Problem Set 4 Solutions

Problem 4.1

Show that if $\mathcal{C}$ is a binary linear block code, then in every coordinate position either all codeword components are 0 or half are 0 and half are 1.

$\mathcal{C}$ is linear if and only if $\mathcal{C}$ is a group under vector addition. The subset $\mathcal{C}' \subseteq \mathcal{C}$ of codewords with 0 in a given coordinate position is then clearly a (sub)group, as it is closed under vector addition. If there exists any codeword $\mathbf{c} \in \mathcal{C}$ with a 1 in the given coordinate position, then the (co)set $\mathcal{C}' + \mathbf{c}$ is a subset of $\mathcal{C}$ of size $|\mathcal{C}' + \mathbf{c}| = |\mathcal{C}|$ consisting of the codewords with a 1 in the given coordinate position (all are codewords by the group property, and every codeword $\mathbf{c}'$ with a 1 in the given position is in $\mathcal{C}' + \mathbf{c}$, since $\mathbf{c}' + \mathbf{c}$ is in $\mathcal{C}'$). On the other hand, if there exists no codeword $\mathbf{c} \in \mathcal{C}$ with a 1 in the given position, then $\mathcal{C}' = \mathcal{C}$. We conclude that either half or none of the codewords in $\mathcal{C}$ have a 1 in the given coordinate position.

Show that a coordinate in which all codeword components are 0 may be deleted ("punctured") without any loss in performance, but with savings in energy and in dimension.

If all codewords have a 0 in a given position, then this position does not contribute to distinguishing between any pair of codewords; *i.e.,* it can be ignored in decoding without loss of performance. On the other hand, this symbol costs energy α^2 to transmit, and sending this symbol reduces the code rate (nominal spectral efficiency). Thus for communications purposes, this symbol has a cost without any corresponding benefit, so it should be deleted.

Show that if $\mathcal{C}$ has no such all-zero coordinates, then $s(\mathcal{C})$ has zero mean: $\mathbf{m}(s(\mathcal{C})) = \mathbf{0}$.

By the first part, if $\mathcal{C}$ has no all-zero coordinates, then in each position $\mathcal{C}$ haas half 0s and half 1s, so $s(\mathcal{C})$ has zero mean in each coordinate position.

Problem 4.2 (RM code parameters)

Compute the parameters (k, d) of the RM codes of lengths $n = 64$ and $n = 128$.

Using

$$k(r, m) = \sum_{0 \le j \le r} \binom{m}{j}$$

or

$$k(r, m) = k(r, m-1) + k(r-1, m-1),$$

the parameters for the $n = 64$ RM codes are

$$(64, 64, 1); (64, 63, 2); (64, 57, 4); (64, 42, 8); (64, 22, 16); (64, 7, 32), (64, 1, 64); (64, 0, \infty).$$

Similarly, the parameters for the nontrivial $n = 128$ RM codes are

$$(128, 127, 2); (128, 120, 4); (128, 99, 8); (128, 64, 16); (128, 29, 32); (128, 8, 64); (128, 1, 128).$$

Problem 4.3 (optimizing SPC and EH codes)

(a) Using the rule of thumb that a factor of two increase in K_b costs 0.2 dB in effective coding gain, find the value of n for which an $(n, n-1, 2)$ SPC code has maximum effective coding gain, and compute this maximum in dB.

The nominal coding gain of an $(n, n-1, 2)$ SPC code is $\gamma_c = 2(n-1)/n$, and the number of nearest neighbors is $N_2 = n(n-1)/2$, so the number of nearest neighbors per bit is $K_b = n/2$. The effective coding gain in dB is therefore approximately

$$\begin{aligned}\gamma_{\text{eff}} &= 10\log_{10} 2(n-1)/n - (0.2)\log_2 n/2 \\ &= 10(\log_{10} e)\ln 2(n-1)/n - (0.2)(\log_2 e)\ln n/2.\end{aligned}$$

