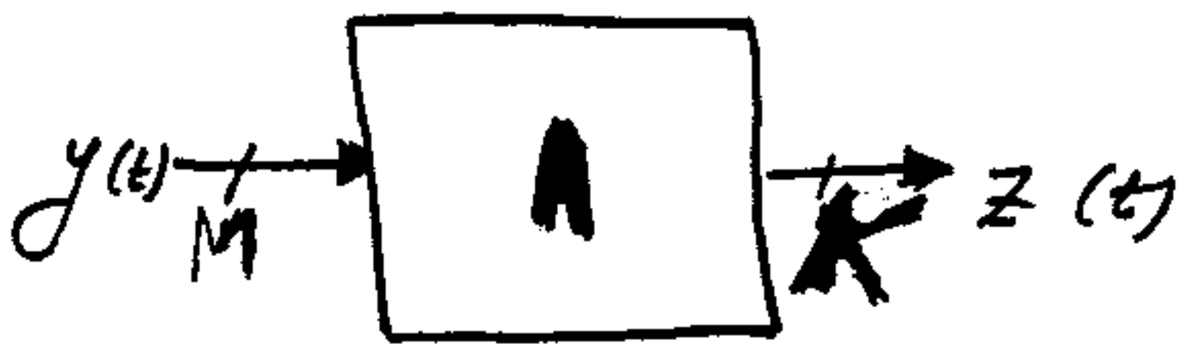
Concurrent Checking of Linear Devices

Device is **Linear** if it can be implemented by **XOR** gates and **FFs only**

Linear **combinational** devices:



$Z(t) = y(t) \cdot A$ all computations mod 2

Example Network computing syndromes for $(M = 2^m - 1, \; 2^m - m - 1, \; d = 3)$ Hamming code

[redacted]

Linear sequential devices

$\mathcal{D}(t+1) = \mathcal{D}(t)\, A \oplus y(t+1)$

$Z(t+1) = \mathcal{D}(t+1)$

$\mathcal{D}(t), y(t)$ are n-bit vectors

A is $(n \times n)$ binary matrix

$\mathcal{D}(t)$ internal state

$t = n$

Select code C of length t to protect a linear device (C is a (t, κ) code $r = t - \kappa$)

A generating matrix of C can always be presented as

$$G = (I \mid P)$$

where I is the $(\kappa \times \kappa)$ identity matrix and P is $\kappa \times (t-r)$ matrix

EXAMPLE C_{is} (7,4) HAMMING with check matrix

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

PTR

If $(v_1, v_2, v_3, v_4, v_5, v_6, v_7) \in C$ then

$v_2 \oplus v_3 \oplus v_4 \oplus v_5 = 0$ $\quad v_5 = v_2 \oplus v_3 \oplus v_4$

$v_1 \oplus v_3 \oplus v_4 \oplus v_6 = 0$ $\quad v_6 = v_1 \oplus v_3 \oplus v_4$

$v_1 \oplus v_2 \oplus v_4 \oplus v_7 = 0$ $\quad v_7 = v_1 \oplus v_2 \oplus v_4$

$$G = \left[\begin{array}{ccccc|ccc} v_1 & v_2 & v_3 & v_4 & & v_5 & v_6 & v_7 \\ 1 & 0 & 0 & 0 & & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & & 1 & 1 & 1 \end{array}\right] \Rightarrow P = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$$

P

$(v_1, \ldots, v_k, v_{k+1}, \ldots, v_t) \in C$ if

$R(v_1, \ldots, v_k) = (v_{k+1}, \ldots, v_t) = (v_1, \ldots, v_k) P.$

redundand bits in a codeword

↖ ENCODING

Example For the above (7,4) code

$$(1001) \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} = (100)$$

and (1001 100) is a codeword

Thus for combinatonal linear machines ~~for~~ we have for redundant outputs

$$R(Z(t)) = y(t)\,A\,P = y(t)\,A'$$

where H' is $H \bullet P$ and $Z(t) = Y(t)A$

EXAMPLE 1 Let the original linear combinatonal device is defined as

$$Z(H = y(t) \bullet \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix} \quad M=5 \quad K=3$$

and we want to protect it with (4,3) 1dim parity, then we have for the parity bit $P = \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix}$

