ERROR DETECTING / CORRECTING CODES

Consider set F_q^m of all m-dimensional vectors $y = (y_0, \ldots, y_{m-1})$ where y_i is a b bit binary vector and $q = 2^b$

Code V is any subset of F_q^m

$$V \subseteq F_q^m$$

vectors from a code are codewords

FOR ANY $y, z \in F_q^m$

$$y \oplus z = (y_0 \oplus z_0, \ldots, y_{m-1} \oplus z_{m-1}) \in F_q^m$$

HAMMING distance

FOR ANY $y, z \in F_q^m$

$d(y,z)$ = number of noncoinsiding components in y and z

<u>EXAMPLE</u> $b=2$, $q=4$, $m=3$

$$y = (00, 10, 11)$$
$$z = (10, 10, 01)$$
$$y \oplus z = (10, 00, 10)$$

$$d(y,z) = 2$$

FOR ANY $y, z \in F_q^m$

$$0 \le d(y,z) \le m$$

$$d(y,z) = 0 \Rightarrow y = z$$

for $b=1$, $q=2$, $d(y,z) = m \Rightarrow y = \bar{z}$

$d(\mathbb{0}, y) = \|y\|$ HAMMING NORM OF y = number of nonzero components in y

$$\mathbb{0} = (0, \ldots, 0)$$

Error - Detecting / Correcting Codes.

Hamming Distance:

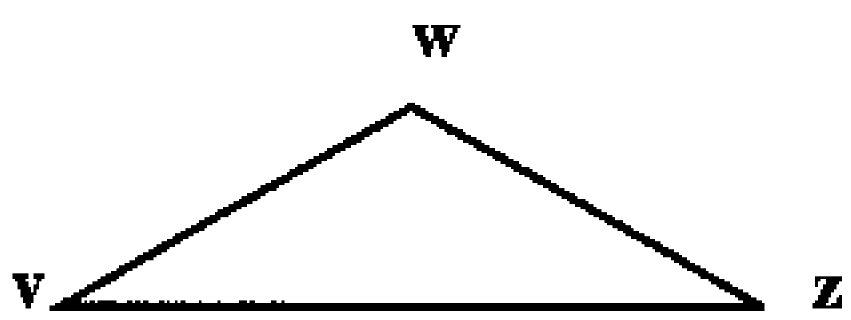
FOR b=2

$$v = (v_1, \ldots, v_n),\ w = (w_1, \ldots, w_n) \Rightarrow d(v, w) = \sum_{i=1}^{n} (v_i \oplus w_i)$$

Example : n = 5 , d (10110 , 11001) = 4

FOR ANY b:

$0 \le d(v,w) \le n$; $d(v,w) + d(w,z) \ge d(v,z)$



Code with distance d :

Set of vectors U such that $\min_{v,w \in U} d(v,w) = d$

Example : U = { 00000, 10011, 01110, 11101 } . Code with distance d(U) = 3 , b= 2

(D. P. Sewiorek, R.S. Swartz, "Theory and Practice of Reliable System Design, Ch3 and Appendix A).

$$d(\tau \oplus v, \tau \oplus w) = d(v, w) \Rightarrow (0, 0, \ldots, 0) \in V$$

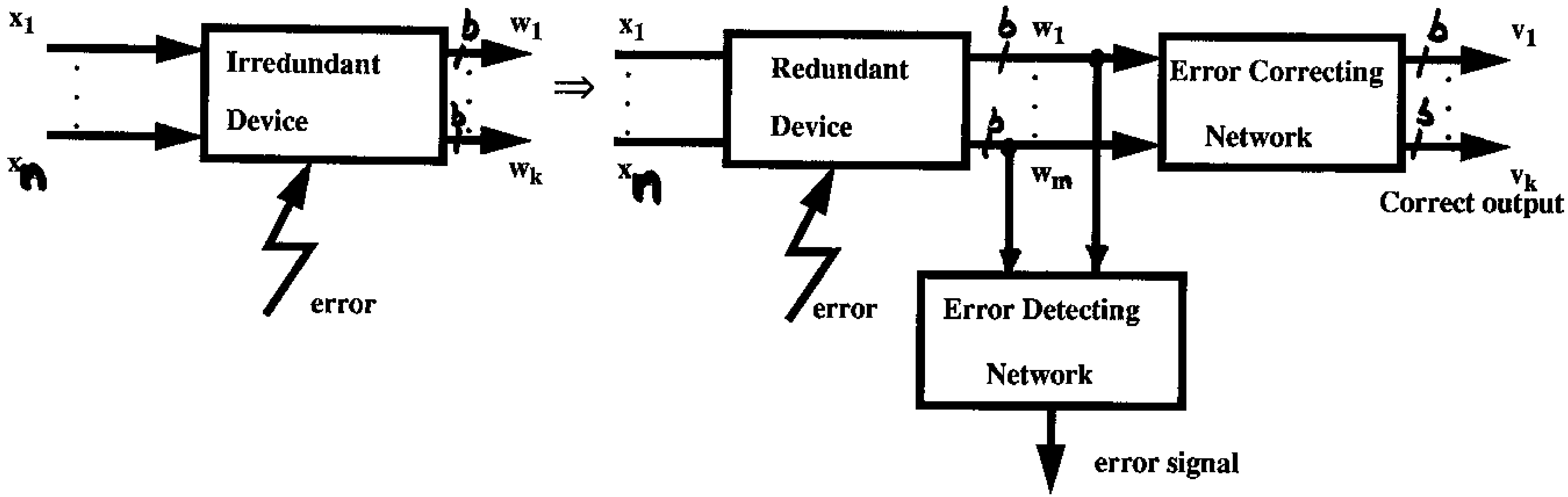
Error : $v \dashrightarrow w$, $e = v \oplus w$

