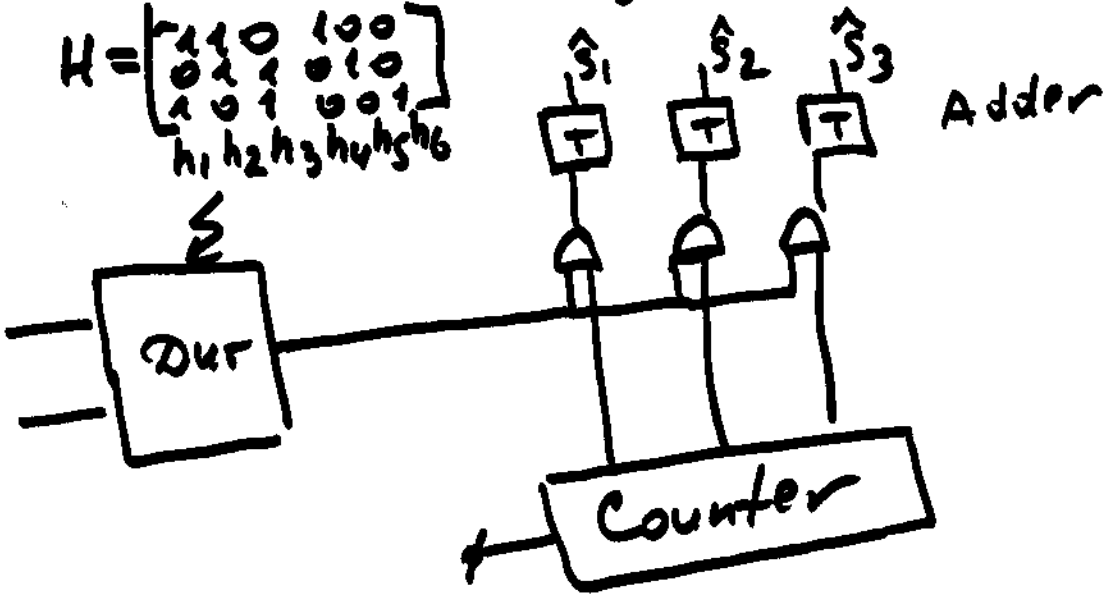
H is a check matrix of a (best) $(n, 2^k, l+1)$ code

Example $l=2$. Hamming code

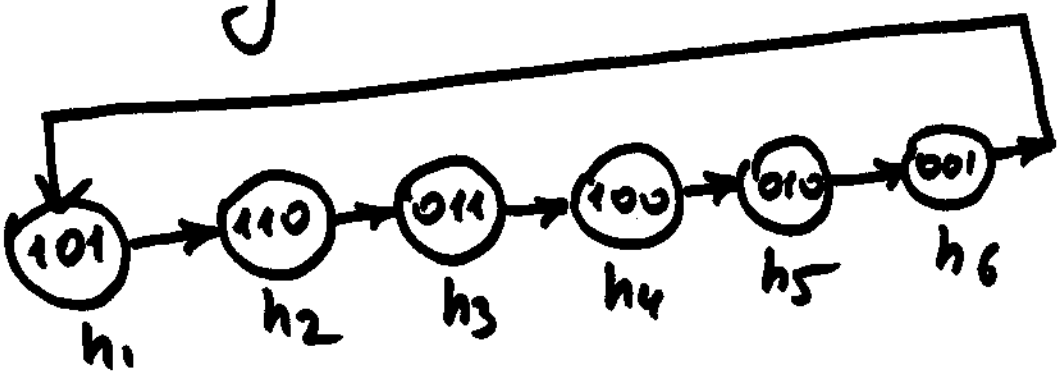
$n=6$, $k=3$, $r=3$

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

$h_1\ h_2\ h_3\ h_4\ h_5\ h_6$



Counting sequence (transition diagram)



3 FFs

q-ary HAMMING CODES

HAM (r, q)

$\left(\frac{q^r-1}{q-1}, q^k, 3\right)$,

where $k = n - r$

$n = \frac{q^r-1}{q-1}$

Any two columns of H are linearly independent

$H = [h_1, h_2, \ldots, h_n] \Rightarrow$

$h_i \neq 0$, $h_i \neq h_j$, $h_i \neq \alpha h_j$

$h_i, h_j \in Z_q^r$ $\alpha \in Z_q$

EXAMPLES $q=3$ TERNARY

1) HAM $(2,3)$ $(4,3^2,3)$

$$H=\begin{bmatrix}0&1&1&1\\1&0&1&2\end{bmatrix}$$

2) HAM $(3,3)$ $(13,10,3)$

$$H=\begin{bmatrix}0&0&0&0&1&1&1&1&1&1&1&1&1\\0&1&1&1&0&0&0&1&1&1&2&2&2\\1&0&1&2&0&1&2&0&1&2&0&1&2\end{bmatrix}$$

① All HAMMING CODES ARE PERFECT

Proof $n=\frac{q^r-1}{q-1}$

volume of a ball with radius 1 is $1+n(q-1)=$

$=q^r$

$$|HAM(r,q)| = \frac{q^n}{V}=\frac{q^n}{q^r}=q^{n-r}$$

SHORTENED CODES

If $\mathbb{C}$ is a (n, q^k, d) code with the check matrix H then by deleting any s $(s < n)$ columns in H we have the check matrix H_{SH} of the shortened code $\mathbb{C}_{SH}$ with $(n-s, q^{k-s}, d)$

EXAMPLE

By shortening (7, 16, 3) HAM (2,3) code with

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

have (5, 4, 3) shortened HAMMING CODE with

$$H_{SH} = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

By shortening HAMMING codes we can construct best single error correcting codes for any n

SHORTENED ERROR CORRECTING HAMMING CODES ARE NOT PERFECT.

EXAMPLE $q=2$

$HAM(5,2)$ $(31, 2^{26}, 3)$

BY SHORTENING BY $s=5$ bit

we have

$(26, 2^{21}, 3)$ code