Differentiating with respect to n, we find that the maximum occurs when

$$10(\log_{10} e)\left(\frac{1}{n-1} - \frac{1}{n}\right) - (0.2)(\log_2 e)\frac{1}{n} = 0,$$

which yields

$$n - 1 = \frac{10\log_{10} e}{(0.2)\log_2 e} \approx 15.$$

Thus the maximum occurs for $n = 16$, where

$$\gamma_{\text{eff}} \approx 2.73 - 0.6 = 2.13 \text{ dB}.$$

(b) Similarly, find the m such that the $(2^m, 2^m - m - 1, 4)$ extended Hamming code has maximum effective coding gain, using

$$N_4 = \frac{2^m(2^m-1)(2^m-2)}{24},$$

and compute this maximum in dB.

Similarly, the nominal coding gain of a $(2^m, 2^m - m - 1, 4)$ extended Hamming code is $\gamma_c = 4(2^m - m - 1)/2^m$, and the number of nearest neighbors is $N_4 = 2^m(2^m-1)(2^m-2)/24$, so the number of nearest neighbors per bit is $K_b = 2^m(2^m-1)(2^m-2)/24(2^m - m - 1)$. Computing effective coding gains, we find

$$\begin{aligned}\gamma_{\text{eff}}(8, 4, 4) &= 2.6 \text{ dB}; \\ \gamma_{\text{eff}}(16, 11, 4) &= 3.7 \text{ dB}; \\ \gamma_{\text{eff}}(32, 26, 4) &= 4.0 \text{ dB}; \\ \gamma_{\text{eff}}(64, 57, 4) &= 4.0 \text{ dB}; \\ \gamma_{\text{eff}}(128, 120, 4) &= 3.8 \text{ dB},\end{aligned}$$

which shows that the maximum occurs for $2^m = 32$ or 64 and is about 4.0 dB.

Problem 4.4 (biorthogonal codes)

We have shown that the first-order Reed-Muller codes $\mathrm{RM}(1, m)$ *have parameters* $(2^m, m+1, 2^{m-1})$*, and that the* $(2^m, 1, 2^m)$ *repetition code* $\mathrm{RM}(0, m)$ *is a subcode.*

(a) Show that $\mathrm{RM}(1, m)$ *has one word of weight 0, one word of weight* 2^m*, and* $2^{m+1} - 2$ *words of weight* 2^{m-1}*. [Hint: first show that the* $\mathrm{RM}(1, m)$ *code consists of* 2^m *complementary codeword pairs* $\{\mathbf{x}, \mathbf{x} + \mathbf{1}\}$*.]*

Since the $\mathrm{RM}(1, m)$ code contains the all-one word $\mathbf{1}$, by the group property it contains the complement of every codeword. The complement of the all-zero word $\mathbf{0}$, which has weight 0, is the all-one word $\mathbf{1}$, which has weight 2^m. In general, the complement of a weight-w word has weight $2^m - w$. Thus if the minimum weight of any nonzero word is 2^{m-1}, then all other codewords must have weight exactly 2^{m-1}.

(b) Show that the Euclidean image of an $\mathrm{RM}(1, m)$ *code is an* $M = 2^{m+1}$ *biorthogonal signal set. [Hint: compute all inner products between code vectors.]*

The inner product between the Euclidean images $s(\mathbf{x}), s(\mathbf{y})$ of two binary n-tuples $\mathbf{x}, \mathbf{y}$ is

$$\langle s(\mathbf{x}), s(\mathbf{y}) \rangle = (n - 2d_H(\mathbf{x}, \mathbf{y}))\alpha^2.$$

Thus $\mathbf{x}$ and $\mathbf{y}$ are orthogonal when $d_H(\mathbf{x}, \mathbf{y}) = n/2 = 2^{m-1}$. It follows that every codeword $\mathbf{x}$ in $\mathrm{RM}(1, m)$ is orthogonal to every other word, except $\mathbf{x} + \mathbf{1}$, to which it is antipodal. Thus the Euclidean image of $\mathrm{RM}(1, m)$ is a biorthogonal signal set.

