6.451 Principles of Digital Communication II
MIT, Spring 2005

Wednesday, April 6, 2005
Handout #17
Due: Wednesday, April 13, 2005

Problem Set 7

Problem 7.1 (State space sizes in trellises for RM codes)

Recall the $|u|u+v|$ construction of a Reed-Muller code $\mathrm{RM}(r,m)$ with length $n = 2^m$ and minimum distance $d = 2^{m-r}$:

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

Show that if the past $\mathcal{P}$ is taken as the first half of the time axis and the future $\mathcal{F}$ as the second half, then the subcodes $\mathcal{C}_\mathcal{P}$ and $\mathcal{C}_\mathcal{F}$ are both effectively equal to $\mathrm{RM}(r-1,m-1)$ (which has the same minimum distance $d = 2^{m-r}$ as $\mathrm{RM}(r,m)$), while the projections $\mathcal{C}_{|\mathcal{P}}$ and $\mathcal{C}_{|\mathcal{F}}$ are both equal to $\mathrm{RM}(r,m-1)$. Conclude that the dimension of the minimal central state space of $\mathrm{RM}(r,m)$ is

$$\dim \mathcal{S} = \dim \mathrm{RM}(r,m-1) - \dim \mathrm{RM}(r-1,m-1).$$

Evaluate $\dim \mathcal{S}$ for all RM codes with length $n \leq 32$.

Similarly, show that if the past $\mathcal{P}$ is taken as the first quarter of the time axis and the future $\mathcal{F}$ as the remaining three quarters, then the subcode $\mathcal{C}_\mathcal{P}$ is effectively equal to $\mathrm{RM}(r-2,m-2)$, while the projection $\mathcal{C}_{|\mathcal{P}}$ is equal to $\mathrm{RM}(r,m-2)$. Conclude that the dimension of the corresponding minimal state space of $\mathrm{RM}(r,m)$ is

$$\dim \mathcal{S} = \dim \mathrm{RM}(r,m-2) - \dim \mathrm{RM}(r-2,m-2).$$

Using the relation $\dim \mathrm{RM}(r,m) = \dim \mathrm{RM}(r,m-1) + \dim \mathrm{RM}(r-1,m-1)$, show that

$$\dim \mathrm{RM}(r,m-2) - \dim \mathrm{RM}(r-2,m-2) = \dim \mathrm{RM}(r,m-1) - \dim \mathrm{RM}(r-1,m-1).$$

Problem 7.2 (Projection/subcode duality and state space duality)

Recall that the dual code to an (n,k,d) binary linear block code $\mathcal{C}$ is defined as the orthogonal subspace $\mathcal{C}^\perp$, consisting of all n-tuples that are orthogonal to all codewords in $\mathcal{C}$, and that $\mathcal{C}^\perp$ is a binary linear block code whose dimension is $\dim \mathcal{C}^\perp = n - k$.

Show that for any partition of the time axis $\mathcal{I}$ of $\mathcal{C}$ into past $\mathcal{P}$ and future $\mathcal{F}$, the subcode $(\mathcal{C}^\perp)_\mathcal{P}$ is equal to the dual $(\mathcal{C}_{|\mathcal{P}})^\perp$ of the projection $\mathcal{C}_{|\mathcal{P}}$, and *vice versa*. [Hint: notice that $(\mathbf{a}, \mathbf{0})$ is orthogonal to $(\mathbf{b}, \mathbf{c})$ if and only if $\mathbf{a}$ is orthogonal to $\mathbf{b}$.]

Conclude that at any time the minimal state spaces of $\mathcal{C}$ and $\mathcal{C}^\perp$ have the same dimension.

Problem 7.3 (Trellis-oriented generator matrix for $(16, 5, 8)$ RM code)

Consider the following generator matrix for the $(16, 5, 8)$ RM code, which follows directly from the $|u|u + v|$ construction:

$$\begin{bmatrix} 1111111100000000 \\ 1111000011110000 \\ 1100110011001100 \\ 1010101010101010 \\ 1111111111111111 \end{bmatrix}.$$

(a) Convert this generator matrix to a trellis-oriented generator matrix.

(b) Determine the state complexity profile of a minimal trellis for this code.

(c) Determine the branch complexity profile of a minimal trellis for this code.

Problem 7.4 (Minimum-span generators for convolutional codes)

Let $\mathcal{C}$ be a rate-$1/n$ binary linear convolutional code generated by a rational n-tuple $\mathbf{g}(D)$, and let $\mathbf{g}'(D)$ be the canonical polynomial n-tuple that generates $\mathcal{C}$. Show that the generators $\{D^k\mathbf{g}'(D), k \in \mathbb{Z}\}$ are a set of minimum-span generators for $\mathcal{C}$.

Problem 7.5 (Trellis complexity of MDS codes, and the Wolf bound)

Let $\mathcal{C}$ be a linear $(n, k, d = n - k + 1)$ MDS code over a finite field $\mathbb{F}_q$. Using the property that in an MDS code there exist $q-1$ weight-d codewords with support $\mathcal{J}$ for every subset $\mathcal{J} \subseteq \mathcal{I}$ of size $|\mathcal{J}| = d$, show that a trellis-oriented generator matrix for $\mathcal{C}$ must have the following form:

$$\begin{bmatrix} xxxx0000 \\ 0xxxx000 \\ 00xxxx00 \\ 000xxxx0 \\ 0000xxxx \end{bmatrix},$$

where $xxxx$ denotes a span of length $d = n - k + 1$, which shifts right by one position for each of the k generators (*i.e.,* from the interval $[1, n - k + 1]$ to $[k, n]$).

For example, show that binary linear $(n, n - 1, 2)$ and $(n, 1, n)$ block codes have trellis-oriented generator matrices of this form.

Conclude that the state complexity profile of any $(n, k, d = n - k + 1)$ MDS code is

$$\{1, q, q^2, \ldots, |\mathcal{S}|_{\max}, |\mathcal{S}|_{\max}, \ldots, q^2, q, 1\},$$

where $|\mathcal{S}|_{\max} = q^{\min(k,\ n-k)}$.

Using the state space theorem and Problem 7.2, show that this is the worst possible state complexity profile for a (n, k) linear code over $\mathbb{F}_q$. This is called the Wolf bound.

Problem 7.6 (Muder bounds on state and branch complexity profiles of $(24, 12, 8)$ code)

The maximum possible dimension of an $(n, k, d \geq 8)$ binary linear block code is known to be

$$k_{\max} = \{0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 2, 2, 3, 4, 5, 5, 6, 7, 8, 9, 10, 11, 12\}$$

for $n = \{1, 2, \ldots, 24\}$, respectively. [These bounds are achieved by $(8, 1, 8), (12, 2, 8)$, $(16, 5, 8)$ and $(24, 12, 8)$ codes and shortened codes thereof.]

Show that the best possible state complexity profile of any $(24, 12, 8)$ code (known as a binary Golay code) is

$$\{1, 2, 4, 8, 16, 32, 64, 128, 64, 128, 256, 512, 256, 512, 256, 128, 64, 128, 64, 32, 16, 8, 4, 2, 1\}.$$

Show that the best possible branch complexity profile is

$$\{2, 4, 8, 16, 32, 64, 128, 128, 128, 256, 512, 512, 512, 512, 256, 128, 128, 128, 64, 32, 16, 8, 4, 2\}.$$

[Note: there exists a standard coordinate ordering for the Golay code that achieves both of these bounds.]