8

Other aspects of coding theory

We end this introduction to coding and information theory by giving two examples of how coding theory relates to quite unexpected other fields. Firstly we give a very brief introduction to the relation between Hamming codes and projective geometry. Secondly we show a very interesting application of coding to game theory.

8.1 Hamming code and projective geometry

Though not entirely correct, the concept of projective geometry was first developed by Gerard Desargues in the sixteenth century for art paintings and for architectural drawings. The actual development of this theory dated way back to the third century to Pappus of Alexandria. They were all puzzled by the axioms of Euclidean geometry given by Euclid in 300 BC who stated the following.

(1) Given any distinct two points in space, there is a unique line connecting these two points.
(2) Given any two nonparallel[1] lines in space, they intersect at a unique point.
(3) Given any two distinct parallel lines in space, they never intersect.

The confusion comes from the third statement, in particular from the concept of parallelism. How can two lines never intersect? Even to the end of universe?

[1] Note that in some Euclidean spaces we have three ways of how two lines can be arranged: they can intersect, they can be skew, or they can be parallel. For both skew and parallel lines, the lines never intersect, but in the latter situation we additionally have that they maintain a constant separation between points closest to each other on the two lines. However, the distinction between skew and parallel relies on the definition of a norm. If such a norm is not defined, "distance" is not properly defined either and, therefore, we cannot distinguish between skew and parallel. We then simply call both types to be "parallel."

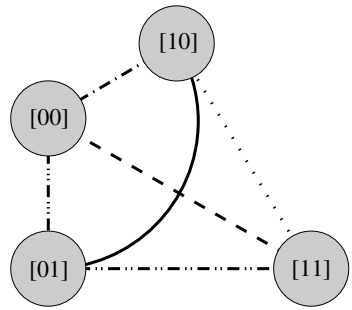

Figure 8.1 Two-dimensional binary Euclidean space.

In your daily life, the two sides of a road are parallel to each other, yet you do see them intersect at a distant point. So, this is somewhat confusing and makes people very uncomfortable. Revising the above statements gives rise to the theory of projective geometry.

Definition 8.1 (Axioms of projective geometry)

(1) Given any two distinct points in space, there is a unique line connecting these two points.
(2) Given any two distinct lines in space, these two lines intersect at a unique point.

So, all lines intersect with each other in projective geometry. For parallel lines, they will intersect at *a point at infinity.* Sounds quite logical, doesn't it? Having solved our worries, let us now focus on what the projective geometry looks like. We will be particularly working over the binary space.

Consider a two-dimensional binary Euclidean space[2] as shown in Figure 8.1. Do not worry about the fact that one line is curved and is not a straight line. We did this on purpose, and the reason will become clear later. Here we have four points, and, by the first axiom in Euclidean geometry, there can be at most $\binom{4}{2} = 6$ lines.

Exercise 8.2 *Ask yourself: why* at most *six? Can there be fewer than six lines given four points in space?* ◊

We use $[XY]$ to denote the four points in space. Consider, for example, the dash–single-dotted line $\overline{[00][10]}$ and the dash–double-dotted line $\overline{[01][11]}$. The

[2] Note that, as mentioned in Section 3.3.2, the Euclidean distance fails to work in the binary Euclidean space.

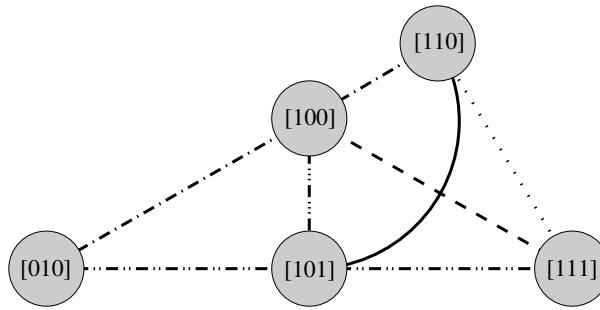

Figure 8.2 Two-dimensional binary Euclidean space with a point at infinity.

dash–single-dotted line $\overline{[00][10]}$ represents the line $Y = 0$ and the dash–double-dotted line $\overline{[01][11]}$ is the line of $Y = 1$. In Euclidean geometry, these two lines never intersect, hence it worries people. Now we introduce the concept of a "point at infinity" and make these two lines intersect as shown in Figure 8.2.

To distinguish the points at infinity from the original points, we add another coordinate Z in front of the coordinates $[XY]$. The points in the new plots are read as $[ZXY]$. The points with coordinates $[1XY]$ are the original points and the ones with $[0XY]$ are the ones at infinity. But why do we label this new point at infinity with coordinate $[010]$ and not something else? This is because points lying on the same line are *co-linear*:

$$[101] + [111] = [010], \tag{8.1}$$

i.e. we simply add the coordinates. Note that the same holds for $[100] + [110] = [010]$. Having the same result for these two sums means that the lines of $\overline{[100][110]}$ and $\overline{[101][111]}$ intersect at the same point, $[010]$.

