

1. From the defining linear homogeneous equations

$$x_0 + x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 = 0 \tag{1}$$

$$x_0 + x_1 + x_2 + x_3 = 0 \tag{2}$$

$$x_0 + x_1 + x_4 + x_5 = 0 \tag{3}$$

$$x_0 + x_2 + x_4 + x_6 = 0, \tag{4}$$

we see that

$$\bar{x} = (x_0, x_1, \dots, x_7) \in \mathcal{H}_8 \text{ iff } \tilde{\mathbf{H}}\bar{x}^T = 0,$$

where

$$\tilde{\mathbf{H}} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

Thus,  $\tilde{\mathbf{H}}$  is a legitimate parity check matrix for the code *provided it is of full rank*—i.e., all of the rows of  $\tilde{\mathbf{H}}$  are linearly independent). To verify this, use Gaussian elimination to reduce  $\tilde{\mathbf{H}}$  to its canonical form:

$$\begin{aligned} \tilde{\mathbf{H}} &\sim \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} && \text{(Adding first row to each lower row)} \\ &\sim \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} && \text{(Swapping second and fourth rows)} \\ &\sim \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} && \text{(Adding second to first row)} \\ &\sim \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} && \text{(Adding third to first row)} \\ &\sim \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} && \text{(Adding fourth to first row).} \end{aligned}$$

The last matrix is in canonical form—columns corresponding to positions  $x_0, x_1, x_2,$  and  $x_4$  form a  $4 \times 4$  identity matrix. Hence,  $\tilde{\mathbf{H}}$  is a parity check matrix for the code and so are any of the matrices derived from it via Gaussian elimination.

Since it is easier to work with the canonical form, we take

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

as our preferred parity check matrix. Since

$$\bar{x} = (x_0, x_1, \dots, x_7) \in \mathcal{H}_8 \quad \text{iff} \quad \mathbf{H}\bar{x}^T = 0,$$

the code words of  $\mathcal{H}_8$  satisfy the parity check equations:

$$\begin{aligned} x_0 &= x_3 + x_5 + x_6 \\ x_1 &= x_3 + x_5 + x_7 \\ x_2 &= x_3 + x_6 + x_7 \\ x_4 &= x_5 + x_6 + x_7. \end{aligned}$$

These equations say that we get the code words of  $\mathcal{H}_8$  by freely choosing the values of  $x_3$ ,  $x_5$ ,  $x_6$ , and  $x_7$ , as 0 or 1, and then computing the remaining coordinates. A basis for the code is most easily determined by selecting those code words that have exactly one of the freely chosen variables equal to 1. This gives the following basis set:

$$\begin{aligned} \bar{g}_0 &= (1 \ 1 \ 1 \ \underline{1} \ 0 \ \underline{0} \ \underline{0} \ \underline{0}) \\ \bar{g}_1 &= (1 \ 1 \ 0 \ \underline{0} \ 1 \ \underline{1} \ \underline{0} \ \underline{0}) \\ \bar{g}_2 &= (1 \ 0 \ 1 \ \underline{0} \ 1 \ \underline{0} \ \underline{1} \ \underline{0}) \\ \bar{g}_3 &= (0 \ 1 \ 1 \ \underline{0} \ 1 \ \underline{0} \ \underline{0} \ \underline{1}). \end{aligned}$$

Hence,

$$\mathbf{G} = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

is a generator matrix for  $\mathcal{H}_8$ .

Note that, if you're careful, you can also get  $\mathbf{G}$  directly from  $\mathbf{H}$  using the following trick:

$$\mathbf{G}_{\text{canonical}} = [ \mathbf{P}_{k \times r} \mid \mathbf{I}_{k \times k} ] \leftrightarrow \mathbf{H}_{\text{canonical}} = [ \mathbf{I}_{r \times r} \mid (\mathbf{P}_{k \times r})^T ].$$

(Care is required since you first temporarily interchange columns  $x_3$  and  $x_4$ , then apply the trick, and finally swap the columns back.)

The code  $\mathcal{H}_8$  is the row space of  $\mathbf{G}$ ; hence, it consists of all linear combinations of the rows of  $\mathbf{G}$ . There are 16 code words:

$$\begin{aligned} c_{0000} &= (0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0) \\ c_{1000} &= (1 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0) \\ c_{0100} &= (1 \ 1 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0) \\ c_{1100} &= (0 \ 0 \ 1 \ 1 \ 1 \ 1 \ 0 \ 0) \\ c_{0010} &= (1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0) \\ c_{1010} &= (0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 1 \ 0) \\ c_{0110} &= (0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 1 \ 0) \\ c_{1110} &= (1 \ 0 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0) \\ c_{0001} &= (0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 0 \ 1) \\ c_{1001} &= (0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 0 \ 1) \\ c_{0101} &= (1 \ 0 \ 1 \ 0 \ 0 \ 1 \ 0 \ 1) \\ c_{1101} &= (0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1) \\ c_{0011} &= (1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 1) \\ c_{1011} &= (0 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 1) \\ c_{0111} &= (0 \ 0 \ 0 \ 0 \ 1 \ 1 \ 1 \ 1) \\ c_{1111} &= (1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1). \end{aligned}$$

The code's length is  $n = 8$  and dimension is  $k = 4$ , so the rate of the code is  $R = k/n = 1/2$ .

