Problem Set 7 Solutions

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*

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

The subcode $\mathcal{C}_{\mathcal{P}}$ is the set of all codewords with second half $\mathbf{u}+\mathbf{v} = \mathbf{0}$, which implies that $\mathbf{u} = \mathbf{v}$. Thus $\mathcal{C}_{\mathcal{P}} = \{(\mathbf{v}, \mathbf{0}) \mid \mathbf{v} \in \mathrm{RM}(r-1, m-1)\}$, which implies that $\mathcal{C}_{\mathcal{P}}$ is effectively $\mathrm{RM}(r-1, m-1)$.

Similarly, the subcode $\mathcal{C}_{\mathcal{F}}$ is the set of all codewords with first half $\mathbf{u} = \mathbf{0}$. Thus $\mathcal{C}_{\mathcal{F}} = \{(\mathbf{0}, \mathbf{v}) \mid \mathbf{v} \in \mathrm{RM}(r-1, m-1)\}$, which implies that $\mathcal{C}_{\mathcal{F}}$ is also effectively $\mathrm{RM}(r-1, m-1)$.

The past projection $\mathcal{C}_{|\mathcal{P}}$ is clearly $\{\mathbf{u} \mid \mathbf{u} \in \mathrm{RM}(r, m-1)\} = \mathrm{RM}(r, m-1)$. Similarly, since $\mathrm{RM}(r-1, m-1)$ is a subcode of $\mathrm{RM}(r, m-1)$, the future projection $\mathcal{C}_{|\mathcal{F}}$ is $\mathrm{RM}(r, m-1)$.

Since $\dim \mathcal{S} = \dim \mathcal{C}_{|\mathcal{P}} - \dim \mathcal{C}_{\mathcal{P}} = \dim \mathcal{C}_{|\mathcal{F}} - \dim \mathcal{C}_{\mathcal{F}}$, it follows that

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

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

For repetition codes $\mathrm{RM}(0,m)$, $\dim \mathcal{S} = \dim \mathrm{RM}(0, m-1) - \dim \mathrm{RM}(-1, m-1) = 1 - 0 = 1$.

For SPC codes $\mathrm{RM}(m-1,m)$, $\dim \mathcal{S} = \dim \mathrm{RM}(m-1, m-1) - \dim \mathrm{RM}(m-2, m-1) = 2^m - (2^m - 1) = 1$.

For the $(8,4,4)$ code, we have $\dim \mathcal{S} = \dim(4,3,2) - \dim(4,1,4) = 2$.

For the $(16,11,4)$ code, we have $\dim \mathcal{S} = \dim(8,7,2) - \dim(8,4,4) = 3$.

For the $(16,5,8)$ code, we have $\dim \mathcal{S} = \dim(8,4,4) - \dim(8,1,8) = 3$.

For the $(32,26,4)$ code, we have $\dim \mathcal{S} = \dim(16,15,2) - \dim(16,11,4) = 4$.

For the $(32,16,8)$ code, we have $\dim \mathcal{S} = \dim(16,11,4) - \dim(16,5,8) = 6$.

For the $(32,6,16)$ code, we have $\dim \mathcal{S} = \dim(16,5,8) - \dim(16,1,16) = 4$.

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*

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

Similarly, since

$$\mathrm{RM}(r-1, m-1) = \{(\mathbf{u}', \mathbf{u}' + \mathbf{v}') \mid \mathbf{u}' \in \mathrm{RM}(r-1, m-2), \mathbf{v}' \in \mathrm{RM}(r-2, m-2)\},$$

we now have that $\mathcal{C}_{\mathcal{P}} = \{(\mathbf{v}', \mathbf{0}) \mid \mathbf{v}' \in \mathrm{RM}(r-2, m-2)\}$, which implies that $\mathcal{C}_{\mathcal{P}}$ is effectively $\mathrm{RM}(r-2, m-2)$. Also, since

$$\mathrm{RM}(r, m-1) = \{(\mathbf{u}'', \mathbf{u}'' + \mathbf{v}'') \mid \mathbf{u}'' \in \mathrm{RM}(r, m-2), \mathbf{v}'' \in \mathrm{RM}(r-1, m-2)\},$$

we now have that $\mathcal{C}_{|\mathcal{P}} = \{\mathbf{u}'' \mid \mathbf{u}'' \in \mathrm{RM}(r, m-2)\}$, which implies that $\mathcal{C}_{|\mathcal{P}}$ is $\mathrm{RM}(r, m-2)$. Therefore

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

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

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

This follows from $\dim \mathrm{RM}(r, m-1) = \dim \mathrm{RM}(r, m-2) + \dim \mathrm{RM}(r-1, m-2)$ and $\dim \mathrm{RM}(r-1, m-1) = \dim \mathrm{RM}(r-1, m-2) + \dim \mathrm{RM}(r-2, m-2)$.

