Wednesday, February 23, 2005
Handout #9
Due: Wednesday, March 2, 2005

Problem Set 4

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

Problem 4.2 (RM code parameters)

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

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.

(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.

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 $\{\mathbf{x}, \mathbf{x} + \mathbf{1}\}$.]

(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.]

(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).]

(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.]

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 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.

(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 $(1 + z)^m$.]

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

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 $r(\mathbf{x} \mid \mathbf{r})$.]

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.

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.]