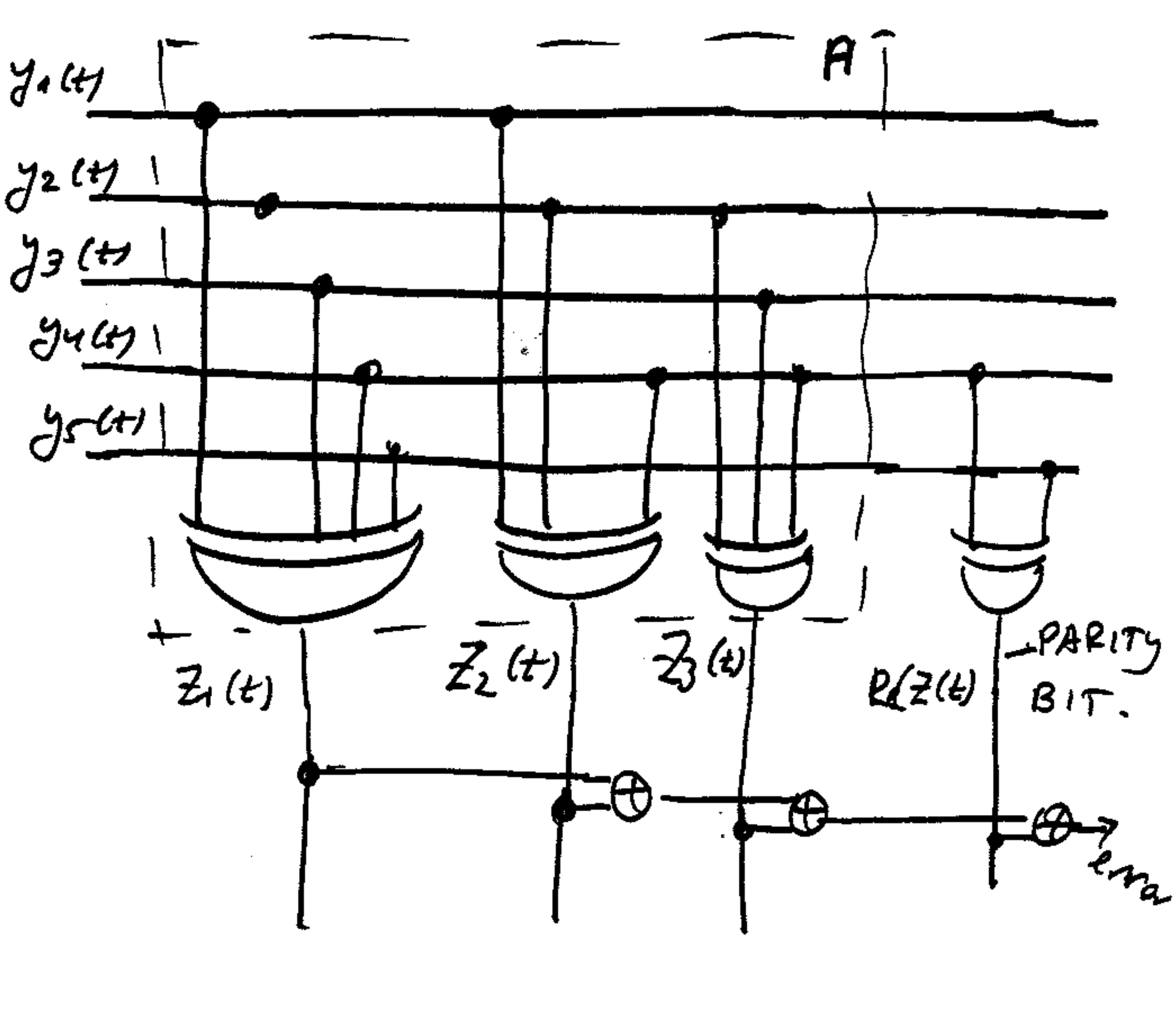
$$R(Z(t)) = y(t)\,A' = y(t) \cdot \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} =$$