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 $\mathbf{b}$.]*

Following the hint, because inner products are defined componentwise, we have

$$\langle \mathbf{x}, \mathbf{y} \rangle = \langle \mathbf{x}_{|\mathcal{P}}, \mathbf{y}_{|\mathcal{P}} \rangle + \langle \mathbf{x}_{|\mathcal{F}}, \mathbf{y}_{|\mathcal{F}} \rangle.$$

Moreover $\langle (\mathbf{a}, \mathbf{0}), (\mathbf{b}, \mathbf{c}) \rangle = 0$ if and only if $\langle \mathbf{a}, \mathbf{b} \rangle = 0$. We therefore have the following logical chain:

$$\mathbf{a} \in \mathcal{C}_{\mathcal{P}} \iff (\mathbf{a}, \mathbf{0}) \in C \iff (\mathbf{a}, \mathbf{0}) \perp C^\perp \iff \mathbf{a} \perp (C^\perp)_{|\mathcal{P}},$$

where we have used the definitions of the subcode $\mathcal{C}_{\mathcal{P}}$, the fact that the dual code of $\mathcal{C}^\perp$ is C, the fact that $(\mathbf{a}, \mathbf{0})$ is orthogonal to $(\mathbf{b}, \mathbf{c})$ if and only if $\mathbf{a}$ is orthogonal to $\mathbf{b}$, and the definition of $(\mathcal{C}^\perp)_{|\mathcal{P}}$, respectively.

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

The dimension $\dim \mathcal{S}$ of the minimal state space of $\mathcal{C}$ for a given partition into past and future is $\dim \mathcal{C}_{|\mathcal{P}} - \dim \mathcal{C}_{\mathcal{P}}$. The dimension $\dim \mathcal{S}$ of the minimal state space of $\mathcal{C}^\perp$ for a given partition into past and future is

$$\dim(\mathcal{C}^\perp)_{|\mathcal{P}} - \dim(\mathcal{C}^\perp)_{\mathcal{P}} = (n_{\mathcal{P}} - \dim \mathcal{C}_{\mathcal{P}}) - (n_{\mathcal{P}} - \dim \mathcal{C}_{|\mathcal{P}}) = \dim \mathcal{C}_{|\mathcal{P}} - \dim \mathcal{C}_{\mathcal{P}},$$

where $n_{\mathcal{P}} = |\mathcal{P}|$, and we have used projection/subcode duality and the fact that the dimension of the dual of a code of dimension k on a time axis of length $n_{\mathcal{P}}$ is $n_{\mathcal{P}} - k$.

The fact that the state spaces of a linear code and its dual have the same dimensions is called the *dual state space theorem.*

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.

A trellis-oriented generator matrix is obtained by adding the first generator to each of the others:

$$\begin{bmatrix} 1111111100000000 \\ 0000111111110000 \\ 0011001111001100 \\ 0101010110101010 \\ 0000000011111111 \end{bmatrix}.$$

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

The starting times of the generator spans are $\{1, 2, 3, 5, 9\}$, and the ending times are $\{8, 12, 14, 15, 16\}$. The state dimension profile (number of active generators at cut times) of a minimal trellis for this code is therefore

$$\{0, 1, 2, 3, 3, 4, 4, 4, 3, 4, 4, 4, 3, 3, 2, 1, 0\}.$$

Note that the state-space dimensions at the center, one-quarter, and three-quarter points are equal to

$$\dim(8, 4, 4) - \dim(8, 1, 8) = \dim(4, 3, 2) - \dim(4, 0, \infty) = 3,$$

in accord with Problem 7.1.

Note: this state dimension profile meets the Muder bound at all times (see Problem 7.6), and thus is the best possible for a $(16, 5, 8)$ code.

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

From the trellis-oriented generator matrix, the branch dimension profile (number of active generators at symbol times) of a minimal trellis for this code is therefore

$$\{1, 2, 3, 3, 4, 4, 4, 4, 4, 4, 4, 4, 3, 3, 2, 1\}.$$

Note: this branch dimension profile meets the Muder bound at all times, and thus is the best possible for a $(16, 5, 8)$ 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 $\mathcal{C}$.

Since $\mathbf{g}'(D)$ is canonical, it is noncatastrophic; *i.e.,* a code sequence $u(D)\mathbf{g}'(D)$ is finite only if $u(D)$ is finite. Therefore if $u(D)\mathbf{g}'(D)$ is finite, then $u(D)$ is finite and $\deg u(D)\mathbf{g}'(D) = \deg u(D) + \deg \mathbf{g}'(D)$, where the degree of an n-tuple of finite sequences is defined as the maximum degree of its components. Similarly, $\mathbf{g}'(D)$ is delay-free, so $\mathrm{del}\ u(D)\mathbf{g}'(D) = \mathrm{del}\ u(D) + \mathrm{del}\ \mathbf{g}'(D)$, where the delay of an n-tuple of finite sequences is defined as the minimum delay of its components. Hence the shortest finite sequence in $\mathcal{C}$ with delay k is $D^k\mathbf{g}'(D)$, for all $k \in \mathbb{Z}$. The set $\{D^k\mathbf{g}'(D)\}$ of shifted generators are thus a set of minimum-span generators for $\mathcal{C}$— *i.e.,* a trellis-oriented generator matrix. We easily verify that all starting times are distinct, and so are all stopping times.