ENEE 420
FALL 2012
COMMUNICATIONS SYSTEMS

ERROR CONTROL AND CODING: LINEAR BLOCK CODES

Linear block codes

A (n,k)-code $C : \mathcal{H}_k \to \mathcal{H}_n$ is a *linear* (block) code if its codebook $\mathcal{C}$ is a *linear* subspace of $\mathcal{H}_n$, i.e., for arbitrary $\boldsymbol{c}$ and $\boldsymbol{c}'$ in $\mathcal{C}$, the vector $\boldsymbol{c}+\boldsymbol{c}'$ is also an element of $\mathcal{C}$. There are many codes (as encoding mappings) which can be used to realize the same codebook. In the case of linear codes, implementations are available which are quite convenient as we now discuss.

All vectors are row vectors and all matrices have entries in $\{0,1\}$. All matrix calculations are done in modulo-2 arithmetic.

With $\boldsymbol{P} \equiv (p_{ij})$ a matrix of dimension $k \times (n-k)$, we construct the *generating* matrix $\boldsymbol{G} \equiv (g_{ij})$ given by

$$\boldsymbol{G} = [\boldsymbol{P} \mid \boldsymbol{I}_k] \,.$$

The matrix $\boldsymbol{G}$ has dimensions $k \times n$.

The generating matrix $\boldsymbol{G}$ defines a *linear* mapping $C_{\boldsymbol{G}} : \mathcal{H}_k \to \mathcal{H}_n$ given by

$$\boldsymbol{x} = C_{\boldsymbol{G}}(\boldsymbol{m}) = \boldsymbol{m}\boldsymbol{G}, \quad \boldsymbol{m} \in \mathcal{H}_k.$$

Whenever this mapping is one-to-one, it can be used to define a (n,k)-code whose codebook is the collection $\mathcal{C}_{\boldsymbol{G}}$ given by

$$\mathcal{C}_{\boldsymbol{G}} = \{\boldsymbol{m}\boldsymbol{G},\ \boldsymbol{m} \in \mathcal{H}_k\} \,.$$

It is plain that $\mathcal{C}_{\boldsymbol{G}}$ is a linear subspace of $\mathcal{H}_n$ and $C_{\boldsymbol{G}}$ is therefore a linear code.

With information vector $\boldsymbol{m}$ in $\mathcal{H}_k$, we associate the codeword $\boldsymbol{c}$ in $\mathcal{H}_n$ given by

$$\boldsymbol{c} = \boldsymbol{m}\boldsymbol{G}.$$

Using the form of the generating matrix $\boldsymbol{G}$, this codeword can be decomposed as

$$\boldsymbol{c} = (\boldsymbol{b}, \boldsymbol{m})$$

with $\boldsymbol{b}$ being the element of $\mathcal{H}_{n-k}$ given by

$$\boldsymbol{b} = \boldsymbol{m}\boldsymbol{P}.$$

This vector is known as the vector of *parity bits* associated with message $\boldsymbol{m}$. By construction this code is in systematic form.

The *syndrome* matrix $\boldsymbol{H} \equiv (h_{ij})$ is the $(n-k) \times n$ matrix given by

$$\boldsymbol{H} = \left[\boldsymbol{I}_{n-k} \mid \boldsymbol{P}^t\right].$$

It plays an essential role in implementing the decoding operations associated with the code $\mathcal{G}_{\boldsymbol{G}}$.

Lemma 0.1 *For any linear block code C with generating matrix $\boldsymbol{G}$, we have*

$$\boldsymbol{H}\boldsymbol{G}^t = \boldsymbol{O}_{(n-k)\times k}.$$

Proof. Applying the definitions of the matrices $\boldsymbol{G}$ and $\boldsymbol{H}$ we get

$$\begin{aligned} \boldsymbol{H}\boldsymbol{G}^t &= \left[\boldsymbol{I}_{n-k} \mid \boldsymbol{P}^t\right] \left[\boldsymbol{P} \mid \boldsymbol{I}_k\right]^t \\ &= \boldsymbol{I}_{n-k}\boldsymbol{P}^t + \boldsymbol{P}^t\boldsymbol{I}_k \\ &= \boldsymbol{P}^t + \boldsymbol{P}^t \\ &= \boldsymbol{O}_{(n-k)\times k} \pmod 2. \end{aligned} \tag{1}$$

■

This last fact leads to the following simple way of checking whether an element of $\mathcal{H}_n$ is a codeword in $\mathcal{C}_{\boldsymbol{G}}$.

