this polynomial to construct the finite field $\mathbb{F}_{16}$, which can be described by

$$\mathbb{F}_{16} = \{a_0 + a_1w + a_2w^2 + a_3w^3,\ a_0, a_1, a_2, a_3 \in \mathbb{F}_2\}$$

and $w^4 + w^3 + 1 = 0$.

Exercise 33. (Revision)

Consider the code $\mathcal{C}_1$ given by the following generator matrix over $\mathbb{F}_4$:

$$G_1 = \begin{bmatrix} 1 & 0 & 0 & 1 & w & w \\ 0 & 1 & 0 & w & 1 & w \\ 0 & 0 & 1 & w & w & 1 \end{bmatrix}.$$

It is called the hexacode. Consider the code $\mathcal{C}_2$ given by the following generator matrix over $\mathbb{F}_4$:

$$G_2 = \begin{bmatrix} 1 & w & 1 & 0 & 0 & w \\ 0 & 1 & w & 1 & 0 & w \\ 0 & 0 & 1 & w & 1 & w \end{bmatrix}.$$

1. Is the code $\mathcal{C}_2$ equivalent to $\mathcal{C}_1$?
2. Compute the minimum distance of the hexacode.
3. Is the hexacode MDS?

Solution 33. 1. We first put G_2 in systematic form by adding row 3 to row 1, then w times row 3 to row 2

$$\begin{bmatrix} 1 & w & 1 & 0 & 0 & w \\ 0 & 1 & w & 1 & 0 & w \\ 0 & 0 & 1 & w & 1 & w \end{bmatrix} \to \begin{bmatrix} 1 & w & 0 & w & 1 & 0 \\ 0 & 1 & 0 & w & w & 1 \\ 0 & 0 & 1 & w & 1 & w \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 0 & 1 & w & w \\ ac0 & 1 & 0 & w & w & 1 \\ 0 & 0 & 1 & w & 1 & w \end{bmatrix}$$

where the last matrix is obtained from the second matrix by adding w times row 2 to row 1. Then swapping columns 5 and 6 gives G_1 thus both codes are equivalent.

2. To compute the minimum distance of the hexacode, we could for example use the generic form of a codeword, then taking $x_1 = 1$ and $x_2 = x_3 = 0$ gives a weight of 4. We cannot get a weight of 3 since we cannot find a linear combination that cancels out two parities. Alternatively, remembering that the code is self-dual, we can look at the columns of the matrix, it has $d = 4$ linearly dependent columns, but no set of $d - 1 = 3$ linearly dependent columns.

3. To know whether the hexacode is MDS, we need to check whether $d = n - k + 1$, that is $4 = 6 - 3 + 1$. The code is thus MDS.

Exercise 34. (Revision)
Consider the linear code over $\mathbb{F}_3$ given by the generator matrix

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

1. What is the dimension of this code?
2. Give the systematic form of the generator matrix.
3. What is the minimum Hamming distance of this code?

Solution 34. 1. Since both rows of G are linearly independent (they are not multiples of each other), the dimension is $k = 2$.

2. Just subtract row 1 from row 2 to get:

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

3. Using the systematic generator matrix, a generic codeword is $(x_1, x_2, 2x_1, 2x_2)$. The minimum Hamming distance is 2. Indeed if $x_1 = 1$, $x_2 = 0$, we get $(1, 0, 2, 0)$ which has weight 2. It is not possible to have a smaller weight, to have a nonzero codeword, either x_1 or x_2 is nonzero, therefore there are at least 2 nonzero entries.

Exercise 35.

Consider the $[4, 2]$ linear code over $\mathbb{F}_3$ given by the generator matrix

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

this is the same code seen in the previous example.

1. Show using two different methods that this code is cyclic.
2. Compute the generator polynomial of this code.
3. Compute the check polynomial of this code.
4. How many cyclic codes of length $n = 4$ are there over $\mathbb{F}_3$?