(c) Show that the code $\mathcal{C}'$ *consisting of all words in* $\mathrm{RM}(1, m)$ *with a 0 in any given coordinate position is a* $(2^m, m, 2^{m-1})$ *binary linear code, and that its Euclidean image is an* $M = 2^m$ *orthogonal signal set. [Same hint as in part (a).]*

By the group property, exactly half the words have a 0 in any coordinate position. Moreover, this set of words $\mathcal{C}'$ evidently has the group property, since the sum of any two codewords in $\mathrm{RM}(1, m)$ that have a 0 in a certain position is a codeword in $\mathrm{RM}(1, m)$ that has a 0 in that position. These words include the all-zero word but not the all-one word. The nonzero words in $\mathcal{C}'$ thus all have weight 2^{m-1}. Thus any two distinct Euclidean images $s(\mathbf{x})$ are orthogonal. Therefore $s(\mathcal{C}')$ is an orthogonal signal set with $M = 2^m$ signals.

(d) Show that the code $\mathcal{C}''$ *consisting of the code words of* $\mathcal{C}'$ *with the given coordinate deleted ("punctured") is a binary linear* $(2^m - 1, m, 2^{m-1})$ *code, and that its Euclidean image is an* $M = 2^m$ *simplex signal set. [Hint: use Exercise 7 of Chapter 5.]*

$\mathcal{C}''$ is the same code as $\mathcal{C}'$, except with one less bit. Since the deleted bit is always a zero, deleting this coordinate does not affect the weight of any word. Thus $\mathcal{C}''$ is a binary linear $(2^m - 1, m, 2^{m-1})$ code in which every nonzero word has Hamming weight 2^{m-1}. Consequently the inner product of the Euclidean images of any two distinct codewords is

$$\langle s(\mathbf{x}), s(\mathbf{y}) \rangle = (n - 2d_H(\mathbf{x}, \mathbf{y}))\alpha^2 = -\alpha^2 = -\frac{E(\mathcal{A})}{2^m - 1},$$

where $E(\mathcal{A}) = (2^m - 1)\alpha^2$ is the energy of each codeword. This is the set of inner products of an $M = 2^m$ simplex signal set of energy $E(\mathcal{A})$, so $s(\mathcal{C}'')$ is geometrically equivalent to a simplex signal set.

Problem 4.5 (generator matrices for RM codes)

Let square $2^m \times 2^m$ matrices U_m, $m \geq 1$, be specified recursively as follows. The matrix U_1 is the 2×2 matrix

$$U_1 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

The matrix U_m is the $2^m \times 2^m$ matrix

$$U_m = \begin{bmatrix} U_{m-1} & 0 \\ U_{m-1} & U_{m-1} \end{bmatrix}.$$

(In other words, U_m is the m-fold tensor product of U_1 with itself.)

(a) Show that $\mathrm{RM}(r,m)$ *is generated by the rows of U_m of Hamming weight 2^{m-r} or greater. [Hint: observe that this holds for $m = 1$, and prove by recursion using the $|u|u+v|$ construction.] For example, give a generator matrix for the $(8,4,4)$ RM code.*

We first observe that U_m is a lower triangular matrix with ones on the diagonal. Thus its 2^m rows are linearly independent, and generate the universe code $(2^m, 2^m, 1) = \mathrm{RM}(m,m)$.

The three RM codes with $m = 1$ are $\mathrm{RM}(1,1) = (2,2,1)$, $\mathrm{RM}(0,1) = (2,1,2)$, and $\mathrm{RM}(-1,1) = (2,0,\infty)$. By inspection, $\mathrm{RM}(1,1) = (2,2,1)$ is generated by the two rows of U_1 of weight 1 or greater (*i.e.,* both rows), and $\mathrm{RM}(0,1) = (2,1,2)$ is generated by the row of U_1 of weight 2 or greater (*i.e.,* the single row $(1,1)$). (Moreover, $\mathrm{RM}(-1,1) = (2,0,\infty)$ is generated by the rows of U_1 of weight 4 or greater (*i.e.,* no rows).)