Lemma 0.2 *For any linear block code C with generating matrix $\boldsymbol{G}$, we have*

$$\mathcal{C}_{\boldsymbol{G}} = \{\boldsymbol{x} \in \mathcal{H}_n : \boldsymbol{x}\boldsymbol{H}^t = \boldsymbol{0}_{n-k}.\}$$

Proof. We need to show that $\mathcal{C}_{\boldsymbol{G}} = \mathcal{C}^\star_{\boldsymbol{H}}$ where for convenience we have set

$$\mathcal{C}^\star_{\boldsymbol{H}} = \{\boldsymbol{x} \in \mathcal{H}_n : \boldsymbol{x}\boldsymbol{H}^t = \boldsymbol{0}_{n-k}\}.$$

For any element $\boldsymbol{c}$ in $\mathcal{C}_{\boldsymbol{G}}$, there exists a message vector $\boldsymbol{m}$ in $\mathcal{H}_k$ such that $\boldsymbol{c} = \boldsymbol{m}\boldsymbol{G}$, whence

$$\begin{aligned} \boldsymbol{c}\boldsymbol{H}^t &= (\boldsymbol{m}\boldsymbol{G})\,\boldsymbol{H}^t \\ &= \boldsymbol{m}\left(\boldsymbol{G}\boldsymbol{H}^t\right) \\ &= \boldsymbol{m}\left(\boldsymbol{H}\boldsymbol{G}^t\right)^t \\ &= \boldsymbol{m}\left(\boldsymbol{O}_{(n-k)\times k}\right)^t \\ &= \boldsymbol{m}\boldsymbol{O}_{k\times(n-k)} \\ &= \boldsymbol{0}_{n-k} \pmod 2 \end{aligned} \tag{2}$$

upon making use of Lemma (0.1). This establishes the inclusion $\mathcal{C}_{\boldsymbol{G}} \subseteq \mathcal{C}^\star_{\boldsymbol{H}}$.

Conversely, pick $\boldsymbol{x}$ in $\mathcal{C}^\star_{\boldsymbol{H}}$. This element of $\mathcal{H}_n$ can always be written as $\boldsymbol{x} = (\boldsymbol{y}, \boldsymbol{z})$ for some $\boldsymbol{y}$ in $\mathcal{H}_{n-k}$ and $\boldsymbol{z}$ in $\mathcal{H}_k$. With this notation we get

$$\begin{aligned} \boldsymbol{0}_{n-k} &= \boldsymbol{x}\boldsymbol{H}^t \\ &= (\boldsymbol{y}, \boldsymbol{z})\left[\boldsymbol{I}_{n-k} \mid \boldsymbol{P}^t\right]^t \\ &= \boldsymbol{y} + \boldsymbol{z}\boldsymbol{P} \pmod 2 \end{aligned} \tag{3}$$

whence

$$\boldsymbol{y} = \boldsymbol{y} + \boldsymbol{y} + \boldsymbol{z}\boldsymbol{P} = \boldsymbol{z}\boldsymbol{P} \pmod 2.$$

As a result,

$$\boldsymbol{x} = (\boldsymbol{z}\boldsymbol{P}, \boldsymbol{z}) = \boldsymbol{z}\boldsymbol{G},$$

and $\boldsymbol{x}$ is the codeword associated with $\boldsymbol{z}$, i.e., $\boldsymbol{x}$ is an element of $\mathcal{C}_{\boldsymbol{G}}$. The reverse inclusion $\mathcal{C}^\star_{\boldsymbol{H}} \subseteq \mathcal{C}_{\boldsymbol{H}}$ is now established. ■

Minimum (Hamming) distance of linear codes

Consider a linear code with generating matrix $\boldsymbol{G}$. We now show that the minimum (Hamming) distance of this code C can be computed efficiently.

Lemma 0.3 *We have*

$$d_H(C) = \min\left(w_H(\boldsymbol{m}\boldsymbol{G}) :\ \boldsymbol{m} \in \mathcal{H}_k,\ \boldsymbol{m} \neq \boldsymbol{0}_k\right) \tag{4}$$

with

$$\begin{aligned} w_H(\boldsymbol{m}\boldsymbol{G}) &= w_H(\boldsymbol{m}\boldsymbol{P}) + w_H(\boldsymbol{m}) \\ &= \sum_{\ell=1}^{n-k}\left(\sum_{j=1}^{k} m_j p_{j\ell}\right)_{\text{mod } 2} + w_H(\boldsymbol{m}), \quad \boldsymbol{m} \in \mathcal{H}_k. \end{aligned} \tag{5}$$

Proof. Pick $\boldsymbol{m}$ and $\boldsymbol{m}'$ in $\mathcal{H}_k$. It is plain that

$$\begin{aligned} d_H(C_{\boldsymbol{G}}(\boldsymbol{m}), C_{\boldsymbol{G}}(\boldsymbol{m}')) &= d_H(\boldsymbol{m}\boldsymbol{G}, \boldsymbol{m}'\boldsymbol{G}) \\ &= w_H(\boldsymbol{m}\boldsymbol{G} - \boldsymbol{m}'\boldsymbol{G}) \\ &= w_H((\boldsymbol{m} - \boldsymbol{m}')\,\boldsymbol{G}). \end{aligned} \tag{6}$$