Repeating the above process gives the geometry shown in Figure 8.3. Finally, noting that the points at infinity satisfy

$$[001] + [011] = [010], \tag{8.2}$$

we see that these three newly added points are co-linear as well. So we can add another line connecting these three points and obtain the final geometry given in Figure 8.4. This is the famous Fano plane for the two-dimensional projective binary plane. There are seven lines and seven points in this plane.

Note that the number of lines and the number of points in the projective geometry are the same, and this is no coincidence. Recall the original definition of projective geometry.

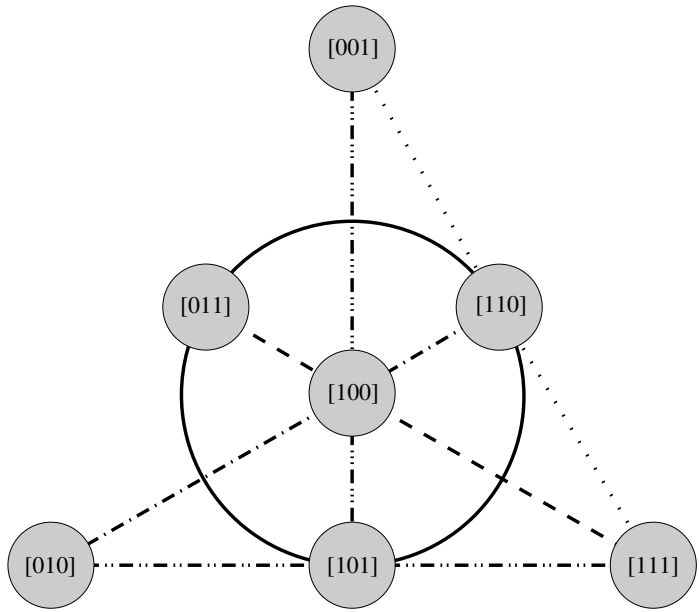

Figure 8.3 Two-dimensional binary Euclidean space with many points at infinity.

(1) Given any two distinct points in space, a unique line lies on these two points.
(2) Given any two distinct lines in space, a unique point lies on these two lines.

For the moment, forget about the literal meanings of "lines" and "points." Rewrite the above as follows.

(1) Given any two distinct □ in space, a unique ◯ lies on these two □.
(2) Given any two distinct ◯ in space, a unique □ lies on these two ◯.

So you see a symmetry between these two definitions, and this means the □s (lines) are just like the ◯s (points) and vice versa. In other words, if we label the points and lines as in Figure 8.5, we immediately discover the symmetry between the two. We only rename the L by P and the P by L in Figure 8.5(a) and Figure 8.5(b). In particular, the patterns of the lines in Figure 8.5(a) are matched to the patterns of the points in Figure 8.5(b) to signify such a duality.

To understand more about the symmetry, consider for example the following.

• Point P_1 is intersected by lines L_2, L_3, and L_5 in Figure 8.5(a). In Fig-

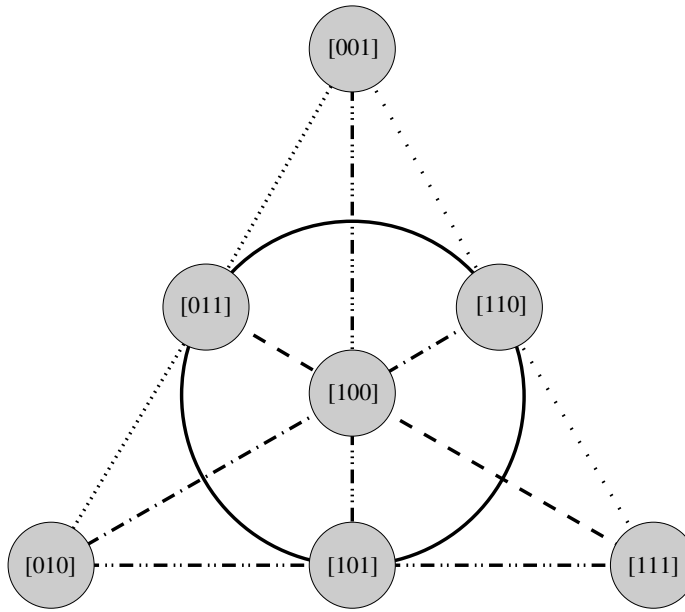

Figure 8.4 Final projective geometry of the two-dimensional binary Euclidean space with points at infinity.

ure 8.5(b), we see exactly the same relation between the lines L_3, L_5, and L_2 and the point P_1.

- Line L_1 is related to points P_2, P_3, and P_5 in Figure 8.5(b). In Figure 8.5(a), we see that L_1 passes through all these three points.

