Exercise Set 9: Solution
Quantum Computation

Exercise 1 *Let* $C = \{0000, 1111, 0011, 1100\}$.

1. *Compute the minimum distance* $d(C)$.
2. *What is the length* n *and the size* $|C|$*?*
3. *Compute the rate* $R = \frac{k}{n}$*, where* $k = \log_2 |C|$.

Solution. We compute the Hamming distances between distinct codewords:

$$d(0000, 1111) = 4, \qquad d(0000, 0011) = 2, \qquad d(0000, 1100) = 2,$$

$$d(1111, 0011) = 2, \qquad d(1111, 1100) = 2, \qquad d(0011, 1100) = 4.$$

Hence the minimum distance is

$$d(C) = 2.$$

Each codeword has length 4, so

$$n = 4.$$

Since the code contains 4 codewords, we have

$$|C| = 4.$$

Now

$$k = \log_2 |C| = \log_2 4 = 2.$$

Therefore the rate is

$$R = \frac{k}{n} = \frac{2}{4} = \frac{1}{2}.$$

■

Exercise 2 *Show the following about linear codes.*

1. *Determine whether the following set is a linear code:*

$$C = \{000, 011, 101, 110\}.$$

2. *Show that a linear code must contain the zero vector.*
3. *Prove that in a linear code, the minimum distance is equal to the minimum weight of a nonzero codeword.*

Solution.

1. To determine whether C is a linear code over $\mathbb{F}_2$, we check whether it is closed under addition.

   First, note that $000 \in C$. Next, compute some sums:

   $$011 + 101 = 110, \qquad 011 + 110 = 101, \qquad 101 + 110 = 011.$$

   Also, for every $x \in C$ we have $x + x = 000 \in C$. Hence the sum of any two codewords is again in C. Therefore C is a linear code.

2. Let C be a linear code. By definition, C is a subspace of $\mathbb{F}_2^n$ (or more generally of $\mathbb{F}_q^n$). Every vector space contains the zero vector. Equivalently, if $c \in C$, then since C is closed under scalar multiplication,

   $$0 \cdot c = 0 \in C.$$

   Thus every linear code contains the zero vector.

3. Let C be a linear code. Recall that the Hamming distance satisfies

   $$d(x, y) = w(x - y),$$

   where $w(\cdot)$ denotes the Hamming weight.

   Since C is linear, for any $x, y \in C$ we have $x - y \in C$. Hence

   $$d(C) = \min_{\substack{x,y \in C \\ x \neq y}} d(x, y) = \min_{\substack{x,y \in C \\ x \neq y}} w(x - y).$$

   Because $x \neq y$, the vector $x - y$ is nonzero. Conversely, every nonzero codeword $c \in C$ can be written as

   $$c = c - 0,$$

   and $0 \in C$ by part (2). Therefore the set of all differences $x - y$ with $x \neq y$ is exactly the set of nonzero codewords of C. It follows that

   $$d(C) = \min\{w(c) : c \in C,\ c \neq 0\}.$$

   So the minimum distance of a linear code is equal to the minimum weight of a nonzero codeword.

■

Exercise 3 *Let*

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

1. *List all codewords of the code generated by G.*
2. *What are the parameters (n, k) of this code?*

Solution. The code generated by G consists of all linear combinations of its rows over $\mathbb{F}_2$.
Let

$$g_1 = (1, 0, 1, 1), \qquad g_2 = (0, 1, 1, 0).$$

Then the possible codewords are:

$$0g_1 + 0g_2 = (0, 0, 0, 0),$$

$$1g_1 + 0g_2 = (1, 0, 1, 1),$$

$$0g_1 + 1g_2 = (0, 1, 1, 0),$$

$$1g_1 + 1g_2 = (1, 1, 0, 1).$$

Thus

$$C = \{0000,\ 1011,\ 0110,\ 1101\}.$$

The length of the code is the number of columns of G, so

$$n = 4.$$

The dimension is the number of linearly independent rows of G. The two rows are clearly independent, so

$$k = 2.$$

Hence the parameters are

$$(n, k) = (4, 2).$$

■

Exercise 4 *Let C be a code with minimum distance d. Prove that:*

1. *C can detect up to $d - 1$ errors.*
2. *C can correct up to $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors.*

Solution.