It is also the case that

$$\left\{ \boldsymbol{m} - \boldsymbol{m}', \quad \begin{array}{c} \boldsymbol{m} \neq \boldsymbol{m}' \\ \boldsymbol{m}, \boldsymbol{m}' \in \mathcal{H}_k \end{array} \right\} = \left\{ \boldsymbol{m} \in \mathcal{H}_k : \quad \begin{array}{c} \boldsymbol{m} \neq \boldsymbol{0}_k \\ \boldsymbol{m} \in \mathcal{H}_k \end{array} \right\}.$$

Using these facts we conclude that

$$\begin{aligned} d_H(C) &= \inf\left(d_H(C(\boldsymbol{m}), C(\boldsymbol{m}')), \quad \begin{array}{c} \boldsymbol{m} \neq \boldsymbol{m}' \\ \boldsymbol{m}, \boldsymbol{m}' \in \mathcal{H}_k \end{array} \right) \\ &= \inf\left(w_H((\boldsymbol{m} - \boldsymbol{m}')\boldsymbol{G}), \quad \begin{array}{c} \boldsymbol{m} \neq \boldsymbol{m}' \\ \boldsymbol{m}, \boldsymbol{m}' \in \mathcal{H}_k \end{array} \right) \\ &= \inf\left(w_H(\boldsymbol{m}\boldsymbol{G}), \quad \boldsymbol{m} \in \mathcal{H}_k,\ \boldsymbol{m} \neq \boldsymbol{0}_k \right), \end{aligned} \tag{7}$$

and (4) is established.

Next, for each $\boldsymbol{m}$ in $\mathcal{H}_k$, we have

$$\begin{aligned} w_H(\boldsymbol{m}\boldsymbol{G}) &= \sum_{\ell=1}^{n} (\boldsymbol{m}\boldsymbol{G})_\ell \\ &= \sum_{\ell=1}^{n-k} (\boldsymbol{m}\boldsymbol{G})_\ell + \sum_{i=1}^{k} m_i \\ &= \sum_{\ell=1}^{n-k} (\boldsymbol{m}\boldsymbol{P})_\ell + \sum_{i=1}^{k} m_i \end{aligned} \tag{8}$$

and (5) readily follows. ■

Parity bits

Wth positive integer p, for each $\boldsymbol{x}$ in $\mathcal{H}_p$ we set

$$\texttt{Par}(\boldsymbol{x}) = x_1 + \ldots + x_p \pmod 2.$$

Thus $\texttt{Par}(\boldsymbol{x})$ is either 0 or 1, and we shall refer to it as the *(even) parity bit* associated with the information vector $\boldsymbol{x}$.

Let $\mathbf{1}_p$ denote the element in $\mathcal{H}_p$ whose p entries are identical and equal to 1, i.e.,

$$\mathbf{1}_p = (\underbrace{1, \ldots, 1}_{p \text{ times}}).$$

It is easy to check that

$$\texttt{Par}(\boldsymbol{x}) = \boldsymbol{x}\mathbf{1}_p^t \pmod 2$$

for each $\boldsymbol{x}$ in $\mathcal{H}_p$.

Single parity check (PBC) codes

Definitions – The (even) *parity bit check* (PBC) code can be defined as follows: With an information vector $\boldsymbol{m}$ in $\mathcal{H}_k$, we associate the codeword $\boldsymbol{c}$ in $\mathcal{H}_n$ given by

$$\boldsymbol{c} = (\texttt{Par}(\boldsymbol{m}), \boldsymbol{m}).$$

Obviously, $n = k + 1$. This is a linear block code with generating matrix $\boldsymbol{G}$ given by

$$\boldsymbol{G} = \left[\mathbf{1}_k^t | \boldsymbol{I}_k\right]$$

with the $k \times 1$ matrix $\boldsymbol{P}$ given by

$$\boldsymbol{P} = \mathbf{1}_k^t.$$

Consequently,

$$\mathcal{C}_{\rm PBC} = \left\{(\texttt{Par}(\boldsymbol{m}), \boldsymbol{m}),\ \boldsymbol{m} \in \mathcal{H}_k\right\}.$$

Structural properties – Here the matrix $\boldsymbol{H}$ is a $1 \times (k+1)$ matrix (thus a row vector) and takes the form

$$\boldsymbol{H} = [1|\mathbf{1}_k].$$

It is a simple matter to check membership in $\mathcal{C}_{\rm PBC}$: Pick $\boldsymbol{x}$ in $\mathcal{H}_n$, say of the form $\boldsymbol{x} = (y, \boldsymbol{z})$ with y in $\{0, 1\}$ and $\boldsymbol{z}$ in $\mathcal{H}_k$, and note that

$$\boldsymbol{x}\boldsymbol{H}^t = y + \boldsymbol{z}\mathbf{1}_k^t \pmod 2.$$

By Lemma 0.2 we conclude that $\boldsymbol{x} = (y, \boldsymbol{z})$ belongs to $\mathcal{C}_{\rm PBC}$ if and only if

$$y + \boldsymbol{z}\mathbf{1}_k^t = 0 \pmod 2.$$

Put differently, $\boldsymbol{x}$ belongs to $\mathcal{C}_{\rm PBC}$ if and only if $\mathtt{Par}(\boldsymbol{x}) = 0$, hence the characterization

$$\mathcal{C}_{\rm PBC} = \{\boldsymbol{x} \in \mathcal{H}_n : \mathtt{Par}(\boldsymbol{x}) = 0\}.$$