Suppose now that $\mathrm{RM}(r,m-1)$ is generated by the rows of U_{m-1} of Hamming weight 2^{m-1-r} or greater. By the $|u|u+v|$ construction,

$$\mathrm{RM}(r,m) = \{(\mathbf{u}, \mathbf{u}+\mathbf{v}) \mid \mathbf{u} \in \mathrm{RM}(r,m-1), \mathbf{v} \in \mathrm{RM}(r-1,m-1)\}.$$

Equivalently, since $\mathrm{RM}(r-1,m-1)$ is a subcode of $\mathrm{RM}(r,m-1)$, we can write

$$\mathrm{RM}(r,m) = \{(\mathbf{u}'+\mathbf{v}, \mathbf{u}') \mid \mathbf{u}' \in \mathrm{RM}(r,m-1), \mathbf{v} \in \mathrm{RM}(r-1,m-1)\},$$

where $\mathbf{u}' = \mathbf{u}+\mathbf{v}$. Thus a set of generators for $\mathrm{RM}(r,m)$ is

$$\{(\mathbf{u}', \mathbf{u}'), \mid \mathbf{u}' \in \mathrm{RM}(r,m-1)\}; \{(\mathbf{v}, \mathbf{0}), \mid \mathbf{v} \in \mathrm{RM}(r-1,m-1)\}.$$

Now from the construction of U_m from U_{m-1}, each of these generators is a row of U_m with weight 2^{m-r} or greater, so these rows certainly suffice to generate $\mathrm{RM}(r,m)$. Moreover, they are linearly independent, so their number is the dimension of $\mathrm{RM}(r,m)$:

$$k(r,m) = k(r,m-1) + k(r-1,m-1).$$

For example, the $(8,4,4)$ code is generated by the four rows of U_8 of weight 4 or more:

$$U_8 = \begin{bmatrix} 1&0&0&0&0&0&0&0 \\ 1&1&0&0&0&0&0&0 \\ 1&0&1&0&0&0&0&0 \\ 1&1&1&1&0&0&0&0 \\ 1&0&0&0&1&0&0&0 \\ 1&1&0&0&1&1&0&0 \\ 1&0&1&0&1&0&1&0 \\ 1&1&1&1&1&1&1&1 \end{bmatrix}; \qquad G_{(8,4,4)} = \begin{bmatrix} 1&1&1&1&0&0&0&0 \\ 1&1&0&0&1&1&0&0 \\ 1&0&1&0&1&0&1&0 \\ 1&1&1&1&1&1&1&1 \end{bmatrix}.$$

(b) Show that the number of rows of U_m of weight 2^{m-r} is $\binom{m}{r}$. [Hint: use the fact that $\binom{m}{r}$ is the coefficient of z^{m-r} in the integer polynomial $(1+z)^m$.]

Following the hint, let $N(r,m)$ denote the number of rows of U_m of weight precisely 2^{m-r}, and define the generator polynomial

$$g_m(z) = \sum_{r=0}^{m} N(r,m) z^r.$$

Then since $N(0,1) = N(1,1) = 1$, we have $g_1(z) = 1 + z$. Moreover, since the number of rows of U_m of weight precisely 2^{m-r} is equal to the number of rows of U_{m-1} of weight 2^{m-r} plus the number of rows of U_{m-1} of weight 2^{m-r-1}, we have

$$N(r,m) = N(r-1,m-1) + N(r,m-1).$$

This yields the recursion $g_m(z) = (1+z)g_{m-1}(z)$, from which we conclude that

$$g_m(z) = (1+z)^m = \sum_{r=0}^{m} \binom{m}{r} z^r.$$

Consequently $N(r,m)$ is the coefficient of z^r, namely $N(r,m) = \binom{m}{r}$.

