

1. It is simplest (but sufficiently general) to consider the following generator matrix structure:

$$\mathbf{G} = [I \mid P] = \left[\begin{array}{cc|cccccc} 1 & 0 & 1 & 1 & \cdots & 1 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 & 1 & 1 & \cdots & 1 \end{array} \right],$$

where \mathbf{P} has b consecutive ones flush left in the first row and d consecutive ones flush right on the last row.

Experimentation yields the following solutions:

$$\begin{aligned} n = 2 & \implies d_{\min} = 1, & \mathbf{G} &= \left[\begin{array}{cc|c} 1 & 0 & \\ 0 & 1 & \end{array} \right] \\ n = 3 & \implies d_{\min} = 2, & \mathbf{G} &= \left[\begin{array}{cc|c} 1 & 0 & 1 \\ 0 & 1 & 1 \end{array} \right] \\ n = 4 & \implies d_{\min} = 2, & \mathbf{G} &= \left[\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{array} \right] \\ n = 5 & \implies d_{\min} = 3, & \mathbf{G} &= \left[\begin{array}{cc|ccc} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{array} \right] \\ n = 6 & \implies d_{\min} = 4, & \mathbf{G} &= \left[\begin{array}{cc|cccc} 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 \end{array} \right] \\ n = 7 & \implies d_{\min} = 4, & \mathbf{G} &= \left[\begin{array}{cc|ccccc} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \end{array} \right] \\ n = 8 & \implies d_{\min} = 5, & \mathbf{G} &= \left[\begin{array}{cc|ccccc} 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \end{array} \right] \\ n = 9 & \implies d_{\min} = 6, & \mathbf{G} &= \left[\begin{array}{cc|cccccc} 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{array} \right] \\ n = 10 & \implies d_{\min} = 6, & \mathbf{G} &= \left[\begin{array}{cc|cccccc} 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{array} \right] \\ n = 11 & \implies d_{\min} = 7, & \mathbf{G} &= \left[\begin{array}{cc|ccccccc} 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array} \right] \\ n = 12 & \implies d_{\min} = 8, & \mathbf{G} &= \left[\begin{array}{cc|cccccccc} 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array} \right]. \end{aligned}$$

For $k = 2$ and general n , it is straightforward to show—but surprisingly tedious!—that the best possible minimum Hamming distance is given by $d_{\min} = \lfloor \frac{2n}{3} \rfloor$. Our experimental findings are consistent with this result.

2. In this simple example, we can solve the problem by trial and error—perhaps even by inspection! Larger codes would require a more systematic approach (pun intended), which is illustrated in my solution below.

We make use of the following neat trick from linear algebra. Let \mathbf{A} be a $\ell \times m$ matrix with canonical form \mathbf{B} , and let $\mathbf{M} = [\mathbf{A} \mid \mathbf{I}]$ be the $\ell \times (m + \ell)$ matrix produced from \mathbf{A} by appending the $\ell \times \ell$ identity matrix \mathbf{I} . Gaussian elimination applied to \mathbf{M} produces its canonical form $[\mathbf{B} \mid \mathbf{Q}]$, where \mathbf{Q} has the curious property that

$$\mathbf{QA} = \mathbf{B}.$$

In effect, \mathbf{Q} “memorizes” the Gaussian elimination steps that changes \mathbf{A} to \mathbf{B} .

This is in fact the usual method for finding the multiplicative inverse of a square matrix (or showing that it doesn’t exist). In particular, if \mathbf{B} is the identity matrix, then \mathbf{A} is invertible, with inverse $\mathbf{A}^{-1} = \mathbf{Q}$. If \mathbf{B} is not the identity matrix, then \mathbf{A} is not invertible.

$$\begin{array}{c}
\sim \\
\left[\begin{array}{cccc|cccccccc}
1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array} \right] \\
\end{array} \quad \text{(adding 3rd to rows 1 - 2, 4 - 6)}$$

$$\begin{array}{c}
\sim \\
\left[\begin{array}{cccc|cccccccc}
1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1
\end{array} \right] \\
\end{array} \quad \text{(adding 4th to rows 5 - 6, 8 - 10),}$$

which achieves the desired canonical form for \mathbf{M} . The matrices of interest are

$$\mathbf{B} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad \text{and} \quad \mathbf{Q} = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