$$= y(t) \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} \leftarrow H'$$

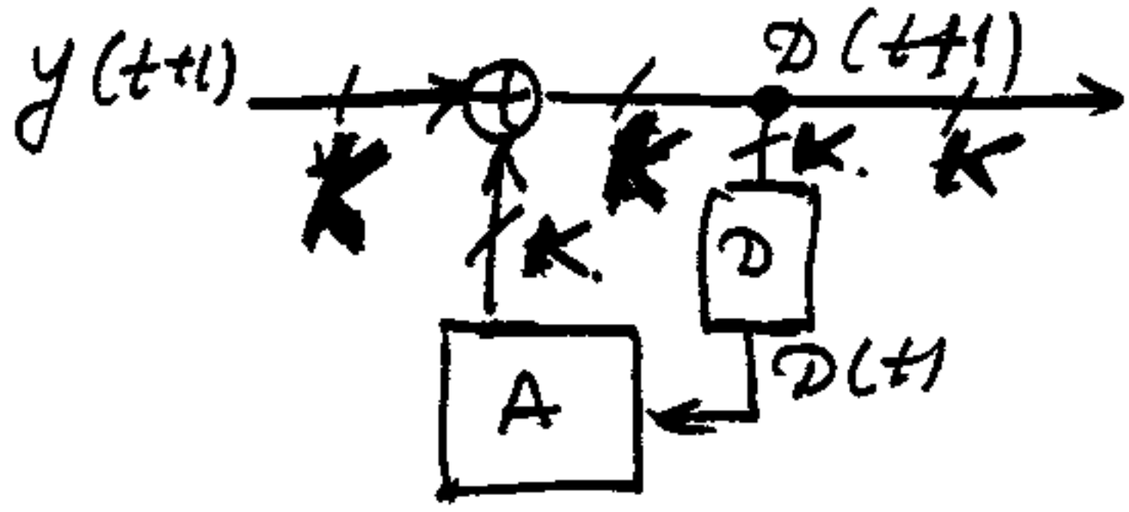
. If $y(t) = (y_1(t), y_2(t), y_3(t), y_4(t), y_5(t))$

