Coding Theory

Sheet 2 Solutions

Spring and Summer 2010

1. For a q-ary (n, M, d) code with $d = 2e + 2$, the same argument as before shows that

$$M \left\{ \sum_{i=0}^{e} \binom{n}{i} (q-1)^i \right\} \leq q^n.$$

2. For $q = 2$, the Sphere Packing Bound for an $(n, M, 2e + 1)$ code is

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

   Here $n = 5, d = 3, e = 1$. So

$$M \left\{ 1 + \binom{5}{1} \right\} \leq 2^5.$$

   Hence $6M \leq 32$, whence $M \leq 5$.

3. Choose two words in C as $a_1 = 00000, a_2 = 11100$. Since $d(x, a_1) \geq 3$ for any x in C the only other possible elements of C are the 9 words with three 1's, apart from a_2, the 5 words with four 1's, and $u = 11111$. As $d(u, a_2) = 2$, so $u \notin C$.

   Three 1's: $11010, 11001, 10110, 10101, 10011, 01110, 01101, 01011, 00111$;

   Four 1's: $11110, 11101, 11011, 10111, 01111$.

   The words with three 1's and two of the first three coordinates 1 are at distance 2 from a_2. This leaves

$$b_1 = 10011, \quad b_2 = 01011, \quad b_3 = 00111.$$

   Similarly, the first two words with four 1's are at distance 1 from a_2. This leaves

$$c_1 = 11011, \quad c_2 = 10111, \quad c_3 = 01111.$$

   Now, $d(b_i, b_j) = 2$, $d(c_i, c_j) = 2$ for $i \neq j$. So there can only be one b_i and one c_j in C. Hence $|C| \leq 4$.

   In fact, taking $b_1 \in C$, the only possibility is c_3. This gives $C = \{a_1, a_2, b_1, c_3\}$ as a $(5, 4, 3)$ code.

4. Let C be a binary $(8, M, 5)$ code with $M \geq 4$. Calling the number of 1's in a word the *weight*, without loss of generality, let $a_1 = 00000000$, $a_2 = 11111000 \in C$. There can be no word of weight 7 or 8 in C as they are too close to a_2. Also, there can be at most one word of weight 6, since two words of weight 6, such as 11111100 and 00111111, are the maximum distance apart namely 4. So, there must be another word of weight 5 in C. This must have 1's in the last three places, as otherwise it is at distance at most 4 from a_2; so let it be $a_3 = 00011111$. Now, the only possible word than can be added to C is $a_4 = 11100111$.

5. Let e be the packing radius and ρ the covering radius.

$$\begin{aligned}
&C_1 = \{00, 01, 10, 11\} : && e = 0, \quad \rho = 0;\\
&C_2 = \{000, 011, 101, 110\} : && e = 0, \quad \rho = 1;\\
&C_3 = \{00000, a_1 = 01101, a_2 = 10110, a_3 = 11011\} : && e = 1, \quad \rho = 2.
\end{aligned}$$

For C_3, all the words with four 1's are either a_3 or at distance 2 from this codeword, since they can be obtained by an interchange of two symbols from it.

There are 10 words with three 1's; apart from a_1, a_2, they are as follows:

x	11100	11010	11001	10101
	$d(x, a_1) = 2$	$d(x, a_2) = 2$	$d(x, a_3) = 2$	$d(x, a_2) = 2$
x	10011	01110	01011	00111
	$d(x, a_2) = 2$	$d(x, a_1) = 2$	$d(x, a_1) = 2$	$d(x, a_1) = 2$

6. The code $C = \{a_0 = 000\ldots0, a_1 = 111\ldots1\}$ is of of length n. Any vector x in $(F_2)^n$ has t coordinates 1, and $n - t$ coordinates 0. So $d(x, a_0) = t$ and $d(x, a_1) = n - t$. Hence, if $t < n/2$, then x is uniquely decoded as a_0, whereas, if $t > n/2$, then x is uniquely decoded as a_1. So C is perfect and corrects $\lfloor n/2 \rfloor = (n-1)/2$ errors.

   This can also be done using the Sphere Packing Bound.