2. (a) In this case, we see that

$$\bar{x} = (x_0, x_1, \dots, x_7) \in \mathcal{H}_8^* \quad \text{iff} \quad \mathbf{H}\bar{x}^T = 0,$$

where

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

Applying Gaussian elimination to  $\mathbf{H}$ , we derive its canonical form:

$$\tilde{\mathbf{H}} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{bmatrix}.$$

The matrix  $\tilde{\mathbf{H}}$  has rank 3 (three independent rows) and is a parity check matrix for  $\mathcal{H}_8^*$ ; so  $\mathcal{H}_8^*$  has parameters  $n = 8$ ,  $r = \text{rank}(\mathbf{H}) = 3$ ,  $k = n - r = 5$ , and rate  $R = 5/8$ .

To check whether or not,  $\mathcal{H}_8^*$  is 1-error correcting, we use  $\tilde{\mathbf{H}}$  to build a syndrome table for the error patterns of weight less or equal to 1.

Error Pattern	Syndrome
00000000	000
10000000	100
01000000	010
00100000	001
00010000	111
00001000	011
00000100	101
00000010	110
00000001	000

The syndrome table shows a repetition, so syndrome table decoding does not work. Considering this further, we note that both 00000000 and 00000001 are code words, since their syndromes are all zero. Hence, an error in position  $x_7$  is not even detectable! Thus,  $\mathcal{H}_8^*$  is not 1-error correcting.

(b) In this case, we have the same parity check matrices as in part (a), except that the last column is dropped. Hence, the code  $\mathcal{H}_7$  has canonical parity check matrix

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

From the parity check matrix, we see that the code has parameters  $n = 7$ ,  $r = \text{rank}(\mathbf{H}) = 3$ ,  $k = n - r = 4$ , and  $R = 4/7$ . The corresponding syndrome table is shown below:

Error Pattern	Syndrome
$\bar{e}_0 = (0000000)$	000
$\bar{e}_1 = (1000000)$	100
$\bar{e}_2 = (0100000)$	010
$\bar{e}_3 = (0010000)$	001
$\bar{e}_4 = (0001000)$	111
$\bar{e}_5 = (0000100)$	011
$\bar{e}_6 = (0000010)$	101
$\bar{e}_7 = (0000001)$	110

From the syndrome table, it is clear that the code is 1-error correcting.

3. This follows directly from the syndrome table for  $\mathcal{H}_7$  given in the previous problem. You will note that every possible 3-tuple appears exactly once as a syndrome. Consider any received vector  $\bar{r}$ . Its syndrome appears somewhere in the table, say at row  $i$  with corresponding error pattern  $\bar{e}_i$ . Then  $\bar{r} + \bar{e}_i$  is a code word.
4. The code  $\mathcal{H}_7$  has canonical parity check matrix

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix},$$

so the code words satisfy the parity check equations

$$\begin{aligned} x_0 &= x_3 + x_5 + x_6 \\ x_1 &= x_3 + x_4 + x_6 \\ x_2 &= x_3 + x_4 + x_5. \end{aligned}$$

Let the erasures occur at positions  $x_i, x_j$  with  $i \neq j$ . Regardless of the choice of  $i$  and  $j$ , there is at least one equation in which either  $x_i$  appears without  $x_j$ , or  $x_j$  appears without  $x_i$ . Use this equation to solve for the erasure at that position. Any parity check equation containing the other variable can now be used to solve for the second erasure. This algorithm shows that  $\mathcal{H}_7$  is capable of correcting all error patterns with two or fewer erasures.

5. The matrix  $\mathbf{A}$  is in canonical form. To reduce  $\mathbf{B}$  to canonical form, perform Gaussian elimination:

$$\begin{aligned} \mathbf{B} &\sim \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} && \text{(Adding first to third row)} \\ &\sim \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} && \text{(Adding third to first and second rows),} \end{aligned}$$

which is different than the canonical form for  $\mathbf{A}$ . To reduce  $\mathbf{C}$  to canonical form, perform Gaussian elimination:

$$\begin{aligned} \mathbf{C} &\sim \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix} && \text{(Adding first to third row)} \\ &\sim \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix} && \text{(Adding second to first row)} \\ &\sim \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix} && \text{(Adding third to first and second rows),} \end{aligned}$$

which is the same as  $\mathbf{A}$ . All three canonical forms have rank 3, so all are generator matrices for  $[6, 3]$  codes.  $\mathbf{A}$  and  $\mathbf{C}$  generate the *same* code; whereas  $\mathbf{B}$  generates a *different* code.

6. We have

$$p(\text{parity check matrix}) = \frac{\text{number of binary matrices of rank } r = n - k}{\text{number of binary matrices}}.$$

The total number of  $r \times n$  binary matrices is  $2^{nr}$ .

In order to determine the number of binary matrices of rank  $r$ , we count as follows. There are  $2^n - 1$  choices for the first row, which only has to be nonzero. Given that choice, there are  $2^n - 2$  choices for the second row, which can be any binary vector other than the all-zero vector and the first row itself. In general, having selected  $i$  previous rows, there are  $2^n - 2^i$  choices for the next

row, since any vector that is not among the  $2^i$  linear combinations of the previously chosen rows can be used. Thus, the number of binary matrices of rank  $k$  is  $\prod_{i=0}^{r-1} (2^n - 2^i)$ .

Then

$$\begin{aligned} p(\text{parity check matrix}) &= \frac{\prod_{i=0}^{r-1} (2^n - 2^i)}{2^{nr}} \\ &= \prod_{i=0}^{r-1} \left(1 - \frac{2^i}{2^n}\right). \end{aligned}$$