SOLUTIONS/HINTS TO PROBLEM SET 5

Problem 1. Exercise 3.1.5: Answered in the textbook.

Exercise 3.1.6:
(a) Hint: This is a $(15, 3, 5)$ linear code.
(b) Hint: This is a $(6, 3, 3)$ linear code.
(c) Hint: This is a $(7, 4, 3)$ linear code.

Problem 2. Exercise 3.1.10: Let $u = (1, 1, 1)$ be the information vector. The codeword $uG = (1, 0, 0, 1, 0)$ has zeroes in positions 2, 3, and 5.

Exercise 3.1.11: Without loss of generality, assume the first k columns are linearly dependent. It follows that the $k \times k$ submatrix A formed from rows $1..k$ and columns $1..k$ is singular. Thus, there exists a nonzero vector $\mathbf{u} = (u_1, \ldots, u_k)$ such that $\mathbf{u}A = \mathbf{0}$. Since the rows of G are linearly independent, we have

$$\mathbf{0} \neq \mathbf{u}G = \mathbf{u}[A|X] = [\mathbf{u}A|\mathbf{u}X] = [\mathbf{0}|\mathbf{w}]$$

where $\mathbf{w} = (w_1, \ldots, w_{n-k}) \neq \mathbf{0}$.

Problem 3.
(a) Since $d = 3$, we have $t = 1$. Thus

$$|C| \leq \frac{2^8}{\binom{8}{0} + \binom{8}{1}} = 28.4.$$

Since we are considering only linear codes in this problem, $|C|$ must be a power of 2. So, $|C| \leq 16$, i.e., $k \leq 4$.

(b) Since $d = 3$, we have $t = 1$. Thus

$$|C| \leq \frac{2^7}{\binom{7}{0} + \binom{7}{1}} = 16 = 2^4.$$

Hence, $k \leq 4$.

(c) Since $d = 3$, we have $t = 1$. Thus

$$|C| \leq \frac{2^{15}}{\binom{15}{0} + \binom{15}{1}} = 2048 = 2^{11}.$$

Hence, $k \leq 11$.

(d) Since $d = 7$, we have $t = 3$. Thus

$$|C| \leq \frac{2^{23}}{\binom{23}{0} + \binom{23}{1} + \binom{23}{2} + \binom{23}{2}} = 4096 = 2^{12}.$$

Hence, $k \leq 12$.

Problem 4.

(a) By the Gilbert-Varshamov bound (Corollary 3.1.14), we have

$$|C| \geq \frac{2^{n-1}}{\binom{n-1}{0}+\binom{n-1}{1}+\binom{n-1}{2}+\binom{n-1}{3}} = \frac{2^9}{\binom{9}{0}+\binom{9}{1}+\binom{9}{2}+\binom{9}{3}} = 3.93.$$

Since C is linear, $|C|$ must be a power of 2, i.e., $|C| \geq 4$. Therefore, $M = 4$.

(b) The upper bound on $|C|$ is found using the Hamming bound. In this case, $t = \lfloor (d-1)/2 \rfloor = 2$. Thus,

$$|C| \leq \frac{2^n}{\binom{n}{0}+\binom{n}{1}+\binom{n}{2}} = \frac{2^{10}}{\binom{10}{0}+\binom{10}{1}+\binom{10}{2}} = 18.28.$$

Since C is linear, $|C|$ must be a power of 2, i.e., $|C| \leq 16$.

(c) A code C is *perfect* if it attains the Hamming bound (Theorem 3.1.3); that is, if

$$|C| = \frac{2^n}{\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{t}}.$$

By Part (b), C would have 18.28 codewords. No code has 18.28 codewords. Hence, there is no perfect code having length $n = 10$ and distance $d = 5$.

Problem 5. The rate is $k/n = 1/3$, i.e., $n = 3k$. The distance should be $d = 5$ (since it is a 2-error-correcting code). According to the Gilbert-Varshamov (GV) bound, a linear code with parameters $(n = 3k, k, d = 5)$ exists if

$$\binom{3k-1}{0}+\binom{3k-1}{1}+\cdots+\binom{3k-1}{3} < 2^{n-k} = 2^{2k}.$$

By manual inspection, we conclude that $k = 4$ is the smallest integer for which the above inequality holds. It does not hold for $k = 1, 2$, and 3.

Therefore, the smallest n (code length) for which the GV bound guarantees the existence of a $(n, k, 5)$-code of rate 1/3 is $n = 3k = 12$.

Problem 6. Answered in the textbook.

Problem 7.

(a) Denote the entries in the jth column of G by $g_{1j}, g_{2j}, \ldots, g_{kj}$, $j = 1, \ldots, n$. At least one of those entries is nonzero. Now, each entry x in the jth column of the array can be expressed as

$$x = x_1 \cdot g_{1j} + x_2 \cdot g_{2j} + \cdots + x_k \cdot g_{kj},$$

where additions and multiplications are all modulo 2. The equation

$$x_1 \cdot g_{1j} + x_2 \cdot g_{2j} + \cdots + x_k \cdot g_{kj} = 0 \qquad (*)$$

(in the x_i) has 2^{k-1} solutions. That is, half of the k-tuples $(x_1, x_2, \ldots, x_k) \in \{0,1\}^k$ are solutions to it. This can be justified as follows: Without loss of generality, suppose that $g_{1j} = 1$. Once a value of 0 or 1 is freely assigned to each one of $x_2, \ldots, x_k$, the variable x_1 is determined uniquely in order for

$$x_1 + x_2 \cdot g_{2j} + \cdots + x_k \cdot g_{kj} = 0$$

to hold. Thus, the equation in $(*)$ has 2^{k-1} solutions (half of the k-tuples in $\{0,1\}^k$) – and so does

$$x_1 \cdot g_{1j} + x_2 \cdot g_{2j} + \cdots + x_k \cdot g_{kj} = 1.$$

(b) The sum $\sum_{\mathbf{c}\in C} w(\mathbf{c})$ can be calculated by writing all codewords as rows of a $2^k \times n$ matrix and then adding the weights of all the columns of that matrix. By Part (a), a given column will have either no ones or exactly 2^{k-1} ones. Hence,
$$\sum_{\mathbf{c}\in C} w(\mathbf{c}) = n \cdot 2^{k-1}.$$
Now,
$$n \cdot 2^{k-1} = \sum_{\mathbf{c}\in C} w(\mathbf{c}) \geq (2^k - 1) \cdot d_{\min},$$
whence $d_{\min} \leq \dfrac{n \cdot 2^{k-1}}{2^k - 1}$. This is known as the *Plotkin bound*.

Problem 8. Exercise 3.2.5:
$$\binom{2^r - 1}{0} + \binom{2^r - 1}{1} = 1 + 2^r - 1 = 2^r.$$

Exercise 3.2.6: A code C is *perfect* if it attains the Hamming bound (Theorem 3.1.3); that is, if
$$|C| = \frac{2^n}{\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{t}}.$$

(a) Since
$$\frac{2^{15}}{\binom{15}{0} + \binom{15}{1}} = 2^{11},$$
a linear perfect code with $n = 15$ and $d = 3$ may exist.

(b) Since
$$\frac{2^{31}}{\binom{31}{0} + \binom{31}{1}} = 2^{26},$$
a linear perfect code with $n = 31$ and $d = 3$ may exist.

(c) Since
$$\frac{2^{15}}{\binom{15}{0} + \binom{15}{1} + \binom{15}{2}} = 270.81$$
a linear perfect code with $n = 15$ and $d = 5$ does not exist.