Also note that, in terms of the $[ZXY]$ axes, the lines are defined by the following functions:

$$\begin{aligned} L_1 &: \quad Z = 0, \\ L_2 &: \quad X = 0, \\ L_3 &: \quad Y = 0, \\ L_4 &: \quad Z + X = 0, \\ L_5 &: \quad X + Y = 0, \\ L_6 &: \quad Z + X + Y = 0, \\ L_7 &: \quad Z + Y = 0. \end{aligned} \tag{8.3}$$

Note that the above is quite different from what you learned in high school mathematics. For example, the function $Z = 0$ does not give a plane in projective geometry as it does in Euclidean geometry.

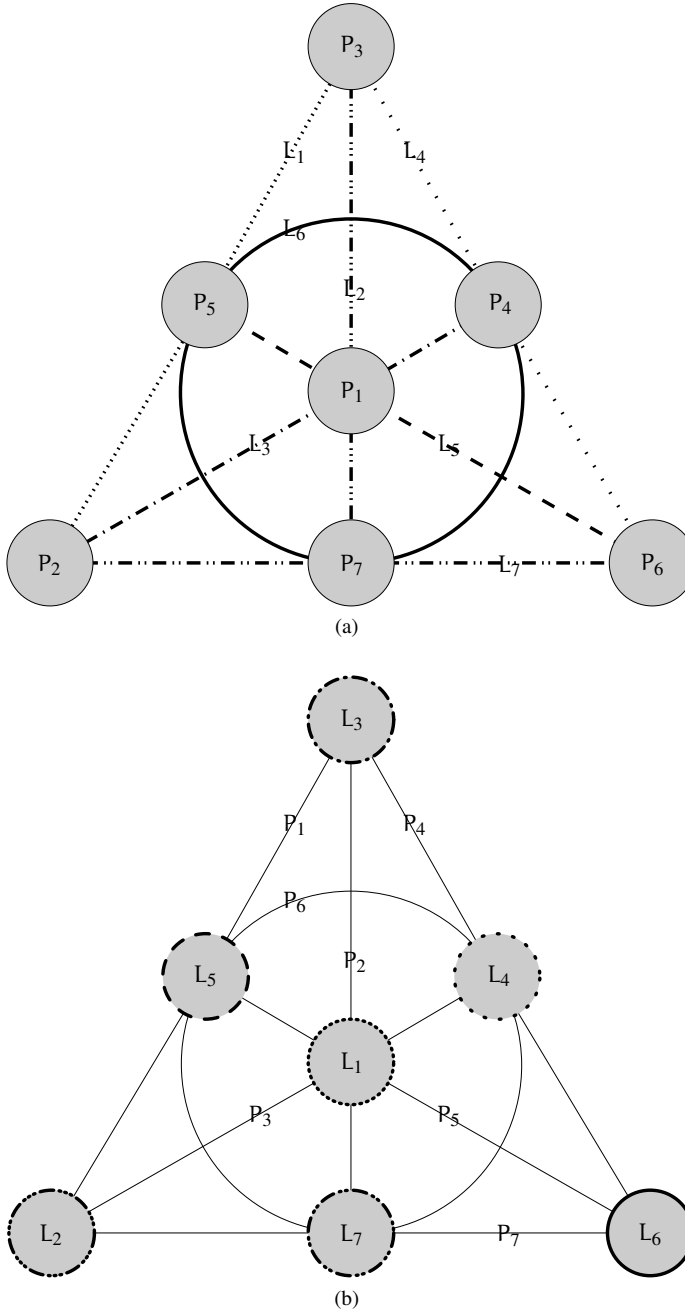

Figure 8.5 Symmetry between two definitions of projective geometry.

In general, the connection between lines in the two-dimensional Euclidean plane and the lines in the two-dimensional projective plane can be easily obtained through the following. For simplicity, let $\mathcal{E}_2$ denote the two-dimensional binary Euclidean plane, and let $\mathcal{P}_2$ denote the two-dimensional binary projective plane. Then the connection between lines in $\mathcal{E}_2$ and $\mathcal{P}_2$ is given by

$$\mathrm{L} : aX + bY + c = 0 \text{ in } \mathcal{E}_2 \quad \Longleftrightarrow \quad \mathrm{L} : aX + bY + cZ = 0 \text{ in } \mathcal{P}_2, \tag{8.4}$$

where not all a, b, and c equal zero.