Since $\bar{c} = \bar{a}\mathbf{G}$, we have $\bar{c}^T = \mathbf{G}^T\bar{a}^T$. We also know that $\mathbf{Q}\mathbf{G}^T = \mathbf{B}$. Then

$$\mathbf{Q}\bar{c}^T = \mathbf{Q}\mathbf{G}^T\bar{a}^T = \mathbf{B}\bar{a}^T = \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}.$$

We do not need the extra zeros in the output, so let \mathbf{A} be the 4×10 matrix consisting of the first

four rows of \mathbf{Q} . Then $\mathbf{\Lambda}\bar{\mathbf{c}}^T = \bar{\mathbf{a}}^T$, so the solution to the problem is the matrix:

$$\mathbf{J} = \mathbf{\Lambda}^T = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

It is easy to check that this \mathbf{J} works.

The matrix \mathbf{G} is not square, so has no multiplicative inverse. The problem would be much simpler if it did! One student asked whether the *pseudo-inverse* from linear algebra can be used to solve this problem. For *real* vector spaces, the equation $\bar{\mathbf{c}} = \bar{\mathbf{a}}\mathbf{G}$ can be solved for $\bar{\mathbf{a}}$ by right-multiplying both sides by the pseudo-inverse

$$\mathbf{J} = \mathbf{G}^T (\mathbf{G}\mathbf{G}^T)^{-1}.$$

For *real* matrices, if \mathbf{G} is of full rank (all rows linearly independent), then $\mathbf{G}\mathbf{G}^T$ is always invertible. Thus, the pseudo-inverse exists, even when the matrix \mathbf{G} has no inverse.

In the *binary* case, the pseudo-inverse technique will not always work. The generator matrix \mathbf{G} satisfies the requirement that it is of full rank over the binary field, but this does not guarantee that $\mathbf{G}\mathbf{G}^T$ is invertible over the binary field. For example, there are codes that are self-dual in which case the product is the all-zero matrix! If $\mathbf{G}\mathbf{G}^T$ is invertible over the binary field, however, the pseudo-inverse does exist and can be used to solve the problem. If not, the method does not work, and one has to resort to the procedure described above.

3. (a) The $\mathbf{C} = \mathbf{G}^T\mathbf{U}\mathbf{G}$ be an array code codeword corresponding to information \mathbf{U} . We must show that every row and column of \mathbf{C} is a codeword of the constituent code \mathcal{C} . First, note that the transpose

$$\begin{aligned} \mathbf{C}^T &= (\mathbf{G}^T\mathbf{U}\mathbf{G})^T \\ &= \mathbf{G}^T\mathbf{U}^T(\mathbf{G}^T)^T \\ &= \mathbf{G}^T\mathbf{U}^T\mathbf{G}, \end{aligned}$$

so that \mathbf{C}^T is also an array code codeword, corresponding to information \mathbf{U}^T . As a result, it is enough to show that each row of \mathbf{C} is in \mathcal{C} . (The columns of \mathbf{C} are just the rows of \mathbf{C}^T .)

Let \bar{a}_i denote the i -th row of the matrix $\mathbf{A} = \mathbf{G}^T\mathbf{U}$. Then the i -th row of $\mathbf{C} = \mathbf{A}\mathbf{G}$ is $\bar{c}_i = \bar{a}_i\mathbf{G}$, which is clearly a codeword of \mathcal{C} since \mathbf{G} is a generator matrix for \mathcal{C} .

- (b) Suppose that \mathbf{V} is a matrix whose rows and columns are codewords in the constituent code \mathcal{C} . Then there exist \mathbf{U}_L satisfying

$$\mathbf{V} = \mathbf{U}_L\mathbf{G}$$

and \mathbf{U}_R satisfying

$$\mathbf{V}^T = \mathbf{U}_R^T\mathbf{G} \quad \text{or} \quad \mathbf{V} = \mathbf{G}^T\mathbf{U}_R.$$

To show that \mathbf{V} is in the array code, we must find \mathbf{U} such that $\mathbf{V} = \mathbf{G}^T\mathbf{U}\mathbf{G}$.