Solution 35. 1. To show the code is cyclic, as a first method, we can just look at all codewords:

$$(1,0,2,0), (2,0,1,0), (1,1,2,2), (2,2,1,1), (2,1,1,2), (1,2,2,1), (0,2,0,1), (0,1,0,2), (0,0,0,0).$$

So we start with $(1, 0, 2, 0)$: $(1, 0, 2, 0) \mapsto (0, 1, 0, 2) \mapsto (2, 0, 1, 0) \mapsto (0, 2, 0, 1)$. Let us see which codewords we get like that:

$$(1,0,2,0)\checkmark, (2,0,1,0)\checkmark, (1,1,2,2), (2,2,1,1),$$

$$(2,1,1,2), (1,2,2,1), (0,2,0,1)\checkmark, (0,1,0,2)\checkmark, (0,0,0,0).$$

So next we shift $(1, 1, 2, 2)$: $(1, 1, 2, 2) \mapsto (2, 1, 1, 2) \mapsto (2, 2, 1, 1) \mapsto (1, 2, 2, 1)$. Let us see which codewords we added:

$$(1,0,2,0)\checkmark, (2,0,1,0)\checkmark, (1,1,2,2)\checkmark, (2,2,1,1)\checkmark,$$

$$(2,1,1,2)\checkmark, (1,2,2,1)\checkmark, (0,2,0,1)\checkmark, (0,1,0,2)\checkmark, (0,0,0,0).$$

So every shift of every codeword is in the codebook, therefore the code is cyclic. As second method, we could consider the generator matrix in systematic form computed in the previous exercise:

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

This matrix is obtained by a first row, and a second row which is a shift of the first row, therefore it is the generator matrix of a cyclic code.

2. To compute the generator polynomial of this code, we have also two methods. Since we have a list of codewords, we can find the monic polynomial of lowest degree: we have two polynomials of lowest degree, $(1,0,2,0) \leftrightarrow 1+2X^2$ and $(2,0,1,0) \leftrightarrow 2+X^2$, but only $2+X^2$ is monic, so it is the generator polynomial. The second method is since we have the generator matrix in systematic form, we can read the coefficients on the first line of the matrix: $1,0,2,0$. This gives the polynomial $1+2X^2$. It is not monic, so to get the monic polynomial with multiply by 2, which yields $2+X^2$ as it should be.

3. The check polynomial of this code is the polynomial $h(X)$ such that $X^4-1 = h(X)(2+X^2)$. So $h(X)$ is a polynomial of degree 2, which must be monic, so $h(X) = X^2 + h_0$. Then

$$X^4 - 1 = X^2(X^2+2) + h_0(X^2+2) = X^4 + 2X^2 + h_0X^2 + 2h_0$$

so $h_0 = -2$ and indeed $-4 \equiv -1 \pmod 3$.

4. Cyclic codes of length $n = 4$ over $\mathbb{F}_3$ have a generator polynomial which divides $X^4 - 1$. So let us have a closer look at $X^4 - 1$ to see what are all its divisors. We already know that $X^4 - 1 = (X^2-2)(X^2+2)$. Now modulo 3, we have $1^2 \equiv 1,\ 2^2 \equiv 1$, so both 1 and 2 are roots of $X^2+2 = (X-1)(X-2)$. This also shows that X^2-2 is irreducible, since no square modulo 3 is 2. Thus

$$X^4 - 1 = (X^2-2)(X-1)(X-2).$$

So now that we have all possible divisors of $X^4 - 1$, we can count cyclic codes by counting possible generator polynomials:

- Technically the constant polynomial 1 is a divisor.
- Then $X-1$ and $X-2$ for degree 1 polynomials.
- Then X^2-2 and $(X-1)(X-2)$ for degree 2 polynomials.
- Then $(X^2-2)(X-1)$ and $(X^2-2)(X-2)$ for degree 3 polynomials.
- Finally X^4-1 itself.

So there are 8 possible cyclic codes, including the two trivial ones.

Exercise 36.

Let $\mathcal{C}_1, \mathcal{C}_2$ be two cyclic codes of length n, generated by $g_1(X)$ and $g_2(X)$ respectively. Show that $\mathcal{C}_1 \cap \mathcal{C}_2$ is cyclic and find the generator polynomial of $\mathcal{C}_1 \cap \mathcal{C}_2$.