Example 8.3 We now apply (8.4) in order to study a solid example so that we can understand more about the two geometries from the algebraic point of view. Consider, for example, lines L_3 and L_7, which represent the functions $Y = 0$ and $Y = 1$ in $\mathcal{E}_2$, respectively. Of course, L_3 and L_7 are parallel in $\mathcal{E}_2$ and do not intersect. On the other hand, lifting these two functions from $\mathcal{E}_2$ to $\mathcal{P}_2$ (by setting $(a,b,c) = (0\,1\,0)$ and $(0\,1\,1)$ in (8.4)) gives $Y = 0$ and $Y + Z = 0$, respectively. It then follows that these two functions do intersect in $\mathcal{P}_2$ at $[ZXY] = [010]$, a point satisfying these two equations. It justifies the fact that any two distinct lines always intersect with each other. An equivalent view from algebra says that every system of linear equations is always solvable in the projective sense. ◊

To relate the Fano plane to the Hamming code, we simply construct Table 8.1. A "1" means the point lies on the line, or, equivalently, that the line passes through the point.

Table 8.1 *Relation of Fano plane to Hamming code*

	P_1	P_2	P_3	P_4	P_5	P_6	P_7
L_1	0	1	1	0	1	0	0
L_2	1	0	1	0	0	0	1
L_3	1	1	0	1	0	0	0
L_4	0	0	1	1	0	1	0
L_5	1	0	0	0	1	1	0
L_6	0	0	0	1	1	0	1
L_7	0	1	0	0	0	1	1

On reading Table 8.1 row-wise and comparing these rows with codewords in Table 3.2, we see that

- line L_1 defines the codeword $(0\,1\,1\,0\,1\,0\,0)$ associated with message $(0\,1\,0\,0)$,

- line L_2 defines the codeword (1010001) associated with message (0001),
- line L_3 defines the codeword (1101000) associated with message (1000),
- line L_4 defines the codeword (0011010) associated with message (1010),
- line L_5 defines the codeword (1000110) associated with message (0110),
- line L_6 defines the codeword (0001101) associated with message (1101),
- line L_7 defines the codeword (0100011) associated with message (0011).

So, the seven lines define seven codewords of a $(7,4)$ Hamming code. What about the remaining $16-7=9$ codewords? Well, if we add an empty line, L_0, to define the codeword (00000000), then the remaining eight codewords are just the binary complement of these eight codewords. For example, the binary complement of (00000000) is (11111111), and the binary complement of (0110100) defined by L_1 is (1001011) (simply replace 0 by 1 and 1 by 0). This way you recover all the 16 codewords of the $(7,4)$ Hamming code.

While all the above seems tricky and was purposely done, it presents a means of generalization of the Hamming code. In particular, extending the two-dimensional Fano plane to higher-dimensional binary projective spaces, say $(u-1)$ dimensions,

(1) we could construct the $(2^u-1, 2^u-u-1)$ Hamming codes defined by the lines in the $(u-1)$-dimensional binary projective space,[3] and
(2) we could construct other codes defined by the s-dimensional subspaces (called s-flats or s-hyperplanes in finite geometry) in the $(u-1)$-dimensional binary projective space. These codes are therefore coined *projective geometry codes*.

Exercise 8.4 *Identify all the 16 Hamming codewords on the Fano plane plus an empty line. The points associated with each codeword form either a line or a complement of a line. Can you use this geometrical fact to decode read-outs with one-bit error? We can give you some hints for this.*

(1) Read-outs with only one nonzero position are decoded to the empty line.
(2) Read-outs with two nonzero positions are decoded to a line. Two nonzero positions mean two points in the Fano plane. The line obtained by joining these two points gives the decoded codeword. For example, if the nonzero positions are P_2 and P_4, then they form the line L_3, and the corrected output should be the codeword associated with L_3.
(3) Read-outs with three nonzero positions correspond to either a line or a triangle in the Fano plane. If it is a line, then the line gives the decoded codeword. Otherwise, the triangle can be made into a quadrangle by adding an

[3] An alternative way of getting this is given in Exercise 3.22.

extra point. Then note that the quadrangle is a complement of a line, which is a codeword. So the codeword associated with this quadrangle is the decoded output. For example, assume the nonzero positions of the read-out are P_1, P_2, *and* P_3, *which form a triangle. To make the triangle into a quadrangle, we should add point* P_6 *(note that adding either* P_4, P_5, *or* P_7 *would not work: it would still be a triangle). Then the quadrangle* $P_1P_2P_3P_6$ *is the complement of the projective line* L_6, *and hence it corresponds to a valid codeword.*

Complete the decodings of read-outs with more than three nonzero positions. ◊

8.2 Coding and game theory

The Hamming code can be used to solve many problems in combinatorial designs as well as in game theory. One of the most famous and most interesting problems is the *hat game*. On April 10, 2001, the New York Times published an article entitled "Why mathematicians now care about their hat color." The game has the following setup.

- A team of n players enters a room, whereupon they each receive a hat with a color randomly selected from r equally probable possibilities. Each player can see everyone else's hat, but not his own.
- The players must simultaneously guess the color of their own hat, or pass.
- The team loses if any player guesses wrong or if all players pass.
- The players can meet beforehand to devise a strategy, but no communication is allowed once they are inside the room.
- The goal is to devise a strategy that gives the highest probability of winning.

