Chapter 2

The Main Coding Theory Problem

A code (n, M, d) has the following desirable properties:

1. small n: fast transmission;
2. large M: many messages;
3. large d: correct many errors.

These are conflicting aims. The main coding theory problem is to find codes optimising one parameter with the other two fixed.

Let $A_q(n, d)$ be the maximum value of M for which there exists a q-ary (n, M, d)-code.

Theorem 2.1.

(i) $A_q(n, 1) = q^n$.

(ii) $A_q(n, n) = q$.

Proof (i) If $d(C) = 1$, all codewords are different. So the largest code is $C = (\mathbf{F}_q)^n$ and has $M = q^n$.

(ii) Let C be a q-ary (n, M, n)-code. So all M codewords are distinct in every coordinate. Consider the first coordinate; hence $M \leq q$. The existence of a q-ary repetition code shows that $M = q$. □

Recall that

$$\begin{aligned}\binom{n}{k} &= \frac{n(n-1)(n-2)\cdots(n-k+1)}{k!} = \frac{n!}{(n-k)!\,k!} \\ &= \text{number of ways of choosing } k \text{ objects out of } n.\end{aligned}$$

Note 2.2. $0! = 1$.

Example 2.3.

$$\binom{n}{0} = 1, \quad \binom{n}{1} = n, \quad \binom{n}{2} = \tfrac{1}{2}n(n-1),$$
$$\binom{4}{2} = 6, \quad \binom{5}{2} = 10, \quad \binom{n}{k} = \binom{n}{n-k}.$$

Notation 2.4. $S(x,r)$ is the ball with centre x and radius r; that is,

$$S(x,r) = \{y \in (\mathbf{F}_q)^n \mid d(x,y) \leq r\}.$$

Lemma 2.5. *A ball of radius r in $(\mathbf{F}_q)^n$, $0 \leq r \leq n$, contains exactly*

$$\binom{n}{0} + \binom{n}{1}(q-1) + \cdots + \binom{n}{r}(q-1)^r$$

vectors.

Proof This is an exercise.

Hint: find the number of vectors at precisely distance $0, 1, \ldots, r$ from a vector x. □

Theorem 2.6. (The sphere packing or Hamming bound)

A q-ary $(n, M, 2e+1)$-code C satisfies

$$M\left\{\binom{n}{0} + \binom{n}{1}(q-1) + \cdots + \binom{n}{e}(q-1)^e\right\} \leq q^n.$$

Proof Consider each codeword x in C and a ball $S(x,e)$ of radius e. As in Theorem 4.19, the balls are disjoint. So we have M disjoint balls of radius e in $(\mathbf{F}_q)^n$ which has q^n elements. Hence

$$M\,|S(x,e)| \leq q^n.$$

By Lemma 2.5,

$$|S(x,e)| = \sum_{i=0}^{e} \binom{n}{i}(q-1)^i,$$

whence the result. □

Corollary 2.7. *A binary $(n, M, 2e+1)$ code satisfies*

$$M\left\{1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{e}\right\} \leq 2^n.$$

Definition 2.8. An e-error-correcting code C in $(\mathbf{F}_q)^n$ is *perfect* if any vector in $(\mathbf{F}_q)^n$ is at distance at most e from exactly one codeword; that is, every received message is corrected!

Corollary 2.9. *A q-ary $(n, M, 2e+1)$ code C is perfect if and only if equality holds in Theorem 2.6.*

Corollary 2.10. *If $d = 2e+1$,*

$$A_q(n,d) \leq q^n / \sum_{i=0}^{e} \binom{n}{i}(q-1)^i.$$

In Example 4.7, C_3 is not perfect since 11000 is at distance 2,3,3,2 from the codewords. However, {000,111} is perfect!

Definition 2.11. If a code C can correct at most e errors, then e is the *packing radius*. The packing radius of C is e if it is the largest integer such that the $S(x,e)$ are all disjoint as x varies in C.

Definition 2.12. The *covering radius* of the code C in $(\mathbf{F}_q)^n$ is the smallest integer $\rho = \rho(C)$ such that $\bigcup_{x \in C} S(x, \rho) = (\mathbf{F}_q)^n$.

Example 2.13. For $C_3 = \{00000, 01101, 10110, 11011\}$, the packing radius is $e = 1$, whereas the covering radius is $\rho = 2$. Verify this!

Example 2.14. When $C = \{0000, 1111\}$, the packing radius $e = 1$, since $d = 4$ and $e = \lfloor \frac{1}{2}(d-1) \rfloor$. The covering radius $\rho = 2$ since every 4-letter word is at distance $0, 1, 2$ from a codeword.

