Chapter 2

Binary linear codes

2.1 The concept of binary linear codes

Exercises 2.1

2.1.1. *Show that our code* $[7, 4, 3]_2$ *is perfect.*

We have $V_2(1, 7) = 8$. The sphere packing bound says $M \cdot 8 \leq 2^7$, which is satisfied with equality.

2.1.2. *Try to decide if an* $[8, 4, 4]_2$ *exists.*

Start from a generator matrix of the $[7, 4, 3]_2$. Append a new bit to each row such that the weight of each row is even. The result is a generator matrix of an $[8, 4, 4]_2$.

2.1.3. *Give an example showing that the basis of a code is not uniquely determined.*

Any old example will do.

2.1.4. *Determine the parameters of the binary linear code generated by the rows of the matrix*

$$\begin{pmatrix} 1\,0\,0\,1\,1\,0\,1 \\ 0\,1\,0\,1\,0\,1\,1 \\ 0\,0\,1\,0\,1\,1\,1 \end{pmatrix}$$

Simply write out all codewords:

$$\boxed{\begin{array}{c} 0000000 \\ 1001101 \\ 0101011 \\ 0010111 \\ 1100110 \\ 1011010 \\ 0111100 \\ 1110001 \end{array}}$$

These are $8 = 2^3$ different codewords. Each nonzero codeword has weight 4. In particular $d = 4$. The parameters are $[7, 3, 4]_2$.

2.1.5. *Compute the parameters $[n, k, d]_2$ of the binary linear code generated by*

$$G = \begin{pmatrix} 1\,1\,0\,0\,0\,0\,1\,1\,0\,1 \\ 0\,0\,1\,1\,0\,0\,1\,0\,1\,1 \\ 0\,0\,0\,0\,1\,1\,0\,1\,1\,1 \end{pmatrix}$$

Find a nonzero codeword of minimum weight.

Again write out all codewords:

0000000000
1100001101
0011001011
0000110111
1111000110
1100111010
0011111100
1111110001

Again we have $8 = 2^3$ codewords. The smallest nonzero weight is $d = 5$. The parameters are $[10, 3, 5]_2$. The second word in the list has weight 5.

2.2 Block coding

Exercises 2.2

2.2.1. *Follow through all stages of block coding for the input string* 00101110 *when transmission errors occur in coordinates* $3, 7$ *and* 14.

Nothing to say here. Just do it.

2.3 The effect of coding

Exercises 2.3

2.3.1. *Compute the block error probability of the repetition code of length* 3, *seen as a code encoding blocks of length* 4 *into messages of length* 12.

For example, 0010 is encoded 000000111000. No decoding error means no error in each of the four blocks of length 3. For each block the probability of no error is $(1-p)^3+3p(1-p)^2 \approx 1-3p^2$. The total probability of no decoding error is therefore

$$\approx (1-3p^2)^4 \approx 1-18p^2$$

and the error probability is $P \approx 18p^2$. This is very close to the case of the binary Hamming code, which has a much higher information rate.

2.3.2. *Compute information rate and block error probability for a code* $[9,5,3]_2$ *(it exists).*

Information rate $R = 5/9$, probability of correct decoding

$$(1-p)^9 + 9p(1-p)^8 \approx 1 + 36p^2 - 72p^2 \approx 1 - 36p^2.$$

Block error probability $P \approx 36p^2$.

2.3.3. *Compute information rate and block error probability for a code* $[23,12,7]_2$ *(the* **binary Golay code***).*

$R = 12/23$. Probability $1-P$ of no error

$$(1-p)^{23} + 23p(1-p)^{22} + \binom{23}{2}p^2(1-p)^{21} + \binom{23}{3}p^3(1-p)^{20}$$

which is $\approx 1 - \binom{23}{4}p^4$. The error probability is $\approx 8855p^4$.

2.3.4. *Show that the block error probability of a* $[n,k,2e+1]_2$*-code is bounded (approximately) by* $\binom{n}{e+1}p^{e+1}$.

This generalizes our earlier calculations. The probability $1-P$ of correct decoding is at least $\sum_{i=0}^{e}\binom{n}{i}p^i(1-p)^{n-i}$ (there are $\binom{n}{i}$ error patterns with precisely i errors, the probability of each such pattern is $p^i(1-p)^{n-i}$). See this expression as a polynomial in p. The leading term (the constant term) is of course 1. Fix some exponent j. The coefficient of p^j is $\sum_{i=0}^{e}\binom{n}{i}(-1)^{j-i}\binom{n-i}{j-i}$.