Solution 36. First $\mathcal{C}_1 \cap \mathcal{C}_2$ is a cyclic code. We have that $\mathbf{0}$ belongs to $\mathcal{C}_1 \cap \mathcal{C}_2$, also if $\mathbf{c}$,$\mathbf{c}'$ both are in $\mathcal{C}_1 \cap \mathcal{C}_2$, this means that $\mathbf{c}$,$\mathbf{c}' \in \mathcal{C}_1$, therefore so is their sum, and $\mathbf{c}$,$\mathbf{c}' \in \mathcal{C}_2$, so is their sum, therefore their sum is in $\mathcal{C}_1 \cap \mathcal{C}_2$ and the code is linear. If $\mathbf{c} \in \mathcal{C}_1 \cap \mathcal{C}_2$, then $\mathbf{c} \in \mathcal{C}_1$ and so are all its shifts, but since $\mathbf{c} \in \mathcal{C}_2$, all its shifts are also in $\mathcal{C}_2$ and thus they are in the intersection.

The generator polynomial is $lcm(g_1(X), g_2(X))$, that is we want to prove that $C_1 \cap C_2 = \{q(X)lcm(g_1(X), g_2(X)),\ \deg q(X) < n - s\}$ where s is the degree of the lcm.

Every codeword in the intersection is divisibly by both generator polynomials, and thus by the least common multiple, which shows the first inclusion.

Conversely, every multiple of the least common multiple belongs to both codes, hence to their intersection, which shows the reverse inclusion.

Exercise 37.

Find the generator matrix for the $[7, 4]$ binary cyclic code $\mathcal{C}$ with generator polynomial $X^3 + X^2 + 1$. Prove that $\mathcal{C}$ is a Hamming code.

Solution 37. A generator matrix is given by

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

In systematic form we have (add row 3 to row 1 and row 4 to row 1,2):

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

The parity check matrix is thus:

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

Since we have as columns every integer from 1 to 7 in binary representation, this is a binary Hamming code.

Exercise 38.

Consider the linear code over $\mathbb{F}_3$ given by the generator matrix

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

Compute the parity check matrix of G using two different methods.

Solution 38. The first method is as usual:

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

so from the systematic form, we get

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

We can check that

$$HG^T = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 2 & 0 \\ 0 & 2 \end{bmatrix} = \mathbf{0}.$$

For a different method, we first compute the check polynomial. A generator polynomial is given by $g(X) = 1 + 2X^2$ so the corresponding monic polynomial is $X^2 + 2 = X^2 - 1$. Thus the check polynomial is $h(X) = X^2 + 1$ since $g(X)h(X) = (X^2 - 1)(X^2 + 1) = X^4 - 1$. Finally we compute the reciprocal polynomial $h^{[-1]}(X)$: $h(X^{-1}) = X^{-2} + 1$, so we multiply by X^2 to get:

$$X^2(X^{-2} + 1) = 1 + X^2.$$

Thus H is obtained putting the coefficients of $h^{[-1]}(X)$ on the first row and the other row is obtained by a cyclic shift:

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

Exercise 39. (*)

Consider the polynomial $X^{15} - 1$ over $\mathbb{F}_2$. We have

$$\begin{aligned} X^{15} - 1 &= (X^3 + 1)(X^4 + X + 1)(X^8 + X^4 + X^2 + X + 1) \\ &= (X^3 + 1)(X^4 + X + 1)(X^4 + X^3 + 1)(X^4 + X^3 + X^2 + X + 1). \end{aligned}$$

1. Are all the four factors $(X^3 + 1)$, $(X^4 + X + 1)$, $(X^4 + X^3 + 1)$, $(X^4 + X^3 + X^2 + X + 1)$ of $X^{15} - 1$ irreducible over $\mathbb{F}_2$? Justify your answer.
2. How many cyclic codes of length $n = 15$ are there over $\mathbb{F}_2$?
3. (a) Consider the generator polynomial $g(X) = X^4 + X + 1$. What is the dimension of the binary code C of length 15 that it generates?
   (b) Compute the corresponding check polynomial.
   (c) Compute the corresponding parity check matrix.
   (d) Consider the following families of codes: MDS codes, Hamming codes, Reed-Mueller codes, Golay codes, Reed-Solomon codes. The code C is equivalent to a code in one of these families, which one? Justify your answer.