Note also that $\mathtt{Par}(\boldsymbol{x}) = 0$ for $\boldsymbol{x}$ in $\mathcal{H}_n$ is just another way to say that $w_H(\boldsymbol{x})$ is even when $\boldsymbol{x} \neq \mathbf{0}_n$.

Any codeword $\boldsymbol{c}$ is of the form $\boldsymbol{c} = (\mathtt{Par}(\boldsymbol{m}), \boldsymbol{m})$ for some $\boldsymbol{m}$ in $\mathcal{H}_k$, and we have

$$w_H(\mathtt{Par}(\boldsymbol{m}), \boldsymbol{m}) = \mathtt{Par}(\boldsymbol{m}) + w_H(\boldsymbol{m}). \tag{9}$$

By Lemma 0.3 we have

$$d_H(C_{\rm PBC}) = \min\left(\mathtt{Par}(\boldsymbol{m}) + w_H(\boldsymbol{m}) : \boldsymbol{m} \in \mathcal{H}_k,\ \boldsymbol{m} \neq \mathbf{0}_k\right). \tag{10}$$

It is plain that $d_H(C_{\rm PBC}) \geq 2$ – Just take $\boldsymbol{m}$ to have exactly one non-zero component. However, it is not possible to have $\mathtt{Par}(\boldsymbol{m}) + w_H(\boldsymbol{m}) = 1$ for some $\boldsymbol{m}$ in $\mathcal{H}_k$. Indeed, $\mathtt{Par}(\boldsymbol{m}) = 1$ implies $w_H(\boldsymbol{m}) = 0$, thus $\boldsymbol{m} = \mathbf{0}_k$ and this contradicts $\mathtt{Par}(\boldsymbol{m}) = 1$! Similarly, if $\mathtt{Par}(\boldsymbol{m}) = 0$, then $w_H(\boldsymbol{m}) = 1$ so that $\boldsymbol{m}$ has exactly one non-zero component. Again, a contradiction arises since such vector has parity $\mathtt{Par}(\boldsymbol{m}) = 1$. Consequently,

$$d_H(C_{\rm PBC}) = 2.$$

By earlier results we conclude that PBC codes can detect the occurence of a single error.

However more happens to be true. Indeed, we readily see that

$$\mathtt{Par}(\boldsymbol{c} + \boldsymbol{x}) = \mathtt{Par}(\boldsymbol{x}), \qquad \begin{matrix}\boldsymbol{c} \in \mathcal{C}_{\rm PBC} \\ \boldsymbol{x} \in \mathcal{H}_n.\end{matrix}$$

Therefore, for any codeword $\boldsymbol{c}$ in $\mathcal{C}_{\rm PBC}$, we get

$$\begin{aligned}
\mathcal{E}_{\rm PBC}(\boldsymbol{c}) &= \{\boldsymbol{e} \in \mathcal{H}_n : \boldsymbol{e} \neq \mathbf{0}_n,\ \boldsymbol{c} + \boldsymbol{e} \in \mathcal{C}_{\rm PBC}\} \\
&= \{\boldsymbol{e} \in \mathcal{H}_n : \boldsymbol{e} \neq \mathbf{0}_n,\ \mathtt{Par}(\boldsymbol{c} + \boldsymbol{e}) = 0\} \\
&= \{\boldsymbol{e} \in \mathcal{H}_n : \boldsymbol{e} \neq \mathbf{0}_n,\ \mathtt{Par}(\boldsymbol{e}) = 0\}. \qquad (11)
\end{aligned}$$

By a remark made earlier we can now conclude that

$$\mathcal{E}_{\rm PBC}(\boldsymbol{c}) = \{\, \boldsymbol{e} \in \mathcal{H}_n :\ \boldsymbol{e} \neq \mathbf{0}_n,\ w_H(\boldsymbol{e}) \text{ even}\} \,. \tag{12}$$

It now follows that PBC codes can detect any error pattern with an *odd* number of errors but will not be able to detect any pattern with an *even* number of errors – After all in this last case the the resulting vector still has zero parity.