Our interpretation of binomial numbers in terms of subsets shows the following identity:

$$\binom{n}{i}\binom{n-i}{j-i} = \binom{n}{j}\binom{j}{i}$$

(these are two ways of counting pairs of disjoint subsets, one of cardinality i, the other of cardinality $j-i$, of an n-set). Our coefficient is therefore

$$\binom{n}{j}\sum_{i=0}^{e}(-1)^{j-i}\binom{j}{j-i}$$

For $j=0$ the result is 1 confirming that the leading term is 1. For $1 \leq j \leq e$ the sum simply is the binomial expansion of $(1-1)^j = 0$, showing that those powers p^j do not occur. For $j = e+1$ we have $\sum_{i=0}^{e}(-1)^{e+1-i}\binom{e+1}{e+1-i} = (1-1)^{e+1} - 1 = -1$.

2.4 Duality

Exercises 2.4

2.4.1. *When is the all-*1*-word orthogonal to itself?*

The all-1-word is orthogonal to itself if the length n is even.

2.4.2. *A code is* **self-dual** *if it equals its dual. Is there a self-dual* $[6,3,3]_2$?

There is no self-dual $[6,3,3]_2$.
As in particular each codeword must be orthogonal to itself, all weights must be even. We would have a code $[6,3,4]_2$. The all-1-word is orthogonal to the code and therefore contained in the code. All other codewords have weight 4. However, the sum of a word of weight 4 and the all-1-word has weight 2, contradiction.

2.4.3. *Find a* $(4,8)$*-matrix in standard form (starting with the unit matrix* I*) which generates a self-dual code (*$\mathcal{C}^{\perp} = \mathcal{C}$*) with parameters* $[8,4,4]_2$.

$$\begin{pmatrix} 1&0&0&0&0&1&1&1\\ 0&1&0&0&1&0&1&1\\ 0&0&1&0&1&1&0&1\\ 0&0&0&1&1&1&1&0 \end{pmatrix}$$

2.4.4. *Find a generator matrix of the Hamming code* $[7,4,3]_2$ *in standard form. Use the P-transform to find a check matrix.*

In order to find a generator matrix in standard form simply pick those codewords of $\mathcal{H}$ starting with the quadruples of weight 1. This yields the generator matrix

$$G = \begin{pmatrix} 1\,0\,0\,0\,0\,1\,1 \\ 0\,1\,0\,0\,1\,0\,1 \\ 0\,0\,1\,0\,1\,1\,1 \\ 0\,0\,0\,1\,1\,1\,0 \end{pmatrix}$$

The P-transform yields the check matrix

$$\begin{pmatrix} 0\,1\,1\,1\,1\,0\,0 \\ 1\,0\,1\,1\,0\,1\,0 \\ 1\,1\,1\,0\,0\,0\,1 \end{pmatrix}$$

2.4.5. *Is there a self-dual* $[12, 6, 6]_2$*-code?*

Write a generator matrix in standard form $G = (I|P)$ where P is a $(6, 6) - matrix$. Because of self-duality the rows of P have odd weight, because of $d = 6$ they have weight 5. The sum of two rows of G has weight ≤ 4, contradiction.

2.4.6. *Is there a* $[12, 6, 6]_2$*-code?*

No. After puncturing (cancel the last coordinate in each codeword) an $[11, 6, 5]_2$-code is obtained. It contradicts the sphere-packing bound.

2.5 Binary Hamming and Simplex codes

Exercises 2.5

2.5.1. *Using matrix* M_3*, find at least* 5 *different codewords in the Hamming code* $[7, 4, 3]_2$.

The codewords in the Hamming code generated by matrix M_3 : the rows 1001101, 0101011, 0010111, the pairwise sums 1100110, 1011010, 0111100 and 0000000, 1110001.

2.5.2. *Use* M_4 *and find at least* 5 *different codewords in* $\mathcal{H}_4(2)$.

Similarly using M_4 : there are 16 codewords.

2.5.3. *Use the binary Hamming code* $[7, 4, 3]_2$. *Decode the received vectors* $y_1 = (1, 1, 0, 1, 1, 0, 0)$, $y_2 = (1, 1, 1, 1, 1, 1, 1)$,
$y_3 = (1, 1, 1, 0, 0, 0, 0)$.

