Decoding with a linear code

Let $C \subseteq V(n,q)$ be a linear code. The cosets of $C$ are subsets of $V(n,q)$ of the form $\overrightarrow{a} + C$. Here $\overrightarrow{a} \in V(n,q)$ is fixed, and

$$\overrightarrow{a} + C = \{ \overrightarrow{a} + \overrightarrow{c} \mid \overrightarrow{c} \in C \}.$$

Note that sometimes $\overrightarrow{a} + C = \overrightarrow{b} + C$ even if $\overrightarrow{a} \neq \overrightarrow{b}$.

**Theorem:** (a) $\overrightarrow{x}$ and $\overrightarrow{y}$ belong to same coset of $C$ if and only if $\overrightarrow{y} - \overrightarrow{x} \in C$.

(b) If $\overrightarrow{x} + C \neq \overrightarrow{y} + C$, then

$$\overrightarrow{x} + C \cap \overrightarrow{y} + C = \emptyset.$$

(c) Assume $\dim(C) = k$, i.e. $|C| = q^k$.

Then $|\overrightarrow{a} + C| = q^k$.

(d) $C$ has $q^{n-k}$ cosets. These cosets partition $V(n,q)$. 
Proof: (a) Suppose \( \vec{x}, \vec{y} \in \vec{a} + C \) for some \( \vec{a} \in C \). In other words,
\[
\vec{x} = \vec{a} + \vec{c}_1 \quad (1)
\]
\[
\vec{y} = \vec{a} + \vec{c}_2 \quad (2)
\]
Subtract (1) from (2): \( \vec{y} - \vec{x} = \vec{c}_2 - \vec{c}_1 \in C \), as claimed.

Conversely, suppose \( \vec{y} - \vec{x} = \vec{c} \in C \). Then \( \vec{y} = \vec{x} + \vec{c} \), so both \( \vec{x} = \vec{x} + \vec{0} \) and \( \vec{y} = \vec{x} + \vec{c} \) belong to the same coset, \( \vec{x} + C \).

(b) If \( \vec{y} - \vec{x} = \vec{c} \) lies in \( C \), then every element of the form \( \vec{y} + \vec{c} \) can be written as \( \vec{x} + (\vec{c} + \vec{c}) = \vec{x} + \vec{c} \).
Thus $\vec{y} + C \subseteq \vec{x} + C$.

Similarly, every element of the form $\vec{x} + \vec{c}$ can be rewritten as $\vec{y} + (\vec{c} - \vec{z}) = \vec{y} + \vec{c''}$, where $\vec{c''} \in C$.
Thus $\vec{x} + C \subseteq \vec{y} + C$, and we conclude that $\vec{x} + C = \vec{y} + C$.

Now assume $\vec{z} = \vec{y} - \vec{x}$ does not lie in $C$. Then we want to show that $\vec{x} + C$ and $\vec{y} + C$ have no words in common. Assume the contrary:

$\vec{x} + \vec{c}_1 = \vec{y} + \vec{c}_2$ for some $\vec{c}_1, \vec{c}_2 \in C$.

Then $\vec{y} - \vec{x} = \vec{c}_1 - \vec{c}_2 \in C$, a contradiction.

(c) Let $C = \langle \vec{c}_1, \vec{c}_2, \ldots, \vec{c}_k \rangle$. Then $\vec{a} + C = \langle \vec{a} + \vec{c}_1, \ldots, \vec{a} + \vec{c}_k \rangle$, and $\vec{a} + \vec{c}_i \neq \vec{a} + \vec{c}_j$ if $\vec{c}_i \neq \vec{c}_j$. Thus $|\vec{a} + C| = k$. 

$|\vec{a} + C| = q^k$. 

Every word in $V(n, q)$ is in some coset: $\overrightarrow{x} \in \overrightarrow{x} + C$. By (6), this tells us that the cosets of $C$ partition $V(n, q)$. By (c) each coset has $q^k$ words. Thus

$$\text{# of cosets of } C = \frac{|V(n, q)|}{q^k} = \frac{q^n}{q^k} = q^{n-k}.$$ 

This completes the proof of the theorem.

Recall, that if a word $\overrightarrow{x} \in C$ is sent and the word $\overrightarrow{y} \in V(n, q)$ is received, then the transmission error $\overrightarrow{e} = \overrightarrow{y} - \overrightarrow{x}$ lies in some coset as $\overrightarrow{y}$, i.e. in the coset $\overrightarrow{y} + C = \overrightarrow{e} + C$. To find $\overrightarrow{e}$ we look for the word of smallest weight in coset $\overrightarrow{y} + C$.

To help us do this, let us put together the info we need about
the cosets of $C$ into a table, called standard (or Slepian) array of $C$. Cosets are written as rows, starting from coset leader which is a word of minimal weight in its coset.

Example: $C = \{(0,0,0,0,0), (1,0,1,1,0), (0,1,1,0,1), (1,1,0,1,1)\} \subset V(5,2)$. Note that $C$ is linear with generator matrix

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

$C$ has $q^{n-k}$ cosets, where $q = 2$, $n = 5$, $k = \dim(C) = 2$.

Standard array for $C$ will have 4 columns, 8 rows.