Performance under the vector error model – Note that the set $\mathcal{E}_{\rm PBC}(\boldsymbol{c})$ is independent of the codeword $\boldsymbol{c}$, hence

$$\mathcal{E}_{\rm PBC}(\boldsymbol{c}) = \mathcal{E}_{\rm PBC}(\mathbf{0}_n), \quad \boldsymbol{c} \in \mathcal{C}_{\rm PBC}.$$

It is also easy to check that

$$|\mathcal{E}_{\rm PBC}(\mathbf{0}_n)| = 2^{n-1} - 1.$$

Therefore,

$$\mathrm{Err}(C_{\rm BPC}) = \frac{|\mathcal{E}_{\rm PBC}(\mathbf{0}_n)|}{2^n} = \frac{2^{n-1}-1}{2^n}$$

with

$$\lim_{n\to\infty} \mathrm{Err}(C_{\rm BPC}) = \frac{1}{2}.$$

Performance under the componentwise model – This time we get

$$\begin{aligned}
\mathrm{Err}(C_{\rm BPC}) &= \sum_{\boldsymbol{e}\in\mathcal{E}_{\rm PBC}(\mathbf{0}_n)} \alpha^{w_H(\boldsymbol{e})}(1-\alpha)^{n-w_H(\boldsymbol{e})} \\
&= \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} \left(\sum_{\boldsymbol{e}\in\mathcal{E}_{\rm PBC}(\mathbf{0}_n):\ w_H(\boldsymbol{e})=2k} \alpha^{w_H(\boldsymbol{e})}(1-\alpha)^{n-w_H(\boldsymbol{e})} \right) \\
&= \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2k} \alpha^{2k}(1-\alpha)^{n-2k} \\
&= \binom{n}{2}\alpha^2(1-\alpha)^{n-2} + \binom{n}{4}\alpha^4(1-\alpha)^{n-4} + \ldots \\
&\simeq \binom{n}{2}\alpha^2
\end{aligned}$$

where the last step requires $\alpha \ll 1$. In that case, only neigbhoring errors matter, i.e., the ones for which

$$w_H(\boldsymbol{e}) = 2.$$

Repetition codes

Here we assume that $n = 2p + 1$ for some positive integer p.

Definitions – A *repetition* code can be defined as follows: With an information bit m in $\{0, 1\}$, we associate the codeword $\boldsymbol{c}$ in $\mathcal{H}_n$ given by

$$\boldsymbol{c} = (\underbrace{m, \ldots, m.}_{2p \text{ times}} m)$$

Thus the bit m is repeated $2p$ times, hence the terminology. Obviously, $k = 1$ and $n = 2p + 1$. This is a linear block code with generating matrix $\boldsymbol{G}$ given by

$$\boldsymbol{G} = [\mathbf{1}_{2p}|1]$$

with the $1 \times 2p$ matrix $\boldsymbol{P}$ given by

$$\boldsymbol{P} = \mathbf{1}_{2p}.$$

Consequently, $\mathcal{C}_{\rm Rep} = \{\mathbf{0}_n, \mathbf{1}_n\}$, whence, $d_H(C_{\rm Rep}) = n$.

It is also easy to check for every $\boldsymbol{c}$ in $\mathcal{C}_{\rm Rep}$ that

$$\mathcal{E}_{\rm Rep}(\boldsymbol{c}) = \{\, \boldsymbol{e} \in \mathcal{H}_n : \ \boldsymbol{e} \neq \mathbf{0}_n, \ \boldsymbol{c} + \boldsymbol{e} \in \mathcal{C}_{\rm Rep}\} = \{\mathbf{1}_n\}.$$

Repetition codes have the message invariance property, so that $\mathcal{E}_{\rm Rep}(\mathbf{0}_n) = \mathcal{E}_{\rm Rep}(\mathbf{1}_n)$.

Performance under the vector error model – It is plain that

$$\mathrm{Err}(C_{\rm Rep}) = 2^{-n}.$$

Performance under the componentwise model – It is plain that

$$\mathrm{Err}(C_{\rm Rep}) = \alpha^n.$$

General linear codes

Consider a linear code with generating matrix $\boldsymbol{G}$.

Performance under the vector error model – It is plain that

$$\mathrm{Err}(C) = 2^{-n} \left| \mathcal{E}_C(\mathbf{0}_n) \right| . \tag{13}$$

Performance under the componentwise model – Write

$$\mathcal{E}_{C,k} = \{ \boldsymbol{e} \in \mathcal{E}_C(\mathbf{0}_n) : \ w_H(\boldsymbol{e}) = k \} , \quad k = 1, \ldots, n.$$

Upon noting

$$\mathcal{E}_C(\mathbf{0}_n) = \cup_{k=1}^n \mathcal{E}_{C,k},$$

we find

$$\begin{aligned}
\mathrm{Err}(C) &= \sum_{\boldsymbol{e} \in \mathcal{E}_C(\mathbf{0}_n)} \alpha^{w_H(\boldsymbol{e})} (1-\alpha)^{n - w_H(\boldsymbol{e})} \\
&= \sum_{k=1}^n \left(\sum_{\boldsymbol{e} \in \mathcal{E}_{C,k}} \alpha^{w_H(\boldsymbol{e})} (1-\alpha)^{n - w_H(\boldsymbol{e})} \right) \\
&= \sum_{k=1}^n \left(\sum_{\boldsymbol{e} \in \mathcal{E}_{C,k}} \alpha^{k} (1-\alpha)^{n-k} \right) \\
&= \sum_{k=1}^n \alpha^{k} (1-\alpha)^{n-k} \left| \mathcal{E}_{C,k} \right| \\
&= \sum_{k=d_H(C)}^n \alpha^{k} (1-\alpha)^{n-k} \left| \mathcal{E}_{C,k} \right| \qquad (14)
\end{aligned}$$

since

$$\mathcal{E}_{C,k} = \emptyset, \quad k = 1, \ldots, d_H(C) - 1.$$

Syndrome decoding

Consider a linear code with generating matrix $\boldsymbol{G}$.