Then $R(Z(t)) = y_4(t) \oplus y_5(t)$

NETWORK FOR THE PREVIOUS EXAMPLE



CONCURRENT CHECKING OF LINEAR SEQUENTIAL DEVICES



$$D(t+1) = D(t)\,A \oplus y(t+1) \qquad D(t),\ y(t) \in GF(2^k)$$

A is a $(k \times k)$ binary matrix

FOR CONCURRENT CHECKING by the code C with k inf. bits. with

$$G = [\,I \mid P\,].$$

we have

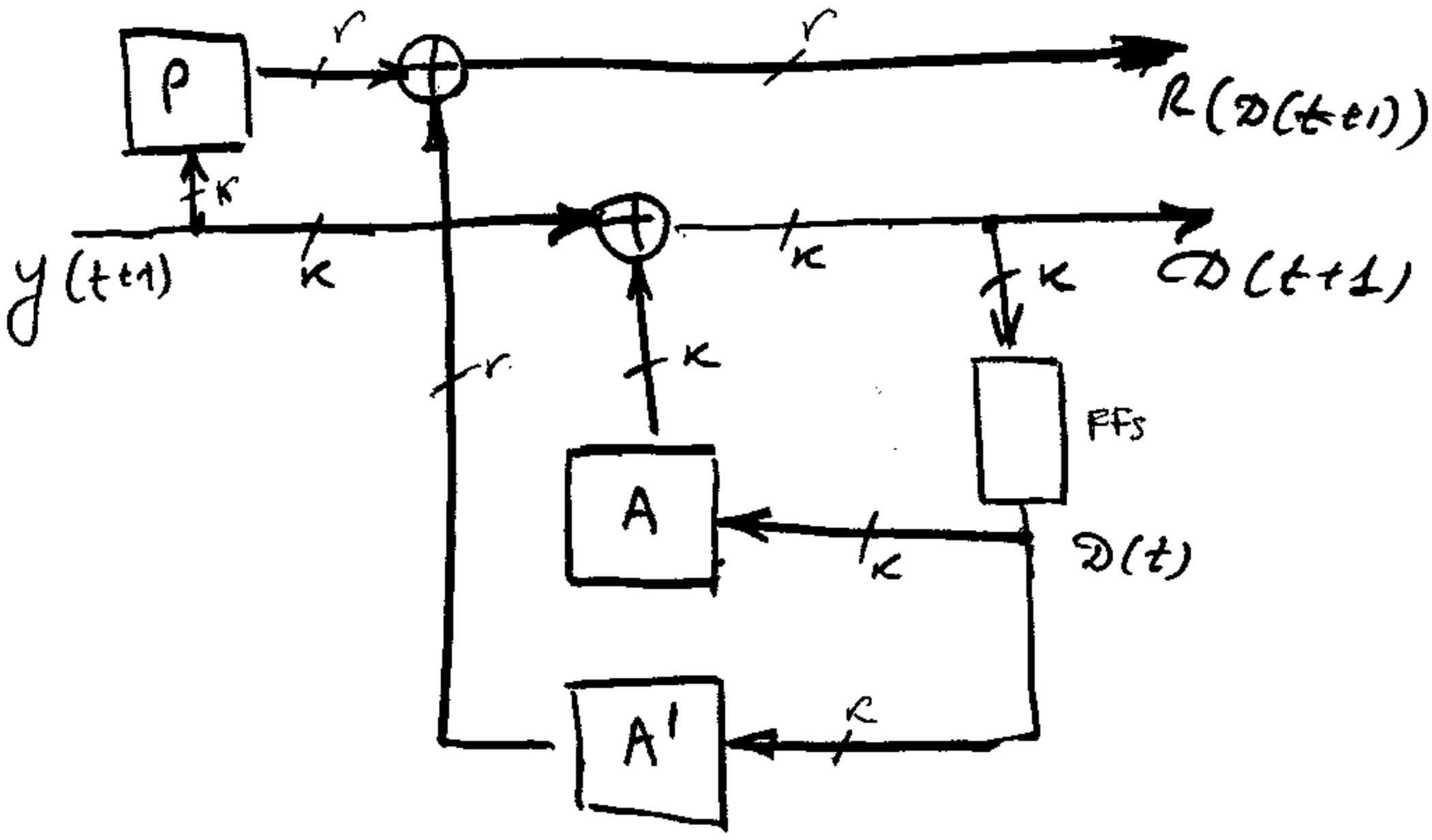
$$R(D(t+1)) = R(D(t)A)) \oplus R(y(t+1))$$

