9 Syndrome decoding

In this lecture we show how the inner parity matrix can be used to accelerate our decoding procedure.

Definition of syndrome. Let $C \subseteq V$ be an $F$ linear code with parity check matrix $H$. For $y \in V$ the syndrome of $y$, denoted $S(y)$, is

$$S(y) = yH^T.$$ 

Remark.

1. By Proposition 20, $S(y) = 0$ if and only if $y \in C$.
2. $S$ is a linear map $S : V \longrightarrow F^{(n-k)}$.

$$S(\lambda y + \mu z) = \lambda S(y) + \mu S(z).$$

The key property of the syndrome map is:

Lemma 22 $S(y) = S(z)$ if and only if $y - z \in C$, which happens if and only if $y$ and $z$ are in the same coset.

Proof. $S(y) = S(z)$ if and only if $S(y - z) = 0$ (linearity). By (1) above this is if and only if $y - z \in C$. The second part follows from the definition of coset. □

Next we see how this helps us with our standard array decoding algorithm: indeed, from the above it follows that now we only need to store the coset leaders $\{a_i\}$ together with their syndrome values $\{S(a_i)\}$.

The algorithm is now, given received vector $\underline{y}$:

Step 1. Calculate $S(\underline{y})$.

Step 2. Find the $a_i$ with $S(a_i) = S(\underline{y})$. (By the lemma above it follows that $\underline{y} \in a_i + C$.)

Step 3. Decode $\underline{y}$ as $\underline{y} - a_i$. (Recall that $a_i$ is assumed to be the error).

Note that the above procedure runs without explicit reference to the various cosets; however, we do need to know these cosets in detail at some point, in order to determine the coset leaders.
10 Incomplete decoding

(Not covered this year)

The following efficient procedure is a mixture of both decoding and error detection.

Let $C$ be $[n, k, d]$ $F$-code with $d = 2t + 1$ or $2t + 2$; then by a result from the previous lectures we know that if a received vector $y$ has at most $t$ errors in it, then it can be correctly decoded by a nearest neighbour algorithm. Recall that our standard array technique is such an algorithm. On the other hand, for more than $t$ errors our procedure may well decode incorrectly.

These conditions suggest that we modify the procedure as follows:

Step 1. Given a received vector $y$, calculate the syndrome $S(y)$.

Step 2. Find the unique coset leader $a_i$ with $S(a_i) = S(y)$. (Recall that $a_i$ is taken to be the error). So if $w(a_i) \leq t$, then we take $x = y - a_i$ as the (unique) nearest neighbour decode of $y$. (Note: this decode of $y$ will be correct if $y$ contains $\leq t$ errors, since $x$ is the (unique) nearest neighbour).

Step 3. If $w(a_i) > t$, then $y$ may well have several nearest neighbours; so we seek re-transmission.

We illustrate the idea of incomplete decoding with the ISBN code.

Example 2. Consider the parity check matrix:

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{bmatrix} = \begin{bmatrix} s_1 \\ s_2 \end{bmatrix}.$$  

This has row rank 2, so determines a $[10, 8]$ code $C$ given by all $x$ which satisfy the equations

$$\sum_{i=1}^{10} x_i = 0$$

and

$$\sum_{i=1}^{10} ix_i = 0$$

in $F_{11}$.

For practical purposes, recall that we usually work with the non-linear sub-code $D$ in which $x_i \leq 9$ for each $i < 10$. Note also that this is only a subcode of the ISBN code. The ISBN code is defined by the one-line parity check matrix

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{bmatrix}.$$  

We add the extra line in order to allow the correction of a single error and to make the example more interesting.

We now describe an incomplete syndrome decode for $D$ which

(a) corrects any single error,

(b) detects any double error arising from transposition.
As usual $x$ denotes the transmitted codeword, and $y$ the received vector. The syndrome of $y$ is given by

$$S(y) = (y \cdot s_1, y \cdot s_2)$$

$$= \left( \sum_{i=1}^{10} y_i, \sum_{i=1}^{10} i y_i \right)$$

$$= (A, B), \text{ say.}$$

Suppose first that a single error occurs:

$$C = \left\{ \begin{array}{ll}
y_j &= x_j + k & \text{some } j, \text{ some } k \neq 0 \\
y_i &= x_i & \text{for each } i \neq j
\end{array} \right.$$  

Then

$$A = \sum_{i=1}^{10} y_i$$

$$= \sum_{i=1}^{10} x_i + k \equiv k \pmod{11}$$

$$B = \sum_{i=1}^{10} i y_i$$

$$= \sum_{i=1}^{10} i x_i + j k \equiv jk \pmod{11}$$

and $A, B$ are both non-zero: the magnitude of the error is given by $A$ and, provided the error $\neq 0$, the position of the error is given by $j = \frac{k j}{k} = \frac{B}{A}$.

Remember that we have seen that the ISBN code detects transposition, thus this subcode will certainly do so too. The above work suggests the following incomplete syndrome decode:

**Step 1.** Given $y$ determine $S(y) = (A, B)$. If $(A, B) = 0$ assume no error.

**Step 2.** If $A \neq 0, B \neq 0$ then assume 1 error of magnitude $A$ in the $B/A$ position.

**Step 3.** If $AB = 0$ but $(A, B) \neq (0, 0)$ then we have detected at least 2 errors. For, by the above, no errors gives $(A, B) = (0, 0)$ and 1 error gives $AB \neq 0$.

So in this case we seek retransmission.

**Note:** Step 3 will arise if a transposition of 2 different numbers has occurred; we proved this in example sheet one, under a slight disguise.