Cosets – Given $\boldsymbol{x}$ in $\mathcal{H}_n$, we define the *coset* induced by $\boldsymbol{x}$ as the set $\texttt{Coset}(\boldsymbol{x})$ defined by

$$\texttt{Coset}(\boldsymbol{x}) = \{ \boldsymbol{x} + \boldsymbol{c}, \ \boldsymbol{c} \in \mathcal{C} \}.$$

It is plain that $\boldsymbol{x}$ is always a member of the coset $\texttt{Coset}(\boldsymbol{x})$ it induces. Note that all the elements in $\texttt{Coset}(\boldsymbol{x})$ are distinct, so that

$$|\texttt{Coset}(\boldsymbol{x})| = 2^k.$$

Furthermore, there are 2^{n-k} distinct cosets and they form a partition of $\mathcal{H}_n$. For distinct $\boldsymbol{x}$ and $\boldsymbol{y}$ in $\mathcal{H}_n$, either $\texttt{Coset}(\boldsymbol{x}) = \texttt{Coset}(\boldsymbol{y})$, or $\texttt{Coset}(\boldsymbol{x}) \neq \texttt{Coset}(\boldsymbol{y})$, with $\texttt{Coset}(\boldsymbol{x}) \cap \texttt{Coset}(\boldsymbol{y}) = \emptyset$ in the latter case.

Lemma 0.4 *With $\boldsymbol{x}$ and $\boldsymbol{y}$ in $\mathcal{H}_n$, we have*

$$\texttt{Coset}(\boldsymbol{x}) = \texttt{Coset}(\boldsymbol{y}) \tag{15}$$

if and only if

$$\boldsymbol{x}\boldsymbol{H}^t = \boldsymbol{y}\boldsymbol{H}^t. \tag{16}$$

As a consequence of Lemma 0.4 we conclude that

$$\texttt{Coset}(\boldsymbol{x}) = \left\{\boldsymbol{y} \in \mathcal{H}_n : \ \boldsymbol{y}\boldsymbol{H}^t = \boldsymbol{x}\boldsymbol{H}^t\right\}. \tag{17}$$

Proof. Pick $\boldsymbol{x}$ and $\boldsymbol{y}$ in $\mathcal{H}_n$ such that (15) holds. For any element $\boldsymbol{z}$ in this set, there exist $\boldsymbol{c}$ and $\boldsymbol{c}'$ in $\mathcal{C}$ such that $\boldsymbol{z} = \boldsymbol{x} + \boldsymbol{c}$ and $\boldsymbol{z} = \boldsymbol{y} + \boldsymbol{c}'$. By Lemma 0.1 we get

$$\boldsymbol{z}\boldsymbol{H}^t = (\boldsymbol{x} + \boldsymbol{c})\,\boldsymbol{H}^t = \boldsymbol{x}\boldsymbol{H}^t \pmod 2$$

and

$$\boldsymbol{z}\boldsymbol{H}^t = (\boldsymbol{y} + \boldsymbol{c}')\,\boldsymbol{H}^t = \boldsymbol{y}\boldsymbol{H}^t \pmod 2,$$

whence (16) holds.

Conversely, if $\boldsymbol{x}$ and $\boldsymbol{y}$ in $\mathcal{H}_n$ satisfy (16), then

$$(\boldsymbol{x} - \boldsymbol{y})\,\boldsymbol{H}^t = \boldsymbol{0}_{n-k} \pmod 2,$$

and by Lemma 0.2 we conclude that $\boldsymbol{c} = \boldsymbol{x} - \boldsymbol{y} \pmod 2$ is a codeword. This shows that $\boldsymbol{x} = \boldsymbol{y} + \boldsymbol{c}$ is an element of $\texttt{Coset}(\boldsymbol{y})$ so $\texttt{Coset}(\boldsymbol{x}) \subseteq \texttt{Coset}(\boldsymbol{y})$. By symmetry $\texttt{Coset}(\boldsymbol{y}) \subseteq \texttt{Coset}(\boldsymbol{x})$ and this completes the proof of (15). ■