Solution 39. 1. Out of the four factors (X^3+1), (X^4+X+1), (X^4+X^3+1), $(X^4 + X^3 + X^2 + X + 1)$ of $X^{15} - 1$, one is of degree 3, and three are of degree 4. To check for linear factors, it is enough to evaluate them in $X = 0, 1$. We observe that $X^3 + 1 = 0$ when $X = 1$, thus it is not irreducible, while all other polynomials evaluated in $X = 0, 1$ give 1. For polynomials of degree 4, we also need to check that they are not a product of irreducible polynomials of degree 2. Over $\mathbb{F}_2$, we have only $X^2 + X + 1$, and $(X^2 + X + 1)^2 = X^4 + X^2 + 1$, so the three polynomials of degree 4 are irreducible.

2. The number of cyclic codes of length $n = 15$ over $\mathbb{F}_2$ is the number of divisors of $X^{15} - 1$, which can be counted using the different ways to combine irreducible factors of $X^{15} - 1$. We know from the above decomposition that there are 5 irreducible factors of $X^{15} - 1$. We could take any one of them (5 choices), or any two of them (2 choose 5 choices), or any three of them (3 choose 5 choices), or any four of them (4 choose 5 choices), or we could take either 1 or $X^{15} - 1$ itself. This gives a total of $2^5 = 32$ cyclic codes of length n over $\mathbb{F}_2$.

3. (a) Consider the generator polynomial $g(X) = X^4 + X + 1$. The dimension of the binary code C of length 15 that it generates is given by $n - \deg(g)$ that is $15 - 4 = 11$.

   (b) To get the corresponding check polynomial, we need $h(X)$ such that $g(X)h(X) = X^{15} - 1$. Using the above factorization, we have $X^{15} - 1 = (X^3 + 1)(X^4 + X + 1)(X^8 + X^4 + X^2 + X + 1)$, thus $h(X) = (X^3 + 1)(X^8 + X^4 + X^2 + X + 1)$ which is $h(X) = X^{11} + X^8 + X^7 + X^5 + X^3 + X^2 + X + 1$.

   (c) To compute the corresponding parity check matrix, we just take the coefficients in $h(X)$, starting from the highest coefficient, that is $[1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1]$ and put them, with padding, on the row of a matrix H. Then every of the 4 rows of H is obtained by a circular shift of one to the right of this row:

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

   (d) The code C is equivalent to a Hamming code, indeed, the binary integer representation of all integers from 1 to 15 is present as the columns of H.

Exercise 40.

Consider the $[7, 4]$ binary cyclic code $\mathcal{C}$ with generator polynomial $X^3 + X^2 + 1$. Give a bound on its minimum distance using the BCH bound.

Solution 40. Since $n = 7$ and $q = 2$, $C_0 = \{0\}$, then the cyclotomic coset C_1 is

$$C_1 = \{1, 2, 2^2 = 4\},\ 2^3 = 8 \equiv 1 \pmod 7.$$

Then

$$C_3 = \{3, 6, 12 \equiv 5\}$$

so we know C_s for every C_s, $0 \leq s < 7$, and each (apart C_0) has $2 = \delta - 1$ consecutive elements, so $d \geq \delta = 3$. We can also compute explicitly α such that $\alpha^7 = 1$ in $\mathbb{F}_{2^t}$ where t is the smallest positive integer such that $n | 2^t - 1$, so $t = 3$. Then choosing α such that $\alpha^3 = \alpha + 1$, we have $\alpha^6 = (\alpha + 1)^2 = \alpha^2 + 1$ so