(c) Conclude that the dimension of $\mathrm{RM}(r,m)$ is $k(r,m) = \sum_{0 \le j \le r} \binom{m}{j}$.

Since $k(r,m)$ is the number of rows of U_m of weight 2^{m-r} or greater, we have

$$k(r,m) = \sum_{0 \le j \le r} N(r,m) = \sum_{0 \le j \le r} \binom{m}{j}.$$

Problem 4.6 ("Wagner decoding")

Let $\mathcal{C}$ be an $(n, n-1, 2)$ SPC code. The Wagner decoding rule is as follows. Make hard decisions on every symbol r_k, and check whether the resulting binary word is in $\mathcal{C}$. If so, accept it. If not, change the hard decision in the symbol r_k for which the reliability metric $|r_k|$ is minimum. Show that the Wagner decoding rule is an optimum decoding rule for SPC codes. [Hint: show that the Wagner rule finds the codeword $\mathbf{x} \in \mathcal{C}$ that maximizes $r(\mathbf{x} \mid \mathbf{r})$.]

The maximum-reliability (MR) detection rule is to find the codeword that maximizes $r(\mathbf{x} \mid \mathbf{r}) = \sum_k |r_k|(-1)^{e(x_k, r_k)}$, where $e(x_k, r_k) = 0$ if the signs of $s(x_k)$ and r_k agree, and 1 otherwise. MR detection is optimum for binary codes on a Gaussian channel.

If there is a codeword such that $e(x_k, r_k) = 0$ for all k, then $r(\mathbf{x} \mid \mathbf{r})$ clearly reaches its maximum possible value, namely $\sum_k |r_k|$, so this codeword should be chosen.

A property of a SPC code is that any word not in the code (*i.e.*, an odd-weight word) may be changed to a codeword (*i.e.*, an even-weight word) by changing any single coordinate value. The resulting value of $r(\mathbf{x} \mid \mathbf{r})$ will then be $(\sum_k |r_k|) - 2|r_{k'}|$, where k' is the index of the changed coordinate. To maximize $r(\mathbf{x} \mid \mathbf{r})$, we should therefore choose the k' for which $|r_{k'}|$ is minimum. This is the Wagner decoding rule.

It is clear that any further changes can only further lower $r(\mathbf{x} \mid \mathbf{r})$, so Wagner decoding succeeds in finding the codeword that maximizes $r(\mathbf{x} \mid \mathbf{r})$, and is thus optimum.

Problem 4.7 (small cyclic groups).

Write down the addition tables for $\mathbb{Z}_2, \mathbb{Z}_3$ and $\mathbb{Z}_4$. Verify that each group element appears precisely once in each row and column of each table.

The addition tables for $\mathbb{Z}_2, \mathbb{Z}_3$ and $\mathbb{Z}_4$ are as follows:

+	0	1
0	0	1
1	1	0

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

In each table, we verify that every row and column is a permutation of $\mathbb{Z}_n$.

Problem 4.8 (subgroups of cyclic groups are cyclic).

Show that every subgroup of $\mathbb{Z}_n$ is cyclic. [Hint: Let s be the smallest nonzero element in a subgroup $S \subseteq \mathbb{Z}_n$, and compare S to the subgroup generated by s.]

Following the hint, let S be a subgroup of $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$, let s be the smallest nonzero element of S, and let $S(s) = \{s, 2s, \ldots, ms = 0\}$ be the (cyclic) subgroup of S generated by s. Suppose that $S \neq S(s)$; *i.e.,* there is some element $t \in S$ that is not in $S(s)$. Then by the Euclidean division algorithm $t = qs + r$ for some $r < s$, and moreover $r \neq 0$ because $t = qs$ implies $t \in S(s)$. But $t \in S$ and $qs \in S(s) \subseteq S$ imply $r = t - qs \in S$; but $r \neq 0$ is smaller than the smallest nonzero element $s \in S$, contradiction. Thus $S = S(s)$; *i.e.,* S is the cyclic subgroup that is generated by its smallest nonzero element.