EC500

Design of Secure and Reliable Hardware

Lecture 6

Mark Karpovsky

Binary Hamming Codes $(n, 2^k, 3)$
$n = 2^r - 1,\ k = n - r$

Ham$(r,\ 2)$: $\left(2^r - 1, 2^{2^r-1-r}, 3\right)$

$$H = \Big[\underbrace{\qquad\qquad}_{2^r-1}\Big]\Big\}r$$

Columns of H are all non-zero r-bit vectors. All columns of H are different → sum of any two columns is not equal to 0. $d = 3.$

Example: $q = 2,\ n = 7,\ k = 4$

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

$\tilde{x} = x + e,\ \|e\| = 1$
$e = [0\quad 0\quad 1\quad 0\quad 0\quad 0\quad 0]$

$$S = H\tilde{x} = Hx + He = He = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} \rightarrow \text{third column of } H$$

In general for Ham$(r,\ 2)$, $H = [h_1, h_2, \cdots, h_n]$, $n = 2^r - 1$, $h_i \in Z_2^r$

$$\text{For single errors: } S_i = H \cdot e_i = [h_1, h_2, \cdots, h_i, \cdots, h_n]\begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \begin{matrix} \\ \\ \swarrow i \\ = h_i \\ \\ \\ \\ \end{matrix}$$

Since $h_i \neq h_j \rightarrow S_i \neq S_j$. Different errors have different syndromes → Errors can be computed if we know the syndrome.

Example:

1. $n = 7,\ k = 4,\ q = 2$

   $$H = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} = [h_1, h_2, h_3, h_4, h_5, h_6, h_7]$$

   If $S = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$, then $e = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$. Bit number four is distorted in the message since $S = h_4$.

2. $G = [1\quad 1\quad 1]$ – repetition code $n = 3$

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

Repetition code for $n = 3$ is $(3, 2, 3)$

T. Hamming Codes $(n, 2^k, 3) = \left(2^r - 1, 2^{2^r-1-r}, 3\right)$ are perfect for $q = 2$.

Proof:
$2^k = 2^{2^r-1-r}$, $l = 1$
Volume of a ball with radius $l = 1$ is $1 + n = 1 + 2^r - 1 = 2^r$
$2^k = 2^{2^r-1-r} = \frac{2^n}{n+1} = \frac{2^{2^r-1}}{2^r}$

Example: $n = 7$, $k = 4$, $r = 3$

$|Ham(3,2)| = 16$
$16 = \frac{2^7}{1+7} = 2^{7-3}$

$Ham(r,2)$ is $\left(2^r - 1, 2^{2^r-1-r}, 3\right)$ perfect single error correcting code. If $H = [h_1, h_2, \cdots, h_n]$, $n = 2^r - 1$, then $h_i \neq 0$, $h_i \neq h_j$, $h_i \in Z_2^r$

Example:
$Ham(3,2) \to (7{,}16{,}3)$ code

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

If $H = [h_1, h_2, \cdots, h_n]$, $S = H\tilde{x} = He$, then $e = (0 \cdots \underset{i}{010} \cdots 0) = e_i$ iff $S = h_i$

Extended Binary Hamming Code $\left(2^r, 2^{2^r-r-1}, 4\right)$
Correct single errors and detect triple errors

$$H_{ext} = \left.\begin{bmatrix} & H & & 0 \\ & & & \vdots \\ & & & 0 \\ 1 & \cdots & \cdots & 1 \end{bmatrix}\right\} r+1$$

Any 3 columns in H_{ext} are linearly independent (sum of any three columns is not equal to the column of all zeros, since in the last row in the sum we have one)

Example: $r = 4$ $(8{,}16{,}4)$

Extended Hamming code with $H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$

Decoding

Let $S = H\tilde{x} = \begin{bmatrix} S_1 \\ S_2 \\ S_3 \\ S_4 \end{bmatrix}$ $(r = 4)$

1. If $S_4 = 0$ and $(S_1, S_2, S_3) = 0 \to$ no errors
2. If $S_4 = 0$ and $(S_1, S_2, S_3) \neq 0 \to$ double errors
3. If $S_4 = 1$ and $(S_1, S_2, S_3) = 0 \to$ error in the last bit
4. If $S_4 = 1$ and $(S_1, S_2, S_3) \neq 0 \to$ single error in the bit j where (S_1, S_2, S_3) is the binary representation of j