7. $C = \{000000, 111111, 222222\}$. So $e = 2$ since two errors will be corrected but three will not; for example, 000111. However, $\rho = 4$, since if a received message as three digits the same, it is at distance 3 from a codeword, but if it has only two digits the same, such as 012012, it is at distance 4 from a codeword.

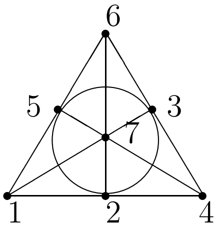
8. Here is the geometry with $P_i = i$.

   Then $\ell_i + \ell_j = a_1a_2a_3a_4a_5a_6a_7$, where

$$\begin{aligned}
a_r = 1 &\iff P_r \text{ lies on precisely one of } \ell_i, \ell_j\ ,\\
a_r = 0 &\iff P_r \text{ lies on the third line through } \ell_i \cap \ell_j.
\end{aligned}$$

   Hence $\ell_i + \ell_j = u + \ell_k = m_k$ for some k, where $u = 1111111$. Then

$$\begin{aligned}
m_i + \ell_j &= u + \ell_i + \ell_j = u + m_k = \ell_k,\\
m_i + m_j &= u + \ell_i + u + \ell_j = \ell_i + \ell_j = m_k.
\end{aligned}$$



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

Figure 1: The projective plane of order 2

9. The Sphere Packing Bound for a binary $(n, M, 7)$ code says that

$$M\left\{\binom{n}{0}+\binom{n}{1}+\binom{n}{2}+\binom{n}{3}\right\}=2^n.$$

So,

$$\binom{n}{0}+\binom{n}{1}+\binom{n}{2}+\binom{n}{3}=2^r;$$

that is,

$$\begin{aligned}
1+n+\tfrac{1}{2}n(n-1)+\tfrac{1}{6}n(n-1)(n-2) &= 2^r,\\
6(n+1)+3n(n-1)+n(n-1)(n-2) &= 3\times 2^{r+1},\\
6(n+1)+n(n-1)\{3+(n-2)\} &= 3\times 2^{r+1},\\
(n+1)\{n^2-n+6\} &= 3\times 2^{r+1},\\
(n+1)\{(n+1)^2-3(n+1)+8\} &= 3\times 2^{r+1}. \qquad (1)
\end{aligned}$$

If 16 divides $n+1$, then the second term on the LHS is divisible by 8 but not by 16; so it is 8 or 24. If it is 8, then

$$(n+1)^2-3(n+1)=0,$$

which is impossible, since $n \geq 7$; if it is 24, then

$$(n+1)^2-3(n+1)-16=0,$$

which is also impossible, as the discriminant is 73.

Therefore, $n+1$ divides 24, whence $n = 7, 11, 23$. Now, $n = 11$ does not satisfy Equation (1). So, $n = 7$ or 23. In fact, perfect codes of these lengths exist, the repetition code of length 7 and the Golay code, respectively.

10. (a) In $\mathbf{F}_5$,

x	1	2	−2	−1
x^{-1}	1	−2	2	−1

(b) In $\mathbf{F}_7$,

x	1	2	3	−3	−2	−1
x^{-1}	1	−3	−2	2	3	−1

(c) In $\mathbf{F}_{13}$,

x	1	2	3	4	5	6	−6	−5	−4	−3	−2	−1
x^{-1}	1	−6	−4	−3	−5	−2	2	5	3	4	6	−1

(d) In $\mathbf{F}_{17}$,

x	1	2	3	4	5	6	7	8	−8	−7	−6	−5	−4	−3	−2	−1
x^{-1}	1	−8	6	−4	7	3	5	−2	2	−5	−3	−7	4	−6	8	−1

11. The equations $2x + y = 1$, $x + 2y = 1$ have the solution $x = y = 1/3$ in all four fields. Now, from Question 10,

$$1/3 = \begin{cases} 2 & \text{in } \mathbf{F}_5, \\ -2 & \text{in } \mathbf{F}_7, \\ -4 & \text{in } \mathbf{F}_{13}, \\ 6 & \text{in } \mathbf{F}_{17}. \end{cases}$$