1. Suppose a codeword $c \in C$ is transmitted and the received word is

   $$r = c + e,$$

   where the error vector e has weight $w(e) \leq d - 1$.

   If the error were not detected, then r would itself be another codeword in C. Since $r \neq c$ whenever $e \neq 0$, we would then have two distinct codewords $c, r \in C$ with

   $$d(c, r) = w(r - c) = w(e) \leq d - 1.$$

   But this contradicts the definition of the minimum distance d, since distinct codewords must be at distance at least d. Therefore no nonzero error pattern of weight at most $d - 1$ can transform one codeword into another codeword. Hence C can detect up to $d - 1$ errors.

2. Let
$$t = \left\lfloor \frac{d-1}{2} \right\rfloor.$$
We show that any pattern of at most t errors can be corrected uniquely.
Assume that $c \in C$ is transmitted and that the received word is
$$r = c + e$$
with $w(e) \leq t$. Suppose there were another codeword $c' \neq c$ such that also
$$d(r, c') \leq t.$$
Then by the triangle inequality,
$$d(c, c') \leq d(c, r) + d(r, c') \leq t + t = 2t.$$
Since $t = \left\lfloor \frac{d-1}{2} \right\rfloor$, we have
$$2t \leq d - 1.$$
Thus
$$d(c, c') \leq d - 1,$$
which contradicts the fact that distinct codewords are at distance at least d.
Therefore there is at most one codeword within distance t of the received word r. So nearest-neighbor decoding recovers the transmitted codeword uniquely whenever at most t errors occur. Hence C can correct up to
$$\left\lfloor \frac{d-1}{2} \right\rfloor$$
errors.

■

Exercise 5 *Let C be a linear code with generator matrix G and parity-check matrix H.*

1. *Show that the rows of H generate a linear code $C^\perp$, called the* dual code.
2. *Prove that $C^\perp = \{x \in \mathbb{F}_2^n : x \cdot c = 0 \text{ for all } c \in C\}$.*
3. *Show that* $\dim(C) + \dim(C^\perp) = n$.

Solution. Let $C \subseteq \mathbb{F}_2^n$ be a linear code of dimension k, with generator matrix G and parity-check matrix H.

1. By definition, the rows of H span a subspace of $\mathbb{F}_2^n$. Any subspace of $\mathbb{F}_2^n$ is a linear code. We denote this row space by
$$C^\perp := \mathrm{Row}(H).$$
This is called the *dual code* of C.

2. Since H is a parity-check matrix for C, a vector $c \in \mathbb{F}_2^n$ lies in C if and only if

$$Hc^T = 0.$$

Write the rows of H as $h_1, \ldots, h_{n-k}$. Then the equation $Hc^T = 0$ means precisely that

$$h_i \cdot c = 0 \qquad \text{for all } i = 1, \ldots, n-k.$$

Thus every row of H is orthogonal to every codeword of C.

Since $C^\perp$ is generated by the rows of H, every vector $x \in C^\perp$ is a linear combination of these rows. Hence x is also orthogonal to every codeword of C. Therefore

$$C^\perp \subseteq \{x \in \mathbb{F}_2^n : x \cdot c = 0 \text{ for all } c \in C\}.$$

For the reverse inclusion, note that the set

$$\{x \in \mathbb{F}_2^n : x \cdot c = 0 \text{ for all } c \in C\}$$

is exactly the orthogonal complement of C in $\mathbb{F}_2^n$. The rows of H form a basis of this orthogonal complement, because H has rank $n-k$ and its rows are orthogonal to C. Hence every vector orthogonal to all codewords lies in the row space of H. So

$$\{x \in \mathbb{F}_2^n : x \cdot c = 0 \text{ for all } c \in C\} \subseteq C^\perp.$$

Combining the two inclusions, we obtain

$$C^\perp = \{x \in \mathbb{F}_2^n : x \cdot c = 0 \text{ for all } c \in C\}.$$

3. If C has dimension k, then a parity-check matrix H has rank $n-k$. Since $C^\perp$ is the row space of H, we get

$$\dim(C^\perp) = n - k.$$

Therefore

$$\dim(C) + \dim(C^\perp) = k + (n-k) = n.$$

This proves the dimension formula.

■