$$= D(t)\,AP \oplus y(t+1)\,P =$$

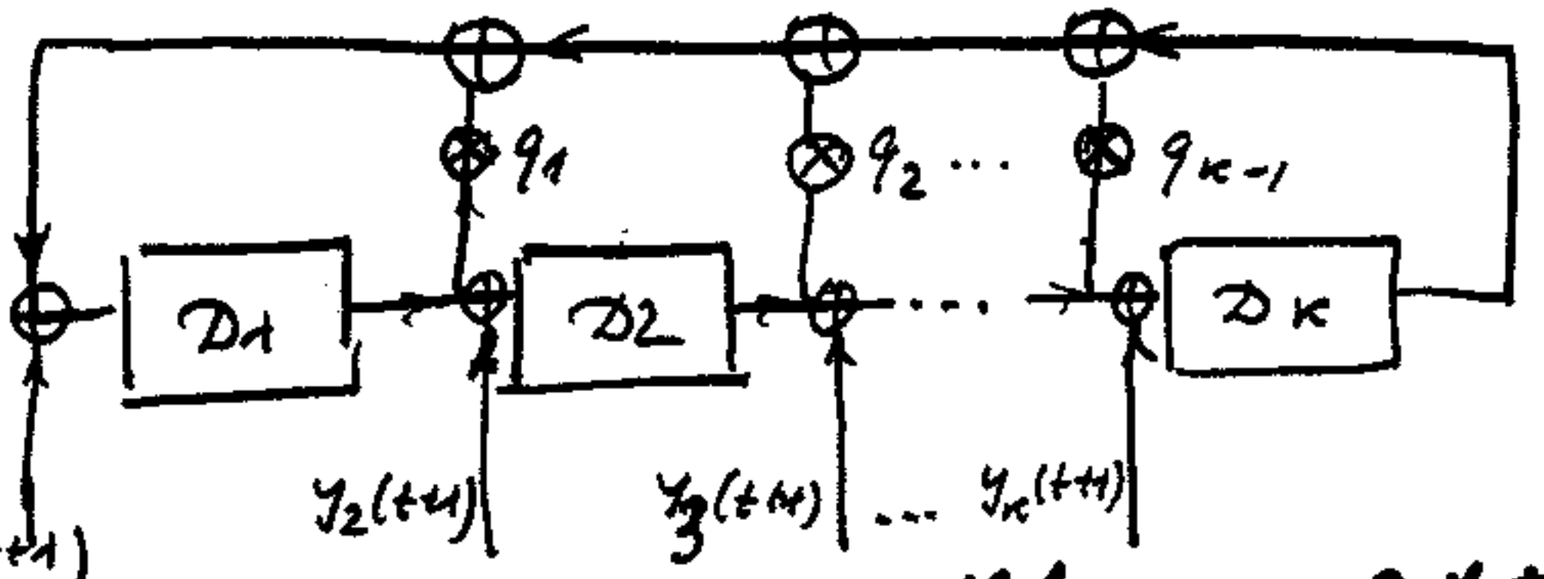
$$= D(t)\,A' \oplus y(t+1)\,P$$

$$A' = A \cdot P$$

Block diagram for concurrent checking of Linear Sequential devices



EXAMPLE Let the sequential device is MISR:



$$x^k + q_{k-1}x^{k-1} + \dots + q_1 x + 1$$

Then

$$A = \underbrace{\begin{bmatrix} q_1 & 1 & 0 & 0 & \dots & 0 \\ q_2 & 0 & 1 & 0 & \dots & 0 \\ q_3 & 0 & 0 & 1 & \dots & 0 \\ \vdots & & & & & \\ q_{k-1} & 0 & 0 & 0 & \dots & 1 \\ 1 & 0 & 0 & 0 & \dots & 0 \end{bmatrix}}_{k} \Bigg\} \quad C = \left[\begin{array}{c|c} q_1 & \\ q_2 & I_{k-1} \\ \vdots & \\ q_{k-1} & \\ \hline 1 & 0 \dots 0 \end{array}\right]$$

