Let $\mathbf{H}$ be an $(n-m) \times n$ parity check matrix and $a = a_1 \cdots a_m$ be a sequence of length m. Let $b = b_1 \cdots b_n$ be a word of length n with $b_i = a_i$, $1 \leq i \leq m$ and $\mathbf{Hb}^t = 0$. Suppose that $\mathbf{H} = (\mathbf{A} \quad \mathbf{I}_{n-m})$. Then $\mathbf{Hb}^t = 0$ implies

$$(\mathbf{A} \quad \mathbf{I}_{n-m}) \begin{pmatrix} \mathbf{a}^t \\ \bar{\mathbf{b}}^t \end{pmatrix} = 0$$

where $\bar{\mathbf{b}}$ is the vector formed from the sequence $\bar{b} = b_{m+1} \cdots b_n$ and so $\mathbf{Aa}^t + \mathbf{I}_{n-m}\bar{\mathbf{b}}^t = 0$, i.e. $\mathbf{Aa}^t + \bar{\mathbf{b}}^t = 0$. Hence, $\bar{\mathbf{b}}^t = \mathbf{Aa}^t$ and $b_{m+1} \cdots b_n$ are uniquely determined by a. This proves that for every $a \in \mathbb{B}^m$ there is a uniquely determined word $b \in \mathbb{B}^n$ with $a_i = b_i$, $1 \leq i \leq m$ and $\mathbf{Hb}^t = 0$. We can thus define an encoding function E: $\mathbb{B}^m \to \mathbb{B}^n$ as follows: for $a \in \mathbb{B}^m$, define $E(a) = b$, where b is the uniquely determined element of $\mathbb{B}^n$ with $a_i = b_i$, $1 \leq i \leq m$ and $\mathbf{Hb}^t = 0$. We define the **syndrome** of a word $r \in \mathbb{B}^n$ by $\mathbf{s} = \mathbf{Hr}^t$.

Observe that the syndrome of a code word is zero. Using syndrome, we see how the parity check matrix $\mathbf{H}$ associated with a generator matrix $\mathbf{G}$ helps in correcting errors that occur in transmission. The **syndrome** (or the **parity check**) **decoding procedure** is defined as follows:

Let $r = r_1 \cdots r_m r_{m+1} \cdots r_n$ be the word received and $\mathbf{s} = \mathbf{Hr}^t$ be its syndrome.

(i) If $\mathbf{s} = 0$, we assume that r is the code word sent and the original message word is $r_1 \cdots r_m$.

(ii) If $\mathbf{s}$ matches the ith column of $\mathbf{H}$, we assume that an error in transmission has occurred in the ith position and take

$$c = r_1 \cdots r_{i-1}(r_i + 1)r_{i+1} \cdots r_n$$

as the code word transmitted. The original message is the sequence formed by the initial m entries of c.

(iii) If $\mathbf{s}$ is neither 0 nor a column of $\mathbf{H}$ then at least two errors occurred in transmission.

Theorem 1.5

An $(n-m) \times m$ parity check matrix $\mathbf{H}$ will decode all single errors correctly iff the columns of $\mathbf{H}$ are non-zero and distinct.

Proof

Suppose that the ith column of $\mathbf{H}$ is zero. Let e be the word of weight 1 with 1 in the ith position and 0 everywhere else. Then for any code word b,

$$\mathbf{H}(\mathbf{b} + \mathbf{e})^t = \mathbf{Hb}^t + \mathbf{He}^t = 0 + 0 = 0$$

and, so, by our decoding procedure $D(b + e) = b + e$ and the error vector $\mathbf{e}$ goes undetected.