Example 8.5 Let $n = 3$ and $r = 2$ with the colors Red and Blue. Let us number the three players by 1, 2, and 3, and denote their hats by H_1, H_2, and H_3, respectively. If the three players receive $(H_1, H_2, H_3) = (\text{Red}, \text{Red}, \text{Blue})$ and they guess $(\text{Red}, \text{Pass}, \text{Pass})$, then they win the game. Otherwise, for example, if they guess $(\text{Pass}, \text{Blue}, \text{Blue})$, then they lose the game due to the wrong guess of the second player. They also lose for the guess of $(\text{Pass}, \text{Pass}, \text{Pass})$. ◊

Random strategy What if the players guess at random? Say, guessing with probability $1/(r+1)$ for each color and probability $1/(r+1)$ for pass. With this random strategy, the probability of winning is given by

$$\Pr(\text{Win by using "random strategy"}) = \left(\frac{2}{r+1}\right)^n - \frac{1}{(r+1)^n}. \tag{8.5}$$

So, in Example 8.5 the random strategy will yield a probability of winning

$$\Pr(\text{Win by using "random strategy"}) = \frac{7}{27} \simeq 26\%, \tag{8.6}$$

i.e. the odds are not good.

Exercise 8.6 *Prove (8.5).*

Hint: the first term of (8.5) describes the probability of the correct color or a pass and that the second term is the probability of all passing. ◊

One-player-guess strategy Another simple strategy is to let only one of the players, say the first player, guess and let the others always pass. It is clear that if the first player passes, then the team loses. So he must make a choice. In this case, the probability of winning the game is given by

$$\Pr(\text{Win by using "one-player-guess strategy"}) = \frac{1}{r}, \tag{8.7}$$

i.e. for Example 8.5 ($r = 2$)

$$\Pr(\text{Win by using "one-player-guess strategy"}) = \frac{1}{2} = 50\%, \tag{8.8}$$

and the first player simply guesses the color to be either Red or Blue, each with probability $1/2$. This strategy is a lot better than the random guess strategy. Now the question is, can we do better than $1/2$? Actually we can, with the help of the three-times repetition code and the Hamming code we learned in Chapter 3.

Repetition code strategy For simplicity, let us focus on the case of $n = 3$ and $r = 2$ with colors being Red (denoted as binary 0) and Blue (denoted as binary 1). Recall that the three-times repetition code $\mathscr{C}_{\text{rep}}$ has two codewords $(0\,0\,0)$ and $(1\,1\,1)$. Using the repetition code, we formulate the following strategy.

- For the first player, let $(?, H_2, H_3)$ be a vector where $H_2, H_3 \in \{0,1\}$ are the hat colors of the second and the third players, respectively. The question mark symbol "?" means that the color of the hat is unknown. The colors H_2 and H_3 are known to the first player according to the setup. Then the first player makes a guess using the following rule:

$$? = \begin{cases} 0 & \text{if } (1, H_2, H_3) \text{ is a codeword in } \mathscr{C}_{\text{rep}}, \\ 1 & \text{if } (0, H_2, H_3) \text{ is a codeword in } \mathscr{C}_{\text{rep}}, \\ \text{pass} & \text{otherwise.} \end{cases} \tag{8.9}$$

- The same applies to the second and the third players. For example, the strategy of the second player is

$$? = \begin{cases} 0 & \text{if } (H_1, 1, H_3) \text{ is a codeword in } \mathscr{C}_{\text{rep}}, \\ 1 & \text{if } (H_1, 0, H_3) \text{ is a codeword in } \mathscr{C}_{\text{rep}}, \\ \text{pass} & \text{otherwise}, \end{cases} \tag{8.10}$$

  where H_1 is the color of the first player's hat known to the second player.

Example 8.7 (Continuation from Example 8.5) If the three players receive $(H_1, H_2, H_3) = (\text{Red}, \text{Red}, \text{Blue}) = (0\,0\,1)$, then

- the first player sees $(?\,0\,1)$, and neither $(0\,0\,1)$ nor $(1\,0\,1)$ is a codeword in $\mathscr{C}_{\text{rep}}$, so he passes;
- the second player sees $(0\,?\,1)$, and neither $(0\,0\,1)$ nor $(0\,1\,1)$ is a codeword in $\mathscr{C}_{\text{rep}}$, so he passes, too;
- the third player sees $(0\,0\,?)$. He notices that $(0\,0\,0)$ is a codeword in $\mathscr{C}_{\text{rep}}$, so he guesses 1.