Decoding:

$$y_1 = (1,1,0,1,1,0,0) \mapsto (1,1,0,1,0,0,0).$$

$$y_2 = (1,1,1,1,1,1,1) \mapsto y_2.$$

$$y_3 = (1,1,1,0,0,0,0) \mapsto (1,1,1,0,0,0,1).$$

2.5.4. *Prove by induction on r that each nontrivial linear combination of the rows of M_r (each nonzero word of the Simplex code $\mathcal{S}_r(2)$) has weight 2^{r-1}.*

For $r = 1$ and $r = 2$ this is immediately checked. Let $r > 2$. Order the columns of M_r (this ordering is immaterial for our problem) such that in the first row we have all zeroes on the left, the ones on the right. Then M_r has the form

$$M_r = \begin{pmatrix} \mathbf{0} & 1 & \mathbf{1} \\ M_{r-1} & 0 & M_{r-1} \end{pmatrix}$$

(in the middle there is a column $(1, \mathbf{0})^t$). Each linear combination not involving the first row has weight $2^{r-2} + 2^{r-2} = 2^{r-1}$. Adding the first row yields weight $2^{r-2} + 1 + (2^{r-1} - 1 - 2^{r-2}) = 2^{r-1}$. Fortunately also the first row has weight 2^{r-1}.

2.5.5. *Show that the binary Simplex codes $\mathcal{S}_r(2), r \geq 3$ are self-orthogonal (contained in their orthogonals).*

Consider the generator matrix M_r. Each codeword is orthogonal to itself as it has even weight 2^{r-1}. Compare row i and row j of M_r. The number of coordinates where both have entry 1 is 2^{r-2}, which is even.

2.6 The principle of duality for binary linear codes

Exercises 2.6

2.6.1. *Define q-ary orthogonal arrays for arbitrary q.*

An array with n columns and entries from a q-set is a **q-ary orthogonal array** of strength t if in the projection onto any set of t columns each t-tuple of entries occurs the same number λ of times. We write the parameters as

$$OA_\lambda(t, n, q).$$

2.6.2. *Show that a binary orthogonal array of strength $t > 1$ also has strength $t - 1$.*

Let A be a binary orthogonal array of strength $t > 1$. Consider any set of $t-1$ columns and embed it in a set of t columns. Because of strength t there is a number λ such that every t-tuple occurs λ times in the projection onto the t columns. This shows that every $(t-1)$-tuple occurs 2λ times in the projection onto the $t-1$ columns.

2.6.3. *Find a check matrix of $\mathcal{S}_3(2)$ by applying the P-transform to M_3. Use this check matrix to prove that $\mathcal{S}_3(2)$ has minimum weight* 4.

Application of the P-transform to M_3 yields as generator matrix of the Hamming code, check matrix of the Simplex code $\mathcal{S}_3(2)$, the matrix

$$H = \left(\begin{array}{ccc|cccc} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right)$$

In order to prove that $\mathcal{S}_3(2)$ has minimum distance 4 we have to see that no 3 or less columns of H add up to 0. There is no 0-column, and there are no two equal columns. Assume 3 columns add to 0. Clearly they are not all in the right section, corresponding to the unit matrix. If two are on the right, the one column on the left must have weight 2, contradiction. If one is on the right, two on the left must add to a weight 1 column. This is not the case. The remaining case is that all are on the left, but the sum of the 3 left columns is $(0,0,0,1)^t$, contradiction.

2.6.4. *Show that each perfect binary linear code of distance $d = 3$ has the parameters of one of the binary Hamming codes.*

We have $2^n = 2^k(1+n)$. This shows that the length n has the form $n = 2^r - 1$. This shows $r + k = n, k = 2^r - 1 - r$.

2.6.5. *Show that each perfect binary linear code of distance $d = 3$ is equivalent to one of the binary Hamming codes.*

Continuing from the previous exercise we see that a check matrix is an $(r, 2^r-1)$-matrix H which has no zero column (because $d > 1$) and no repeated columns (as $d > 2$). It follows that the columns of H are precisely all nonzero r-tuples in some order.

2.6.6. *Describe an $OA_1(n-1, n, 2)$ for arbitrary length n.*

This is the linear sum zero code: use as rows all binary n-tuples of even weight.