Next suppose that the ith and jth columns of $\mathbf{H}$ are identical. Let e^i (respectively e^j) be the word of length n with 1 in the ith (respectively jth)

position and 0 everywhere else. For any code word b, we have

$$\begin{aligned}\mathbf{H}(\mathbf{b}+\mathbf{e}^i)^t &= \mathbf{H}\mathbf{b}^t + \mathbf{H}(\mathbf{e}^i)^t \\ &= \mathbf{H}(\mathbf{e}^i)^t \\ &= i\text{th column of } \mathbf{H} \\ &= j\text{th column of } \mathbf{H} \\ &= \mathbf{H}(\mathbf{b}+\mathbf{e}^j)^t\end{aligned}$$

Thus we are unable to decide if the error occurred in the ith position or the jth.

Conversely, suppose that the columns of $\mathbf{H}$ are non-zero and distinct. For any error vector $\mathbf{e}$ of weight 1 with 1 in the ith position and any code word b,

$$\mathbf{H}(\mathbf{b}+\mathbf{e})^t = \mathbf{H}(\mathbf{b}^t + \mathbf{e}^t) = \mathbf{H}\mathbf{b}^t + \mathbf{H}\mathbf{e}^t = 0 + \mathbf{H}\mathbf{e}^t = i\text{th column of } \mathbf{H}$$

and by our decoding procedure $D(b+e)=b$. Hence every single error is corrected.

Theorem 1.6

(i) If $\mathbf{G} = (\mathbf{I}_m \quad \mathbf{A})$ is an $m \times n$ generator matrix of a code, then

$$\mathbf{H} = (\mathbf{A}^t \quad \mathbf{I}_{n-m})$$

is the unique parity check matrix for the same code.

(ii) If $\mathbf{H} = (\mathbf{B} \quad \mathbf{I}_{n-m})$ is an $(n-m) \times n$ parity check matrix, then

$$\mathbf{G} = (\mathbf{I}_m \quad \mathbf{B}^t)$$

is the unique generator matrix for the same code.

Proof

Let $a \in \mathbb{B}^m$ and b be the code word corresponding to this message word in the code given by the generator matrix $\mathbf{G}$. Then $\mathbf{b} = \mathbf{a}\mathbf{G}$. Suppose that

$$b = b_1 \cdots b_m b_{m+1} \cdots b_n \qquad \text{and} \qquad a = a_1 \cdots a_m$$

As the first m columns of $\mathbf{G}$ form the identity matrix, the relation $\mathbf{b} = \mathbf{a}\mathbf{G}$ shows that $a_i = b_i$, $1 \leq i \leq m$. We write $\bar{b}$ for the word $b_{m+1} \cdots b_n$ so that $\mathbf{b} = (\mathbf{a} \quad \bar{\mathbf{b}})$. Now

$$\begin{aligned}\mathbf{H}\mathbf{b}^t &= (\mathbf{A}^t \quad \mathbf{I}_{n-m})(\mathbf{a}\mathbf{G})^t \\ &= (\mathbf{A}^t \quad \mathbf{I}_{n-m})\mathbf{G}^t\mathbf{a}^t \\ &= (\mathbf{A}^t \quad \mathbf{I}_{n-m})(\mathbf{I}_m \quad \mathbf{A})^t\mathbf{a}^t \\ &= (\mathbf{A}^t \quad \mathbf{I}_{n-m})\begin{pmatrix}\mathbf{I}_m \\ \mathbf{A}^t\end{pmatrix}\mathbf{a}^t \\ &= (\mathbf{A}^t \quad \mathbf{I}_m + \mathbf{I}_{n-m}\mathbf{A}^t)\mathbf{a}^t \\ &= (\mathbf{A}^t + \mathbf{A}^t)\mathbf{a}^t = 0 \times \mathbf{a}^t = 0\end{aligned}$$

Hence, b is the code word corresponding to the message word a in the code given by the parity check matrix $\mathbf{H}$.