$\alpha^9 = (\alpha+1)(\alpha^2+1) = \alpha^3+\alpha+\alpha^2+1 = \alpha^2$, and $\alpha^9+\alpha^6 = 1$ and α^3 is a root of $X^3+X^2+1=0$. We have

$$X^3+X^2+1 = (X-\alpha^3)(X-\alpha^5)(X-\alpha^6)$$

for α a primitive 7th root of unity. Thus

$$C_3 = \{3,6,5\} = \{3,3q,3q^2\} \pmod 7 = \{3,6,12\} \pmod 7.$$

The defining set is C_3, it contains $2 = \delta - 1$ consecutive elements: $\mathcal{S} = \{5,6\}$, thus $d \geq \delta = 3$ (and the minimum distance in this case happens to be 3 since it is a Hamming code as shown in a previous exercise).

Exercise 41.

Consider the polynomial $X^{13}-1$ over $\mathbb{F}_3$. We have

$$X^{13}-1 \quad = \quad (X^4+2X^3+2X^2+1)(X^3+X^2+2)(X^3+X^2+X+2)(X^3+2X^2+2X+2)$$

1. Are all the four factors $(X^4+2X^3+2X^2+1)$, (X^3+X^2+2), (X^3+X^2+X+2), (X^3+2X^2+2X+2) of $X^{13}-1$ irreducible over $\mathbb{F}_3$? Justify your answer.

2. Would your answer change if instead of $\mathbb{F}_3$, we consider the same four factors over $\mathbb{F}_4$? Justify your answer.

3. How many cyclic codes of length $n=13$ are there over $\mathbb{F}_3$?

4. (a) Consider the generator polynomial $g(X) = X^3+X^2+X+2$. What is the dimension of the ternary code C of length 13 that it generates?

   (b) Use the BCH bound to give a bound on the minimum Hamming distance of this code.

Solution 41.

1. Among the four factors $(X^4+2X^3+2X^2+1)$, (X^3+X^2+2), (X^3+X^2+X+2), (X^3+2X^2+2X+2) of $X^{13}-1$, only the first one has degree 4, and it has 1 as a root so it is reducible. All the others are irreducible over $\mathbb{F}_3$ because they never give 0 when evaluated in $0,1,2$.

2. If instead of $\mathbb{F}_3$, we consider the same four factors over $\mathbb{F}_4$, we have that 1 still is a root of the first polynomial, and 0 becomes a root of all other polynomials.

3. To count the number of cyclic codes of length $n=13$ over $\mathbb{F}_3$, we need to count the number of divisors of $X^{13}-1$. To do so, we first count the number of irreducible divisors, namely 5 by the above (we note that $(X^4+2X^3+2X^2+1) = (X-1)(X^3+2X+2)$), and we can combine them in any possible ways, that is we could take a single irreducible factor (1 choose 5), or combine two of them (2 choose 5), or combine three of them (3 choose 5), or combine four of them (4 choose 5), or take either 1 or $X^{13}-1$ for a total of 2^5.

4. (a) Given the generator polynomial $g(X) = X^3 + X^2 + X + 2$, the dimension of the ternary code C of length 13 that it generates is $n - \deg(g(X)) = 13 - 3 = 10$.

   (b) Since $n = 13$ and $q = 3$, we compute

$$C_1 = \{1, 3, 3^2 = 9, 3^3 = 27 \equiv 1 \pmod{n}\} = \{1, 3, 9\}.$$

   Then C_s is obtained by multipliying every element of C_1 by s:

$$C_2 = \{2, 6, 5\},\ C_4 = \{4, 12, 10\},\ C_7 = \{7, 8, 11\},\ C_0 = \{0\}.$$

   Now since $g(X)$ has degree 3, it corresponds to C_2 or C_7 (then both have 2 consecutive elements) or to C_1 or C_4 (then both have 1 consecutive element). In the first case, we would have $d \geq 3$, and in the second case $d \geq 2$. If we want to figure out which, we need to find a primitive 13th root of unity in $\mathbb{F}_{3^3}$. Using $X^3 + 2X + 1$ to generate this finite field, a root α is such that α^2 is a primitive 13th root. Then $(X - \alpha^2)(X - \alpha^6)(X - \alpha^{18}) = X^3 + X^2 + X + 2$ and the right coset is C_1.

