EC500

Design of Secure and Reliable Hardware

Lecture 10

Mark Karpovsky

1 Cyclic Non-Binary Hamming Codes

$n=\frac{q^r-1}{q-1}$, $k=n-r$, $d=3$ (q is prime)

Take $p(x)=a_0+a_1x+a_2x^2+\cdots+a_{r-1}x^{r-1}+a_rx^r$ – primitive
$a_i\in\{0,1,\cdots,q-1\}=GF(q)$

Construct $GF(q^r)=\{0,1,\alpha,\alpha^2,\cdots,\alpha^{q^r-2}\}$ where $p(\alpha)=0$.

Take $H=[1\quad\alpha\quad\alpha^2\quad\alpha^3\quad\cdots\quad\alpha^{n-1}]$, $n=\frac{q^r-1}{q-1}$. All columns are different and $\alpha^i\neq c\alpha^j$, $c\in GF(q)$.

Proof:
Let $\alpha^i=c\alpha^j$, $c\in GF(q)$, $0\leq i,j\leq n-1$, $n=\frac{q^r-1}{q-1}$. Assume $j>i$, then $\alpha^{j-i}=c$. If we let $s=j-i$ then $s<n$ and $\alpha^s=c$. (α is primitive). $\alpha^{s(q-1)}=c^{q-1}=1$ (by Fermat Theorem), but $s(q-1)<n(q-1)=q^r-1$ and we have a contradiction $\begin{cases}\alpha^{s(q-1)}=1\\ s(q-1)<q^r-1\end{cases}$.

Example:
$q=3$, $r=2$, $d=3$
$n=\frac{q^2-1}{q-1}=q+1=4$
$p(x)=x^2+x+2\rightarrow\alpha^2+\alpha+2=0\rightarrow\alpha^2=2\alpha+1$
$GF(q^r)=GF(3^2)\rightarrow GF(q)=\{0,1,2\}$

0	0	0
0	1	1
0	2	α^4
1	0	α
1	1	α^7
1	2	α^6
2	0	α^5
2	1	α^2
2	2	α^3
α	1	$\alpha^8=1$

$H=[1\quad\alpha\quad\alpha^2\quad\alpha^3]=\begin{bmatrix}0&1&2&2\\1&0&1&2\end{bmatrix}$

Consider $v=(2\quad1\quad1\quad0)$, then $Hv=[1\quad\alpha\quad\alpha^2\quad\alpha^3]\begin{bmatrix}2\\1\\1\\0\end{bmatrix}=2+\alpha+\alpha^2=0\leftrightarrow p(\alpha)=0$, thus $(2\quad1\quad1\quad0)$ is a codeword. Let $v=(v_0\quad v_1\quad v_2\quad v_3)$, then $v(x)=v_1+xv_2+x^2v_3+x^3v_4$ and $Hv=v_1+\alpha v_2+\alpha^2v_3+\alpha^3v_4=0$. We get that v is a codeword iff $v(\alpha)=0\rightarrow\alpha$ is a root of $v(x)$.

If $v \in C \rightarrow v(\alpha) = 0$
$\omega(x) = v(x)Q(x)$ for any $Q(x)$, if $\omega(x) = v(x)Q(x) = 0 \rightarrow \omega \in C$

Code consists of all multiples of $v(x)$ if $v \in C$. $x^n = 1$.
Multiplication by x is equivalent to rotation (cyclic shift).

Example:
$v = (2 \quad 1 \quad 1 \quad 0)$
$v(x) = 2 + x + x^2$, $\omega(x) = \text{Rot}\, v(x) = 2x + x^2 + x^3 \rightarrow \omega = (0 \quad 2 \quad 1 \quad 1)$
$y = \text{Rot}\, \omega = (1 \quad 0 \quad 2 \quad 1) \rightarrow y(x) = 1 + 2x^2 + x^3 = \omega(x)x = (2x + x^2 + x^3)x = 2x^2 + x^3 + x^4 = 1 +$
$2x^2 + x^3 \rightarrow y = (1 \quad 0 \quad 2 \quad 1)$ $\nwarrow x^4 = 1$

Since $p(\alpha) = 0$, $p \in C$. For our example, $p(x) = x^2 + x + 2 \rightarrow p = (2 \quad 1 \quad 1 \quad 0) \in C$. $\omega = \text{Rot}\, p =$ $(0 \quad 2 \quad 1 \quad 1) \in C$ and $\text{Rot}\, \omega = (1 \quad 0 \quad 2 \quad 1) \in C$. To verify, $[1 \quad \alpha \quad \alpha^2 \quad \alpha^3] \begin{bmatrix} 1 \\ 0 \\ 2 \\ 1 \end{bmatrix} = 1 + 2\alpha^2 + \alpha^3$.
We have $\alpha^2 = 2\alpha + 1$ and $\alpha^3 = 2\alpha + 2$ and thus $1 + 2\alpha^2 + \alpha^3 = 1 + 2(2\alpha + 1) + 2\alpha + 2 = 1 + 6\alpha +$ $5 = 0$ and so we find $(1 \quad 0 \quad 2 \quad 1) = \text{Rot}\,(0 \quad 2 \quad 1 \quad 1) \in C$.

Thus, we constructed a $(4,3,3)$ ternary cyclic Hamming code with the check matrix $H = [1 \quad \alpha \quad \alpha^2 \quad \alpha^3] = \begin{bmatrix} 0 & 1 & 2 & 2 \\ 1 & 0 & 1 & 2 \end{bmatrix}$ where $r = 2$. The generating matrix for this code is $G = p(x) =$ $[2 \quad 1 \quad 1 \quad 0]$.

Example:
$q = 3$, $r = 3$
$n = \frac{q^3 - 1}{q - 1} = 13$, $k = 13 - 3 = 10$

$H = [1 \quad \alpha \quad \alpha^2 \quad \alpha^3 \quad \alpha^4 \quad \alpha^5 \quad \alpha^6 \quad \alpha^7 \quad \alpha^8 \quad \alpha^9 \quad \alpha^{10} \quad \alpha^{11} \quad \alpha^{12}]$ and $\text{G} = \begin{bmatrix} p(x) \\ xp(x) \\ x^2p(x) \\ x^3p(x) \\ x^4p(x) \\ x^5p(x) \\ x^6p(x) \\ x^7p(x) \\ x^8p(x) \end{bmatrix}$