6 more lectures in this class:

Tue, March 19
Th., March 21
Tue, March 26 — Problem Set 5 due
Th., March 28
Tue, April 2
Th., April 4 — Problem Set 6 due

Binary Hamming codes

Fix $r \geq 2$, integer. Hamming code $C = \text{Ham}(r, 2)$ is given by parity check matrix $H$. $H$ has $r$ rows. The columns of $H$ are all non-zero binary words of length $r$. 
Ex: \( r=2 \)  \( H = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \)  \( n=3 \)

\[ r=3 \]
\[ H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \]  \( n=7 \)

For general \( r \), \( H \) has \( n \) columns, where \( n=2^r-1 \). The code \( C \) depends on how we order the columns of \( H \). Thus Ham \((r,2)\) is not a single code but rather a family of equivalent codes.

One way to order the columns is to start with \((\frac{1}{2})\), \((\frac{0}{2})\), ..., \((\frac{0}{n})\) so that \( H \) is in standard form. In particular, this shows that rows of \( H \) are linearly independent, so that \( H \) really is a parity check matrix. Same is true for any ordering of the columns.
I will order columns of $H$ so that the $i$th column spells "i" in binary, as in the two examples above.

For example, 001 is 1 in binary
010 is 2 in binary
011 is 3 in binary
111 is 7 in binary

Properties of $C = \text{Ham}(r, 2)$.

(a) $n = \text{Length of } C = 2^r - 1$

(b) $\dim(C) = n - r = 2^r - 1 - r = k$

$|C| = 2^{\dim(C)} = 2^{(2^r - 1 - r)} = 2^{n-r}$

(c) $d(C) = 3$

(d) $C$ is a perfect code.
Proof of (c): \( d(C) \leq 3 \) because
\[
\begin{pmatrix}
0 \\
0 \\
1
\end{pmatrix} +
\begin{pmatrix}
0 \\
1 \\
0
\end{pmatrix} +
\begin{pmatrix}
0 \\
0 \\
1
\end{pmatrix} =
\begin{pmatrix}
0 \\
0 \\
1
\end{pmatrix}
\]
\( \text{Col} 1 + \text{Col} 2 + \text{Col} 3 = 0 \). Thus \( H \) has 3 linearly dependent columns.

No zero column: \( d(C) \geq 2 \)
No two columns are equal
(and thus no two are linearly dependent)

We conclude that \( d(C) = 3 \).

Proof of (d): Recall that a code \( C \)
of length \( n \), min. dist. 3 is perfect if
\[
|C| = \frac{2^n}{1+n}.
\]
In our case \( n = 2^r - 1 \),

so \( \frac{2^n}{1+n} = \frac{2^n}{2^r} = 2^{n-r} \). By (6) \( |C| = 2^{n-r} \).

Thus \( C \) is perfect.
Example: If \( r = 3 \), then \( n = 2^{r-1} - 1 = 7 \).

\[ |C| = 2^{n-r} = 2^4 = 16. \]

Thus we recover a binary \((7, 16, 3)\)-code. Our previous construction of a \((7, 16, 3)\)-code relied on finite proj. plane.

Decoding with a binary Hamming Code

- Word sent: \( \overrightarrow{x} \in C \)
- Word received: \( \overrightarrow{y} \)

Error \( \overrightarrow{e} = \overrightarrow{y} - \overrightarrow{x} \). Know \( \overrightarrow{y} \).

Want to find \( \overrightarrow{x} \) or equivalently want to find \( \overrightarrow{e} \), \( \overrightarrow{x} = \overrightarrow{y} - \overrightarrow{e} \).

Compute \( S(\overrightarrow{y}) = \overrightarrow{y} \cdot H^T \).

\( (s_1, -s_r) \)
Examples with \( r = 3 \)

\[
H = \begin{pmatrix}
0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 1 & 1 & 0 & 0 & 1 & 1 \\
1 & 0 & 1 & 0 & 1 & 0 & 1
\end{pmatrix}
\]

(i) Received \( \vec{y} = (1,1,1,1,1,1,1) \)
Syndrome: \( S(\vec{y}) = (0,0,0) \).
Assume no error, \( \vec{x} = \vec{y} = (1,1,1,1,1,1) \).