Hence, the team wins. ◊

Exercise 8.8 *Show by listing all possibilities that the three-times repetition code strategy gives a probability of winning*

$$\Pr\big(\text{Win by using ``}\mathscr{C}_{\text{rep}}\text{ code strategy''}\big) = \frac{3}{4} \tag{8.11}$$

when $n = 3$ *and* $r = 2$. ◊

It turns out that for $n = 3$ and $r = 2$, the three-times repetition code $\mathscr{C}_{\text{rep}}$ is the best possible strategy for this game. Also, by carrying out Exercise 8.8 you will see that the only cases for the $\mathscr{C}_{\text{rep}}$ strategy to fail are the ones when the players are given hats as $(0\,0\,0)$ and $(1\,1\,1)$, which are exactly the two codewords in $\mathscr{C}_{\text{rep}}$.

$(7,4)$ **Hamming code strategy** The $(7,4)$ Hamming code strategy is the best strategy when $n = 7$ and $r = 2$. But, prior to handing over the strategy, we quickly review what happened in the three-times repetition code case. In the previous example of $n = 3$ and $r = 2$, the ith player, given the observation $(H_1, \ldots, H_{i-1}, ?, H_{i+1}, \ldots, H_3)$, makes the following guess:

$$? = \begin{cases} 0 & \text{if } (H_1, \ldots, H_{i-1}, 1, H_{i+1}, \ldots, H_3) \text{ is a codeword in } \mathscr{C}_{\text{rep}}, \\ 1 & \text{if } (H_1, \ldots, H_{i-1}, 0, H_{i+1}, \ldots, H_3) \text{ is a codeword in } \mathscr{C}_{\text{rep}}, \\ \text{pass} & \text{otherwise.} \end{cases} \tag{8.12}$$

So, for the case of $n = 7$ and $r = 2$, let $\mathscr{C}_{\mathrm{H}}$ be the $(7,4)$ Hamming code with 16 codewords given in Table 3.2. Then we use the following similar strategy.

- The ith player, given the observation $(H_1, \ldots, H_{i-1}, ?, H_{i+1}, \ldots, H_7)$, makes the following guess:

$$? = \begin{cases} 0 & \text{if } (H_1, \ldots, H_{i-1}, 1, H_{i+1}, \ldots, H_7) \text{ is a codeword in } \mathscr{C}_{\mathrm{H}}, \\ 1 & \text{if } (H_1, \ldots, H_{i-1}, 0, H_{i+1}, \ldots, H_7) \text{ is a codeword in } \mathscr{C}_{\mathrm{H}}, \\ \text{pass} & \text{otherwise.} \end{cases} \tag{8.13}$$

Example 8.9 For example, the seven players are given hats according to

$$(\text{Blue}, \text{Red}, \text{Blue}, \text{Red}, \text{Blue}, \text{Blue}, \text{Blue}) = (1\,0\,1\,0\,1\,1\,1). \tag{8.14}$$

Based on the strategy in (8.13) and the codewords of $\mathscr{C}_{\mathrm{H}}$ in Table 3.2, the players make the following guesses.

- The first player observes $(?\,0\,1\,0\,1\,1\,1)$ and notices that $(0\,0\,1\,0\,1\,1\,1)$ is a codeword. So he guesses 1, i.e. Blue.
- The second player observes $(1\,?\,1\,0\,1\,1\,1)$ and notices that neither $(1\,0\,1\,0\,1\,1\,1)$ nor $(1\,1\,1\,0\,1\,1\,1)$ are codewords. So he passes.
- You can check the remaining cases and show that they all pass.

Since the first player makes the right guess and the others pass, the team wins. ◊

We can show the following theorem.

Theorem 8.10 *For the case of $n = 7$ and $r = 2$, the $(7,4)$ Hamming code strategy given as in (8.13) yields the probability of winning*

$$\Pr(\text{Win by using "}\mathscr{C}_{\mathrm{H}}\text{ code strategy"}) = 1 - \frac{16}{2^7} = \frac{7}{8}. \tag{8.15}$$

Proof Note that from the sphere bound of Theorems 3.20 and 3.21, we see that the $(7,4)$ Hamming code $\mathscr{C}_{\mathrm{H}}$ is a perfect packing of 16 spheres of radius 1 in the seven-dimensional binary space. Hence, given any combination of hats $\mathbf{H} = (H_1, H_2, \ldots, H_7)$, $\mathbf{H}$ must lie in one of the 16 spheres. In other words, there must exist a codeword $\mathbf{x} = (x_1, \ldots, x_7)$ of $\mathscr{C}_{\mathrm{H}}$ that is at Hamming distance at most 1 from $\mathbf{H}$. We distinguish the following cases.

Case I: If $\mathbf{H} \in \mathscr{C}_{\mathrm{H}}$, then according to the strategy (8.13), the ℓth player for every $1 \le \ell \le 7$ would notice that $(H_1, \ldots, H_{\ell-1}, x_\ell, H_{\ell+1}, \ldots, H_7)$ is a codeword in $\mathscr{C}_{\mathrm{H}}$, hence he will guess $\bar{x}_\ell$, the binary complement of x_ℓ. The team always loses in this case.