Conversely, suppose that $c = c_1 \cdots c_n$ is the code word corresponding to the message word $a = a_1 \cdots a_m$ in the code determined by the parity check matrix $\mathbf{H} = (\mathbf{A}^t \quad \mathbf{I}_{n-m})$. Then $c_i = a_i$, $1 \leq i \leq m$ and

$$\mathbf{H}\mathbf{c}^t = 0 \qquad \text{or} \qquad \mathbf{H}\begin{pmatrix} \mathbf{a} \\ \bar{\mathbf{c}}^t \end{pmatrix} = 0$$

where $\bar{c} = c_{m+1} \cdots c_n$, or

$$(\mathbf{A}^t \quad \mathbf{I}_{n-m})\begin{pmatrix} \mathbf{a} \\ \bar{\mathbf{c}}^t \end{pmatrix} = 0 \qquad \text{or} \qquad \mathbf{A}^t\mathbf{a}^t + \mathbf{I}_{n-m}\bar{\mathbf{c}}^t = 0$$

This implies that $\bar{\mathbf{c}} = \mathbf{a}\mathbf{A}$. Therefore,

$$\mathbf{c} = (\mathbf{a} \quad \bar{\mathbf{c}}) = (\mathbf{a}\mathbf{I}_m \quad \mathbf{a}\mathbf{A}) = \mathbf{a}(\mathbf{I}_m \quad \mathbf{A}) = \mathbf{a}\mathbf{G}$$

showing thereby that c is the code word corresponding to the message word a in the code defined by the generator matrix $\mathbf{G}$.

This proves that codes defined by the parity check matrix $\mathbf{H}$ and the generator matrix $\mathbf{G}$ are identical.

Suppose that to the generator matrix $\mathbf{G} = (\mathbf{I}_m \quad \mathbf{A})$ corresponds another parity check matrix $\mathbf{H}_1 = (\mathbf{B} \quad \mathbf{I}_{n-m})$. Let e^i be the message word with 1 in the ith position and 0 everywhere else. The corresponding code word is $\mathbf{e}^i\mathbf{G}$, i.e. the ith row of $\mathbf{G}$. We may write $\mathbf{e}^i\mathbf{G} = (\mathbf{e}^i \quad \tilde{\mathbf{e}}^i)$ where $\tilde{\mathbf{e}}^i$ is the ith row of $\mathbf{A}$. Since $\mathbf{H}_1$ is a parity check matrix of the code defined by $\mathbf{G}$,

$$\mathbf{H}_1(\mathbf{e}^i \quad \tilde{\mathbf{e}}^i)^t = 0$$

or

$$(\mathbf{B} \quad \mathbf{I}_{n-m})\begin{pmatrix} (\mathbf{e}^i)^t \\ (\tilde{\mathbf{e}}^i)^t \end{pmatrix} = 0$$

or

$$\mathbf{B}(\mathbf{e}^i)^t + (\tilde{\mathbf{e}}^i)^t = 0$$

so that $(\tilde{\mathbf{e}}^i)^t = \mathbf{B}(\mathbf{e}^i)^t$ matches the ith column of $\mathbf{B}$ and $\tilde{\mathbf{e}}^i$ matches the ith row of $\mathbf{B}^t$. Hence the ith row of $\mathbf{A}$ equals the ith column of $\mathbf{B}$. Since this is true for every i, $1 \leq i \leq m$, we have $\mathbf{B} = \mathbf{A}^t$ and so, $\mathbf{H}_1 = \mathbf{H}$. Hence, corresponding to a given generator matrix $\mathbf{G}$, there corresponds a uniquely determined parity check matrix $\mathbf{H} = (\mathbf{A}^t \quad \mathbf{I}_{n-m})$.

If we had started with a given parity check matrix $\mathbf{H}$, the above argument shows that the corresponding generator matrix is also uniquely determined.

Exercise 1.2

1. Proceeding by first principles (i.e. without using the above theorem) obtain the parity check matrices of the matrix codes given by the following

generator matrices:

(a)

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

(b)

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

(c)

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

(d)

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

(e)

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

2. Determine the number of errors that are (a) detected, and (b) corrected by the matrix codes defined by the generator matrices given in question 1 above.
3. Define a code $E: \mathbb{B}^3 \to \mathbb{B}^6$ with the parity check matrix

(a)

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

(b)

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