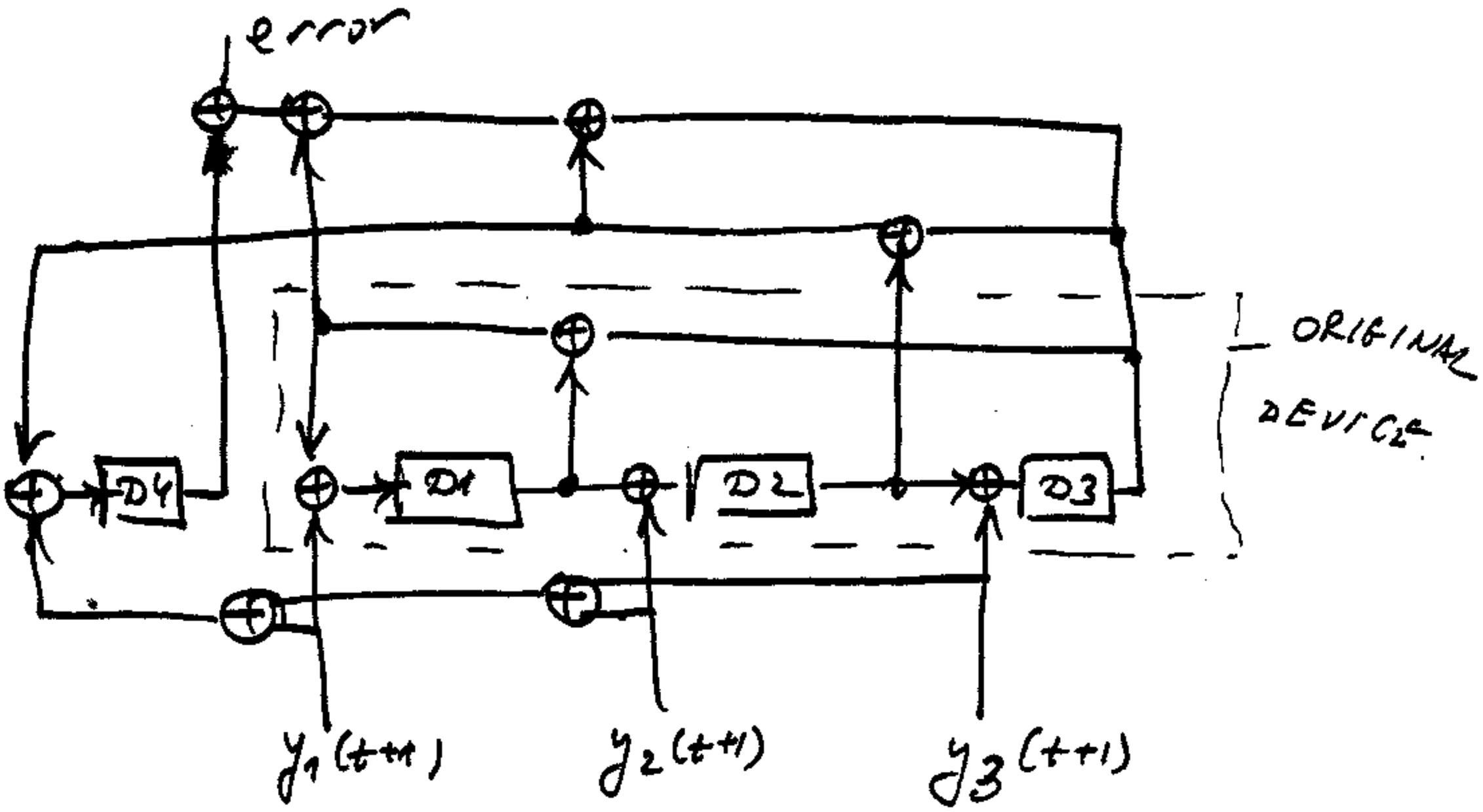
Select $(k+1, k)$ code to protect this MISR