Case II: If $\mathbf{H} \notin \mathscr{C}_{\mathrm{H}}$, then $\mathbf{H}$ is at Hamming distance 1 from some codeword $\mathbf{x}$. Say the difference is at the jth place, for some j, i.e. the hat color H_j of the jth player equals $\bar{x}_j$.

- For the ℓth player, $\ell \neq j$, we see from strategy (8.13) that $(H_1, \ldots, H_{\ell-1}, x_\ell, H_{\ell+1}, \ldots, H_7)$ is at Hamming distance 1 from $\mathbf{x}$ and $(H_1, \ldots, H_{\ell-1}, \bar{x}_\ell, H_{\ell+1}, \ldots, H_7)$ is at Hamming distance 2 from $\mathbf{x}$. Both cannot be codewords because the codewords of Hamming code are separated by a distance of at least 3. Thus, the ℓth player always passes in this case.
- The jth player observes that $(H_1, \ldots, H_{j-1}, x_j, H_{j+1}, \ldots, H_7) = \mathbf{x}$ is a codeword, hence he guesses $\bar{x}_j$, which is the correct guess.

Thus, the team wins.

From the above analysis we see that the team loses if, and only if, $\mathbf{H}$ is a codeword in $\mathscr{C}_{\mathrm{H}}$. Since there are 16 such possibilities, we conclude that

$$\Pr(\text{Lose by using "}\mathscr{C}_{\mathrm{H}}\text{ code strategy"}) = \frac{16}{2^7} \tag{8.16}$$

and the theorem is proven. □

The strategy we have devised above is related to the *covering* of error-correcting codes. The concept of covering is the opposite of that of sphere packing: the problem of covering asks what the minimum number of t is such that the radius-t spheres centered at the 2^k codewords of a code fill up the complete n-dimensional binary space. Here the spheres are allowed to overlap with each other. The three-times repetition code $\mathscr{C}_{\mathrm{rep}}$ and the Hamming code $\mathscr{C}_{\mathrm{H}}$ are both 1-covering codes because radius-1 spheres centered at their codewords completely cover the three-dimensional and seven-dimensional binary space, respectively.

In general, we can show the following theorem.

Theorem 8.11 *Let $\mathscr{C}$ be a length-n 1-covering error-correcting code with $|\mathscr{C}|$ codewords. Then for the hat game with n players and $r = 2$ colors, following the strategy defined by $\mathscr{C}$ as in (8.13), yields a winning probability of*

$$\Pr(\text{Win by using "}\mathscr{C}\text{ code strategy"}) = 1 - \frac{|\mathscr{C}|}{2^n}. \tag{8.17}$$

Exercise 8.12 *Prove Theorem 8.11 by showing that (Case I) if $\mathbf{H} \in \mathscr{C}$, the team always loses, and (Case II) if $\mathbf{H} \notin \mathscr{C}$, the team always wins even if the codewords of the 1-covering code are not separated by a distance of at least 3.*

Hint: $(H_1, \ldots, H_{\ell-1}, \bar{x}_\ell, H_{\ell+1}, \ldots, H_n)$ could be a codeword. ◊

Finally we remark that both $\mathscr{C}_{\text{rep}}$ and $\mathscr{C}_{\text{H}}$ are optimal 1-covering codes because they have the smallest possible code size among all 1-covering codes of length 3 and length 7, respectively. The fact that the three-times repetition code $\mathscr{C}_{\text{rep}}$ is an optimal length-3 1-covering code follows from the third case in Theorem 3.21 with $u = 1$.

8.3 Further reading

In this chapter we have briefly discussed two different aspects of coding theory. Using the $(7,4)$ Hamming code as a starting example, we have shown how the error-correcting codes can be used in the study of finite geometry as well as game theory. To encourage further investigations in this direction, we provide a short list of other research fields that are closely related to coding theory.

Cryptography One aim in cryptography is message encryption so that eavesdroppers cannot learn the true meaning of an encrypted message. The encryption device has a key, which is known to the sender and the recipient, but not to the eavesdropper. Given the key $\mathbf{K}$, the encryption device encrypts plaintext $\mathbf{S}$ into ciphertext $\mathbf{C}$. It is hoped that without the key the eavesdropper cannot easily recover the plaintext $\mathbf{S}$ from $\mathbf{C}$. In 1949 Shannon [Sha49] first applied information theory to the study of cryptography and defined the notion of *perfect secrecy*. We say that the communication is perfectly secure if the mutual information between $\mathbf{S}$ and $\mathbf{C}$ is zero, i.e. $I(\mathbf{S};\mathbf{C}) = 0$. Noting that

$$I(\mathbf{S};\mathbf{C}) = H(\mathbf{S}) - H(\mathbf{S}|\mathbf{C}), \tag{8.18}$$

a perfectly secure communication means that the eavesdropper can never learn *any* information about $\mathbf{S}$ from the observation of $\mathbf{C}$. While none of the currently used cryptosystems can offer such perfect secrecy, in 1978 Robert J. McEliece proposed a highly secure cryptosystem based on the use of (n,k) binary linear error-correcting codes. McEliece's cryptosystem with large n is immune to all known attacks, including those made by quantum computers. Readers interested in this line of research are referred to [McE78] and [Sti05] for further reading.