By previous problem, there exists a matrix \mathbf{J} that inverts the action of \mathbf{G} —i.e., if $\bar{\mathbf{c}} = \bar{\mathbf{a}}\mathbf{G}$, then $\bar{\mathbf{c}}\mathbf{J} = \bar{\mathbf{a}}$. Thus,

$$\mathbf{G}\mathbf{J} = \mathbf{I},$$

where \mathbf{I} is an identity matrix. We claim that

$$\mathbf{U} = \mathbf{J}^T \mathbf{V} \mathbf{J}$$

is the desired information matrix that produces \mathbf{V} as an array code codeword. First, some preliminary calculations. Note that

$$\mathbf{V} = \mathbf{U}_L \mathbf{G} \Rightarrow \mathbf{V} \mathbf{J} = \mathbf{U}_L \Rightarrow \mathbf{V} \mathbf{J} \mathbf{G} = \mathbf{V}$$

and

$$\mathbf{V}^T = \mathbf{U}_R^T \mathbf{G} \Rightarrow \mathbf{V}^T \mathbf{J} = \mathbf{U}_R^T \Rightarrow \mathbf{V}^T \mathbf{J} \mathbf{G} = \mathbf{V}^T \Rightarrow \mathbf{G}^T \mathbf{J}^T \mathbf{V} = \mathbf{V}.$$

Therefore,

$$\begin{aligned} \mathbf{G}^T \mathbf{U} \mathbf{G} &= \mathbf{G}^T (\mathbf{J}^T \mathbf{V} \mathbf{J}) \mathbf{G} \\ &= (\mathbf{G}^T \mathbf{J}^T \mathbf{V}) \mathbf{J} \mathbf{G} \\ &= \mathbf{V} \mathbf{J} \mathbf{G} \\ &= \mathbf{V}, \end{aligned}$$

as was to be shown.

4. (a) Any row with a non-zero information bit must have weight at least $d_{\min}(\mathcal{H}_7) = 3$, since it is a code word in \mathcal{H}_7 . Likewise, wherever there is a one in a row, the corresponding column must also have weight at least $d_{\min}(\mathcal{H}_7)$. This argument shows that

$$d_{\min}(\mathcal{C}) \geq d_{\min}(\mathcal{H}_7) \cdot d_{\min}(\mathcal{H}_7) = 9.$$

Note that $\bar{c} = (1100001)$ is a minimum weight code word in \mathcal{H}_7 (as defined in HW#1). It may be used to construct the following code word of weight 9 in \mathcal{C} :

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

Hence, $d_{\min}(\mathcal{C}) = 9$.

- (b) By consideration of two code words at the minimum Hamming distance d_{\min} for the code (as done in lecture), it is easy to see that any combination (τ_c, τ_d) is possible provided

$$2\tau_c + \Delta + 1 \leq d_{\min},$$

where $\Delta = \tau_d - \tau_c \geq 0$. The largest τ_d occurs when $\Delta = d_{\min} - 2\tau_c - 1$. Hence, for $d_{\min} = 9$, the following possibilities exist:

| τ_c | Δ | τ_d |
|----------|----------|----------|
| 0 | 8 | 8 |
| 1 | 6 | 7 |
| 2 | 4 | 6 |
| 3 | 2 | 5 |
| 4 | 0 | 4. |

5. (a) Let \bar{e}_i denote the error pattern having a 1 in the i -th position and 0 everywhere else, and let \mathbf{H} be a parity check matrix with columns $\bar{h}_1, \bar{h}_2, \dots, \bar{h}_n$. Then

$$\mathbf{H}\bar{e}_i^T = \begin{bmatrix} \bar{h}_1 & \cdots & \bar{h}_{i-1} & \bar{h}_i & \bar{h}_{i+1} & \cdots & \bar{h}_n \end{bmatrix} \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = \bar{h}_i.$$

Thus, *the columns of the parity check matrix \mathbf{H} are the syndromes for the 1-bit error patterns.* From the syndrome table, we see

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

Since the parity check matrix is of the form $\mathbf{H} = [\mathbf{P} \mid \mathbf{I}_{r \times r}]$, a generator matrix is given by $\mathbf{G} = [\mathbf{I}_{k \times k} \mid \mathbf{P}^T]$. Thus,

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

- (b) The syndrome for \bar{r} is computed as

$$\bar{s} = \mathbf{H}\bar{r}^T = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}.$$

From the table, the error pattern corresponding to this syndrome is $\bar{e} = (0000110)$. Hence, the decoder output is code word $\bar{c} = \bar{r} + \bar{e} = (1110001)$.