Cosets and Nearest Neighbor decoding – Imagine that the message $\boldsymbol{m}$ in $\mathcal{H}_k$ is being transmitted over an imperfect channel. To that end, the linear block (n,k)-code $C : \mathcal{H}_k \to \mathcal{H}_n$ with generating matrix $\boldsymbol{G}$ is used to encode the message into the codeword $\boldsymbol{c} = \boldsymbol{m}\boldsymbol{G}$ in $\mathcal{H}_n$. After modulation/demodulation, the receiving end is provided with the vector $\boldsymbol{r}$ in $\mathcal{H}_n$. *Assume* that Nearest Neighbor decoding is used. This requires to find the estimate $\widehat{\boldsymbol{c}}_{\rm Near}$ which minimizes $d_H(\boldsymbol{r}, \boldsymbol{c}')$ with respect to $\boldsymbol{c}'$ in $\mathcal{C}$, or equivalently, $\widehat{\boldsymbol{c}}_{\rm Near}$ which minimizes $w_H(\boldsymbol{r} - \boldsymbol{c}')$ with respect to $\boldsymbol{c}'$ in $\mathcal{C}$. However, note that

$$\{\boldsymbol{r} - \boldsymbol{c}',\ \boldsymbol{c}' \in \mathcal{C}\} = \texttt{Coset}(\boldsymbol{r}).$$

Therefore, $\boldsymbol{r} - \widehat{\boldsymbol{c}}$ is that element in $\texttt{Coset}(\boldsymbol{r})$ with the smallest Hamming weight amongst the elements in $\texttt{Coset}(\boldsymbol{r})$. Thus, let $\widehat{\boldsymbol{x}}$ denote any element in $\texttt{Coset}(\boldsymbol{r})$ with smallest Hamming weight amongst the elements in $\texttt{Coset}(\boldsymbol{r})$. Thus, we can take $\widehat{\boldsymbol{c}}_{\rm Near}$ to be such that

$$\boldsymbol{r} - \widehat{\boldsymbol{c}}_{\rm Near} = \widehat{\boldsymbol{x}},$$

i.e.,

$$\widehat{\boldsymbol{c}}_{\rm Near} = \boldsymbol{r} - \widehat{\boldsymbol{x}}.$$

Nearest Neighbor decoding and the standard array – This observaton is implemented through the following *standard array* to be described shortly in further details: We construct a partition $\mathcal{H}_n$ into 2^{n-k} distinct cosets, say $C_1, \ldots, C_{2^{n-k}}$. These cosets are constructed recursively by identifying distinct elements $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{2^{n-k}}$ in $\mathcal{H}_n$ so that

$$C_\ell = \texttt{Coset}(\boldsymbol{x}_\ell), \quad \ell = 1, \ldots, 2^k$$

with $\boldsymbol{x}_\ell$ selected so that

$$w_H(\boldsymbol{x}_\ell) = \arg\min\left(\boldsymbol{x} \in C_\ell : w_H(\boldsymbol{x})\right), \quad \ell = 1, \ldots, 2^{n-k}.$$

Upon reception of the vector $\boldsymbol{r}$, its coset $\texttt{Coset}(\boldsymbol{r})$ is identified. This amounts to finding the unique integer $\ell = \ell(\boldsymbol{r})$ such that

$$\texttt{Coset}(\boldsymbol{r}) = C_\ell.$$

By construction $\boldsymbol{x}_\ell$ has smallest Hamming weight amongst the elements of the coset C_ℓ. According to the earlier discussion it then follows that $\widehat{\boldsymbol{c}}_{\rm Near}$ is determined through

$$\boldsymbol{r} - \widehat{\boldsymbol{c}}_{\rm Near} = \boldsymbol{x}_\ell$$

i.e.,

$$\widehat{\boldsymbol{c}}_{\rm Near} = \boldsymbol{r} - \boldsymbol{x}_\ell.$$

Constructing the standard array – To implement these ideas we construct the so-called standard array. To do so we label the codewords in $\mathcal{C}$, say $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_{2^{n-k}}$, with $\boldsymbol{c}_1 = \mathbf{0}_n$.

1. $\ell = 1$ – We take
$$\boldsymbol{x}_1 = \mathbf{0}_n$$
so that
$$C_1 = \texttt{Coset}(\boldsymbol{x}_1) = \mathcal{C}.$$
We automatically have
$$w_H(\boldsymbol{x}_1) = \min\left(w_H(\boldsymbol{x}), \quad \boldsymbol{x} \in C_1\right) = 0$$
so that $\boldsymbol{x}_1$ is indeed the smallest Hamming weight amongst the elements of C_1. We visualize this coset as a row; see below.