Exercise 42.

Is it possible to construct a Reed-Solomon code of dimension $k = 4$ and length 7 over $\mathbb{F}_8$? If yes, construct the code, if no, explain why.

Solution 42. It is possible. Let $\alpha_0, \alpha_1, \ldots, \alpha_7$ be the 8 elements of $\mathbb{F}_8$. Then

$$\{(f(\alpha_1), \ldots, f(\alpha_7)),\ f(X) = f_0 + f_1 X + f_2 X^2 + f_3 X^3 \in \mathbb{F}_8[X]\}$$

forms a Reed-Solomon over $\mathbb{F}_8$. Since $f(X)$ has degree 3, then code has dimension 4. Since we evaluate f in 7 elements, the code has length 7.

Exercise 43. (*)

1. Construct the finite field $\mathbb{F}_9$.
2. If possible, give an example of MDS code of length 12 and rate 1/2. Justify your answer.

Solution 43.

1. To construct the finite field $\mathbb{F}_9$, we first find an irreducible polynomial over $\mathbb{F}_3$ of degree 2, say $X^2 - 2$. Since evaluated in $0, 1, 2$ it is never 0, it is irreducible. Then $\mathbb{F}_9 = \{a_0 + a_1 w,\ a_0, a_1 \in \mathbb{F}_3\}$, $w^2 = 2$.
2. To get an example of MDS code of length 12 and rate 1/2, we have $n = 12$, $k/n = k/12 = 1/2$ so $k = 6$. Then we build a Reed-Solomon code over $\mathbb{F}_q$ as long as $q \geq 12$. Then for $\alpha_1, \ldots, \alpha_{12}$ distinct elements of $\mathbb{F}_q$, the code is given by

$$\{(f(\alpha_1), \ldots, f(\alpha_{12}),\ \deg(f(X)) \leq 5, f(X) \in \mathbb{F}_q[X]\}.$$

Exercise 44.

1. Construct the finite field $\mathbb{F}_8$.
2. Over $\mathbb{F}_8$, construct a Reed-Solomon code C of maximal length and rate $1/2$.
3. What is the minimum Hamming distance of C?
4. Compute explicitly a generator matrix.

Solution 44. 1. To construct the finite field $\mathbb{F}_8$, we need an irreducible polynomial of degree 3 over $\mathbb{F}_2$, say $X^3 + X + 1$. Then

$$\mathbb{F}_8 = \{a_0 + a_1 w + a_2 w^2,\ a_0, a_1, a_2 \in \mathbb{F}_2\},\ w^3 = w + 1.$$

2. Over $\mathbb{F}_8$, to construct a Reed-Solomon code C of maximal length and rate $1/2$, we can have at most $n = 8$ (the size of the field), thus $k = 4$. Then for $\alpha_1, \ldots, \alpha_8$ 8 distinct elements of $\mathbb{F}_8$, we have

$$\{(f(\alpha_1), \ldots, f(\alpha_8),\ \deg f(X) \leq 3,\ f(X) \in \mathbb{F}_8[X]\}.$$

3. The minimum Hamming distance of C is given by the Singleton bound, namely $n - k + 1 = 8 - 4 + 1 = 5$.
4. A generator matrix is given by

$$\begin{bmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_8 \\ \alpha_1^2 & \alpha_2^2 & \ldots & \alpha_8^2 \\ \alpha_1^3 & \alpha_2^3 & \ldots & \alpha_8^3 \end{bmatrix}$$

Exercise 45.
Give an example of MDS code of length 16 and rate 1/2.

Solution 45. We need a finite field of size at least 16, we could take $\mathbb{F}_{2^4}$. To have a rate of $k/n = 1/2$, we need $k = 8$. We denote by $\alpha_1, \ldots \alpha_{16}$ the elements of $\mathbb{F}_{2^4}$. Then the Reed-Solomon code

$$\{(f(\alpha_1), \ldots, f(\alpha_{16})),\ f(X) \in \mathbb{F}_{2^4}[X],\ \deg f(X) <= 7\}$$

is an MDS code with length 16 and rate 1/2