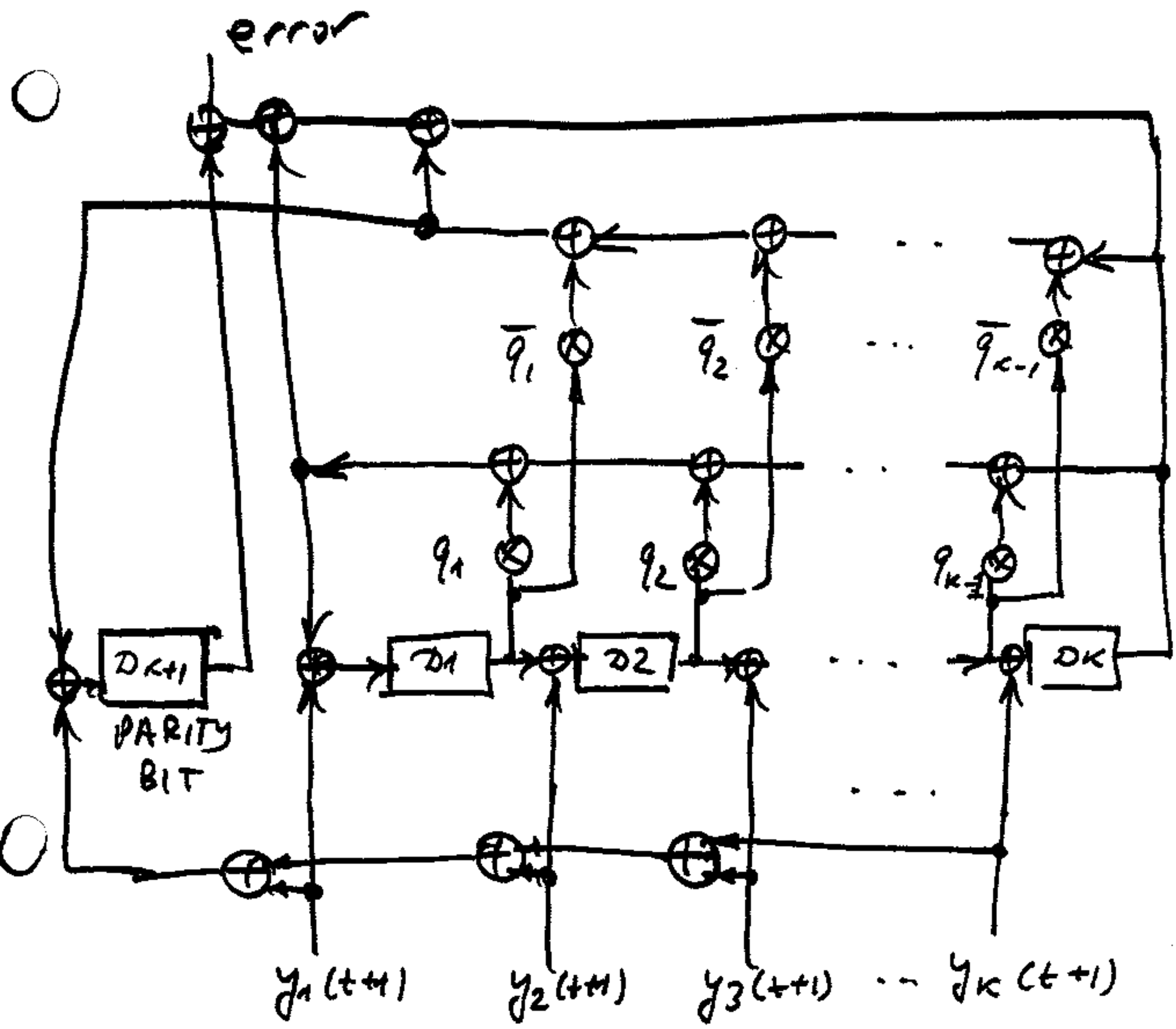
Then $P = \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix}$ and $A' = AP = \begin{bmatrix} \overline{q_1} \\ \overline{q_2} \\ \vdots \\ \overline{q_{k-1}} \\ 1 \end{bmatrix}$, $\overline{q_i} = 1 - q_i$

$$y(t+1)P = \bigoplus_{i=1}^{k} y_i(t+1)$$

$$\mathcal{D}(t)A' = \bigoplus_{i=1}^{k-1} D_i(t)\,\overline{q_i} \;\oplus\; D_k(t)$$

EXAMPLE: $K=3$




error
$\overline{q}_1$
$\overline{q}_2$
$\overline{q}_{k-1}$
q_1
q_2
q_{k-1}
D_{k+1}
PARITY BIT
D_1
D_2
D_k
$y_1(t+1)$
$y_2(t+1)$
$y_3(t+1)$
$y_k(t+1)$