$\texttt{Coset}(\mathbf{0}_n)$	$\mathbf{0}_n$	$\boldsymbol{c}_2$	$\boldsymbol{c}_3$	$\ldots$	$\boldsymbol{c}_j$	$\ldots$	$\boldsymbol{c}_{2^k}$

2. $\ell = 2$ – Next, consider the complement $C_1^\star$ of C_1, namely
$$C_1^\star = \mathcal{H}_n - C_1,$$
and select $\boldsymbol{x}_2$ to be any element in $C_1^\star$ with minimum Hamming weight, i.e.,
$$\boldsymbol{x}_2 = \arg\min\left(\boldsymbol{x} \in C_1^\star : \ w_H(\boldsymbol{x})\right).$$
We then define
$$C_2 = \texttt{Coset}(\boldsymbol{x}_2).$$
By construction $\boldsymbol{x}_2$ has the smallest Hamming weight amongst all the elements of C_2, i.e.,
$$w_H(\boldsymbol{x}_2) \leq w_H(\boldsymbol{x}), \quad \boldsymbol{x} \in \texttt{Coset}(\boldsymbol{x}_2)$$
since $\texttt{Coset}(\boldsymbol{x}_2) \cap \texttt{Coset}(\boldsymbol{x}_1) = \emptyset$ (due to the fact that $\boldsymbol{x} - 2$ is not an element of C_1. We visualize C_1 and C_2 as successive rows in a table in formation; see below.

$\texttt{Coset}(\mathbf{0}_n)$	$\mathbf{0}_n$	$\boldsymbol{c}_2$	$\boldsymbol{c}_3$	$\ldots$	$\boldsymbol{c}_j$	$\ldots$	$\boldsymbol{c}_{2^k}$
$\texttt{Coset}(\boldsymbol{x}_2)$	$\boldsymbol{x}_2+\mathbf{0}_n$	$\boldsymbol{x}_2+\boldsymbol{c}_2$	$\boldsymbol{x}_2+\boldsymbol{c}_3$	$\ldots$	$\boldsymbol{x}_2+\boldsymbol{c}_j$	$\ldots$	$\boldsymbol{x}_2+\boldsymbol{c}_{2^k}$

3. The generic step – This procedure is repeated: For $\ell = j$ for some $j = 1, \ldots, 2^{n-k}$, assume that $C_1, \ldots, C_{\ell-1}$ have been costructed. Consider the complement $C_j^\star$ of $\cup_{s=1}^{\ell-1} C_s$, i.e.

$$C_\ell^\star = \mathcal{H}_n - \left(\cup_{i=1}^{\ell-1} C_i\right),$$

and select $\boldsymbol{x}_\ell$ to be an element in $C_\ell^\star$ with minimum Hamming weight, i.e.,

$$\boldsymbol{x}_\ell = \arg\min\left(w_H(\boldsymbol{x}) : \ \boldsymbol{x} \in C_\ell^\star\right).$$

We then define

$$C_\ell = \texttt{Coset}(\boldsymbol{x}_\ell).$$

By construction $\boldsymbol{x}_\ell$ has the smallest Hamming weight amongst the elements C_ℓ, i.e.,

$$w_H(\boldsymbol{x}_\ell) \le w_H(\boldsymbol{x}), \quad \boldsymbol{x} \in \texttt{Coset}(\boldsymbol{x}_\ell).$$

The final table or array has the following form. Note that each row is a coset and that the *first* element of that row has minimum Hamming weight amongs all the elements in that row. For that reason, the elements $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{2^{n-k}}$ are called the *leaders* of the cosets to which they belong.

$\texttt{Coset}(\mathbf{0}_n)$	$\mathbf{0}_n$	$\boldsymbol{c}_2$	$\boldsymbol{c}_3$	$\ldots$	$\boldsymbol{c}_j$	$\ldots$	$\boldsymbol{c}_{2^k}$
$\texttt{Coset}(\boldsymbol{x}_2)$	$\boldsymbol{x}_2+\mathbf{0}_n$	$\boldsymbol{x}_2+\boldsymbol{c}_2$	$\boldsymbol{x}_2+\boldsymbol{c}_3$	$\ldots$	$\boldsymbol{x}_2+\boldsymbol{c}_j$	$\ldots$	$\boldsymbol{x}_2+\boldsymbol{c}_{2^k}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\texttt{Coset}(\boldsymbol{x}_\ell)$	$\boldsymbol{x}_\ell+\mathbf{0}_n$	$\boldsymbol{x}_\ell+\boldsymbol{c}_2$	$\boldsymbol{x}_\ell+\boldsymbol{c}_3$	$\ldots$	$\boldsymbol{x}_\ell+\boldsymbol{c}_j$	$\ldots$	$\boldsymbol{x}_\ell+\boldsymbol{c}_{2^k}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\texttt{Coset}(\boldsymbol{x}_{2^{n-k}})$	$\boldsymbol{x}_{2^{n-k}}+\mathbf{0}_n$	$\boldsymbol{x}_{2^{n-k}}+\boldsymbol{c}_2$	$\boldsymbol{x}_{2^{n-k}}+\boldsymbol{c}_3$	$\ldots$	$\boldsymbol{x}_{2^{n-k}}+\boldsymbol{c}_j$	$\ldots$	$\boldsymbol{x}_{2^{n-k}}+\boldsymbol{c}_{2^k}$