(ii) \( \vec{y} = (1,1,0,0,0,0,0,0) \)
\( S(\vec{y}) = (0,1,1) \). 011 is the binary representation of 3. Assume 1 error in position 3, \( \vec{x} = (1,1,1,0,0,0,0,0) \).

(iii) \( \vec{y} = (0,0,0,0,0,0,1,1) \)
Syndrome \( S(\vec{y}) = (0,0,1) \).
Error position: 1, because 001 is the binary representation of 1.
\( \vec{x} = (1,0,0,0,0,1,1) \).
If $s(\vec{y}) = (0,\ldots,0)$, then assume that $\vec{e} = (0,\ldots,0)$ and $\vec{x} = \vec{y} - \vec{e} = \vec{y}$. In other words, assume no error.

If $s(\vec{y}) \neq (0,\ldots,0)$, assume one error. In other words, assume position $i$:

$\vec{e} = (0,\ldots,0,1,0,\ldots,0)$.

To find $i =$ error position, we match $s(\vec{y})$ to $s(\vec{e}) = (i$th column$)^T$ of $H$.

Can always do this, because every non-zero word of length $r$ occurs as one of the columns of $H$. In fact $s(\vec{y})$ spells $i =$ error position in binary.
Extended binary Hamming code $\hat{\text{Ham}}(r,2)$

Append an overall parity check digit to $\text{Ham}(r,2) = \mathcal{C}$.

Properties of $\hat{\text{Ham}}(r,2) = \hat{\mathcal{C}}$

1. $n = \text{Length of } \hat{\text{Ham}}(r,2)$
   \[= \text{Length of } \text{Ham}(r,2) + 1\]
   \[= (2^{r-1}) + 1 = 2^r\]

2. $|\hat{\mathcal{C}}| = |\mathcal{C}| = 2^{2^r - r - 1}$.

$\hat{\mathcal{C}}$ is linear (check!) of the same dimension as $\mathcal{C}$, $\dim(\hat{\mathcal{C}}) = \dim(\mathcal{C}) = 2^{2^r - r - 1}$.

3. $d(\hat{\mathcal{C}}) = 4$.

4. $\hat{\mathcal{C}}$ is not perfect. A perfect code has odd min. distance.
(V) \( \hat{C} \) can correct at most 1 error, same as \( C \). However, \( \hat{C} \) can detect up to 3 errors. It is better suited for error detection than \( C \).

A decoding scheme for \( \hat{C} \) using parity check matrix

\[
\tilde{H} = \begin{pmatrix}
H & 0 \\
1 & 1 & 1 & - & 1
\end{pmatrix}, \quad \text{(Check in HW problem)}
\]

\[
\tilde{x} = (x_1, \ldots, x_{2^r-1}, x_{2^r})
\]

Let us precompute the syndromes of the error words of position \( i \)

\[
\tilde{e}_i = (0, \cdots, 0, 1, 0, \cdots, 0)
\]

of weight 1.
\[ S(\bar{e}_i) = (s_1, -, s_r, 0, 1) \quad S(\bar{e}_{2^r}) = (0, 0, -, 0, 1) \]

if \( r = 1, 2, -, 2^r - 1 \).

Decoding scheme

Compute \( S(\bar{y}) = (s_1, -, s_r, s_{r+1}) \).

- If \( S(\bar{y}) = \bar{y} \), then assume no error, decode \( \bar{y} \) as \( \bar{x} = \bar{y} \).

- If \( (s_1, -, s_r) \neq \bar{y} \) and \( s_{r+1} = 1 \), then assume 1 error in first \( 2^r - 1 \) positions. \( (s_1, -, s_r) \) spells error position in binary.

- If \( (s_1, -, s_r) = \bar{y} \) but \( s_{r+1} = 1 \), assume 1 error in position \( 2^r \).

Decode \( \bar{y} \) as \( \bar{x} = \bar{y} - (0, 0, -, 0, 1) \).

- If \( (s_1, -, s_r) \neq \bar{y} \) but \( s_{r+1} = 0 \), then at least 2 errors occurred.

Ask for retransmission.