Theorem 2.15. *The code C is perfect if and only if $\rho = e$.*

Example 2.16. A perfect code

Projective plane $\rightarrow$ finite projective plane $\pi_q \rightarrow$ plane of order two π_2
$\rightarrow$ incidence matrix $\rightarrow$ perfect code.

This provides an example of links between coding theory and other combinatorial structures.

Definition 2.17. A *projective plane* $\pi = (\mathcal{P}, \mathcal{L})$, where $\mathcal{P}$ is a set of *points*, $\mathcal{L}$ is a set of *lines*, with each line a set of points, satisfying the following:

(i) through every two points there is a unique line;

(ii) every two lines meet in a unique point;

(iii) there exists a quadrangle; that is, a set of four points no three on a line.

Definition 2.18. The plane $\pi = \pi_q$ has *order* q if some line contains exactly $q + 1$ points.

In that case, it follows that π has

(i) $q^2 + q + 1$ points,

(ii) $q^2 + q + 1$ lines,

(iii) $q + 1$ points on a line,

(iv) $q + 1$ lines through a point.

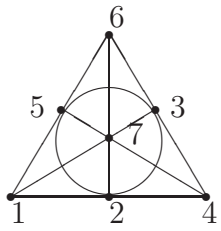
Here is the unique plane $\pi_2 = \mathrm{PG}(2, 2)$ of order 2. Its points are $P_i = i$ and its lines are $\ell_i,\ i = 1, \ldots, 7$.

The plane π_2 has an incidence matrix $A = (a_{ij})$,where

$$a_{ij} = \begin{cases} 1 & \text{if } P_j \in \ell_i, \\ 0 & \text{if } P_j \notin \ell_i. \end{cases}$$

It is

	P_1	P_2	P_3	P_4	P_5	P_6	P_7
ℓ_1	1	1	0	1	0	0	0
ℓ_2	0	1	1	0	1	0	0
ℓ_3	0	0	1	1	0	1	0
ℓ_4	0	0	0	1	1	0	1
ℓ_5	1	0	0	0	1	1	0
ℓ_6	0	1	0	0	0	1	1
ℓ_7	1	0	1	0	0	0	1



1	2	3	4	5	6	7
2	3	4	5	6	7	1
4	5	6	7	1	2	3
ℓ_1	ℓ_2	ℓ_3	ℓ_4	ℓ_5	ℓ_6	ℓ_7

The projective plane of order 2

Let

$$\begin{aligned} u &= 1\quad 1\quad 1\quad 1\quad 1\quad 1\quad 1, \\ z &= 0\quad 0\quad 0\quad 0\quad 0\quad 0\quad 0, \\ m_i &= u + \ell_i. \end{aligned}$$

That is,

$$\begin{aligned} m_1 &= 0\ 0\ 1\ 0\ 1\ 1\ 1, \\ m_2 &= 1\ 0\ 0\ 1\ 0\ 1\ 1, \\ m_3 &= 1\ 1\ 0\ 0\ 1\ 0\ 1, \\ m_4 &= 1\ 1\ 1\ 0\ 0\ 1\ 0, \\ m_5 &= 0\ 1\ 1\ 1\ 0\ 0\ 1, \\ m_6 &= 1\ 0\ 1\ 1\ 1\ 0\ 0, \\ m_7 &= 0\ 1\ 0\ 1\ 1\ 1\ 0. \end{aligned}$$

Then

$$C = \{z, u, \ell_1, \ell_2, \ell_3, \ell_4, \ell_5, \ell_6, \ell_7, m_1, m_2, m_3, m_4, m_5, m_6, m_7\}.$$

Note that $d(l_i, l_j) =$ number of points on exactly one of l_i or l_j. Then

$$\begin{aligned} d(z, l_i) &= 3, & d(z, m_i) &= 4; \\ d(u, l_i) &= 4, & d(u, m_i) &= 3; \\ d(l_i, l_j) &= 4, & d(m_i, m_j) &= 4, \text{ for } i \neq j; \\ d(l_i, m_i) &= 7; & d(l_i, m_j) &= 3, \text{ for } i \neq j; \\ d(u, z) &= 7. \end{aligned}$$

Note that a line determines the complementary quadrangle and conversely. Hence C is a (7,16,3)-code, and

$$16\left\{\binom{7}{0} + \binom{7}{1}\right\} = 16(1+7) = 16\,.\,8 = 2^4\,.\,2^3 = 2^7.$$

Therefore C is perfect.

Theorem 2.19. $A_2(7, 3) = 16$.

Note 2.20. If x and y are two sets in π_2 with $|x| = a$, $|y| = b$ and $|x \cap y| = c$, then $d(x, y) = a + b - 2c$.