Design of pseudo-random sequences The pseudo-random number generator is perhaps one of the most important devices in modern computing. A possible implementation of such a device is through the use

of *maximum-length sequences*, also known as *m-sequences*. The m-sequence is a binary pseudo-random sequence in which the binary values 0 and 1 appear almost statistically independent, each with probability $1/2$. Given the initial seed, the m-sequence can be easily generated by feedback shift registers. It is also one of the key components in modern cellular communication systems that are built upon code-division multiple-access (CDMA) technology. The m-sequence and the Hamming code are closely connected. In fact, the m-sequence is always a codeword in the dual of the Hamming code. Readers are referred to [McE87] and [Gol82] for more details about this connection and about the design of pseudo-random sequences.

Latin square and Sudoku puzzle The Latin square is a special kind of combinatorial object which many people have seen in some mathematical puzzles. Specifically, a Latin square is an $(n \times n)$ array in which each row and each column consist of the same set of elements without repetition. For example, the following is a (3×3) Latin square.

$$\begin{bmatrix} 3 & 1 & 2 \\ 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} \tag{8.19}$$

The famous game of Sudoku can also be regarded as a special kind of (9×9) Latin square. Sudoku puzzles are probably the most popular among all Latin squares. Another interesting extension is called the *orthogonal array*, which has very useful applications in software testing. Two $(n \times n)$ Latin squares A and B are said to be orthogonal if all the n^2 pairs $([\mathsf{A}]_{i,j}, [\mathsf{B}]_{i,j})$ are distinct. For example, the following (4×4) Latin squares are orthogonal to each other:

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \\ 1 & 2 & 3 & 4 \end{bmatrix}. \tag{8.20}$$

While there are many ways to construct mutually orthogonal arrays, one of the most notable constructions is from the finite projective plane we studied in Section 8.1. A famous theorem in this area states that there exists $(n-1)$ mutually orthogonal $(n \times n)$ Latin squares if, and only if, there exists a finite projective plane in which every projective line has $(n-1)$ points. Again, the finite projective planes are tied

closely to the Hamming codes. Please refer to [Bry92] and [vLW01] for a deeper discussion.

Balanced incomplete block designs The problem with block design is as follows: v players form t teams with m members in each team. Two conditions are required: (a) each player is in precisely μ teams, and (b) every pair of players is in precisely λ teams. Configurations meeting the above requirements are termed (v,t,μ,m,λ) *block designs*. It should be noted that these parameters are not all independent. The main challenge is, given a set of parameters, to find out whether the design exists, and, if the answer is yes, how to construct it. For many parameters these questions are still unanswered. The (v,t,μ,m,λ) block designs have many applications to experimental designs, cryptography, and optical fiber communications. Moreover, block designs can be transformed into a class of error-correcting codes, termed *constant-weight codes*. Certain block-designs with $\lambda = 1$ can be obtained from finite projective planes. For more details please refer to [HP03].

References

[Bry92] Victor Bryant, *Aspects of Combinatorics: A Wide-Ranging Introduction*. Cambridge University Press, Cambridge, 1992.

[Gol82] Solomon W. Golomb, *Shift Register Sequences*, 2nd edn. Aegean Park Press, Laguna Hills, CA, 1982.

[HP03] W. Cary Huffman and Vera Pless, eds., *Fundamentals of Error-Correcting Codes*. Cambridge University Press, Cambridge, 2003.

[McE78] Robert J. McEliece, "A public-key cryptosystem based on algebraic coding theory," DSN Progress Report 42-44, Technical Report, January and February 1978.

[McE87] Robert J. McEliece, *Finite Field for Scientists and Engineers*, Kluwer International Series in Engineering and Computer Science. Kluwer Academic Publishers, Norwell, MA, 1987.

[Sha49] Claude E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, October 1949.

[Sti05] Douglas R. Stinson, *Cryptography: Theory and Practice*, 3rd edn. Chapman & Hall/CRC Press, Boca Raton, FL, 2005.

[vLW01] Jacobus H. van Lint and Richard M. Wilson, *A Course in Combinatorics*, 2nd edn. Cambridge University Press, Cambridge, 2001.