$d(C) = 3$
<table>
<thead>
<tr>
<th>Coset Leader</th>
<th>Rest of coset</th>
</tr>
</thead>
<tbody>
<tr>
<td>(0,0,0,0,0)</td>
<td>(0,1,1,0), (0,1,1,0,1), (1,1,0,1,1)</td>
</tr>
<tr>
<td>(1,0,0,0,0)</td>
<td>(0,0,1,1,0), (1,1,1,0,1), (0,1,0,1,1)</td>
</tr>
<tr>
<td>(0,1,0,0,0)</td>
<td>(1,1,1,1,0), (0,0,1,0,1), (1,0,0,1,1)</td>
</tr>
<tr>
<td>(0,0,1,0,0)</td>
<td>(1,0,0,1,0), (0,0,0,0,1), (1,1,1,1,1)</td>
</tr>
<tr>
<td>(0,0,0,1,0)</td>
<td>(1,0,1,0,0), (0,1,1,1,1), (1,1,0,0,1)</td>
</tr>
<tr>
<td>(0,0,0,0,1)</td>
<td>(1,0,1,1,1), (0,1,0,0,0), (1,1,0,1,0)</td>
</tr>
<tr>
<td>(1,1,0,0,0)</td>
<td>(0,1,1,1,0), (1,0,1,0,1), (0,0,0,1,1)</td>
</tr>
<tr>
<td>(1,0,0,0,1)</td>
<td>(0,0,1,1,1), (1,1,1,0,0), (0,1,0,1,0)</td>
</tr>
</tbody>
</table>

Another possible coset leader.

**Decode:** Received word: (0,1,1,1,1) = \( \bar{y} \)  
Coset Reader: \( \bar{e} = (0,0,0,1,0) = \text{error} \)  
Decode \( \bar{y} \) as \( \bar{x} = \bar{y} - \bar{e} = (0,1,1,0,1) \)
Syndrome Decoding

Let $C \subseteq V(n,q)$ be a linear code with parity check matrix $H$.

The syndrome of a word $\overrightarrow{x} \in V(n,q)$ is $\overrightarrow{x} \cdot H^T = (a_1, \ldots, a_{n-k}) = S(\overrightarrow{x})$

$1 \times n \quad n \times (n-k)$

Here $a_i = \text{dot product of } \overrightarrow{x} \text{ with Row } i \text{ of } H$.

By definition of $H$, $\overrightarrow{x}$ lies in $C$ iff $S(\overrightarrow{x}) = \overrightarrow{0}$.

Lemma: (a) $S(\overrightarrow{x} + \overrightarrow{y}) = S(\overrightarrow{x}) + S(\overrightarrow{y})$

(b) $S(\overrightarrow{x}) = S(\overrightarrow{y})$ if and only if $\overrightarrow{x}$, $\overrightarrow{y}$ lie in same coset of $C$.

Proof: (a) $S(\overrightarrow{x} + \overrightarrow{y}) = (\overrightarrow{x} + \overrightarrow{y}) \cdot H^T$

$\quad = \overrightarrow{x} \cdot H^T + \overrightarrow{y} \cdot H^T = S(\overrightarrow{x}) + S(\overrightarrow{y})$
(b) \( S(\overrightarrow{x}) = S(\overrightarrow{y}) \iff \overrightarrow{S(x - y)} = \overrightarrow{0} \iff \overrightarrow{x - y} \in C \iff \overrightarrow{x}, \overrightarrow{y} \) lie in same coset of \( C \).

---

 Syndrome decoding (incomplete).

- Choose coset leaders of weight \( < \frac{d(c)}{2} \).

- Precompute their syndromes (syndrome look-up table).

- If received word is \( \overrightarrow{y} \), compute \( S(\overrightarrow{y}) \) and match it to \( S(\overrightarrow{e}) \) for a suitable coset leader \( \overrightarrow{e} \).

- Now \( \overrightarrow{e} \) becomes error word, decode \( \overrightarrow{y} \) as \( \overrightarrow{x} = \overrightarrow{y} - \overrightarrow{e} \).

Note: \( S(\overrightarrow{x}) \) depends on choice of \( H \).

Need to choose \( H \) ahead of time.
Back to our example:

$C = V(5, 2)$

Generator matrix:

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

Parity check matrix:

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

**Syndrome lookup table**

<table>
<thead>
<tr>
<th>Coset leader</th>
<th>Syndrome</th>
</tr>
</thead>
<tbody>
<tr>
<td>00000</td>
<td>000</td>
</tr>
<tr>
<td>10000</td>
<td>110</td>
</tr>
<tr>
<td>01000</td>
<td>101</td>
</tr>
<tr>
<td>00100</td>
<td>100</td>
</tr>
<tr>
<td>00010</td>
<td>010</td>
</tr>
<tr>
<td>00001</td>
<td>001</td>
</tr>
</tbody>
</table>
Received word: $\overline{y} = (0, 1, 1, 1, 1)$

$S(\overline{y}) = (0, 1, 0)$

Matches to coset leader

$\overline{e} = (0, 0, 0, 1, 0)$

Decode $\overline{y}$ as $\overline{x} = (0, 1, 1, 0, 1)$

$= \overline{y} - \overline{e}$.

Another received word:

$\overline{y} = (0, 0, 1, 1, 1)$.

$S(\overline{y}) = (1, 1, 1, 1)$.

Does not match to $S(\overline{e})$ for any coset leader $\overline{e}$ in table.

Declare an error.
Received word: $\vec{y} = (0,0,1,1,1)$
Coset leader: $\vec{e} = (0,0,0,0)$ = error.
Decode $\vec{y}$ as $\vec{x} = \vec{y} - \vec{e} = (1,0,1,1,0)$.

Incomplete decoding:

Use only cosets that have a unique coset leader. These are coset leaders of weight $< \frac{d(C)}{2}$.

In all other cases declare an error. In above example, declare an error if $\vec{y}$ is in last 2 rows.