$e_i \neq 0$ if v_i is distorted.

Multiplicity ℓ of an error:

$$\ell = d(v,w) = d(e, 00\ldots0) = \|e\|$$

Example e : 01110 ---> 01010, e = 00100, $\|e\| = 1$



For fault - free device v = w

Code vectors ($v_1, \ldots, v_k, v_{k+1}, \ldots, v_{k+r}$), $k + r = n$, *satisfy r equations.*

Problems :

1. Relation between multiplicity of errors and distance of the code (simple).

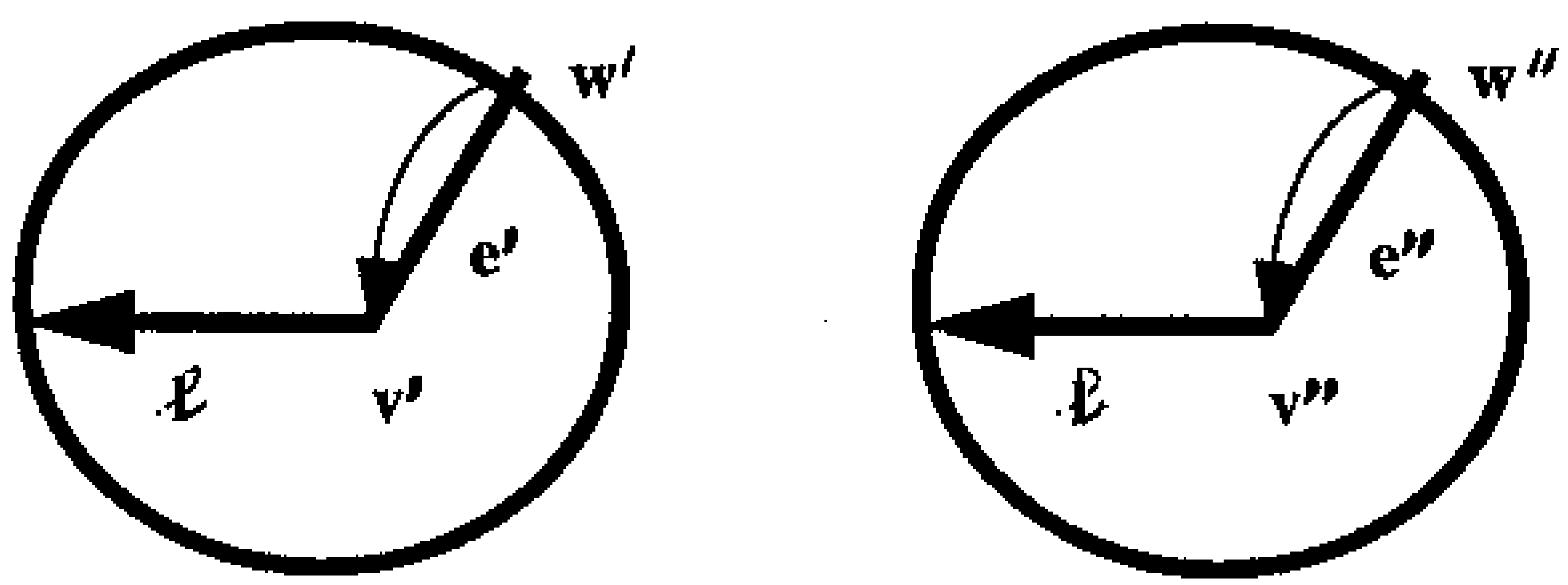
2. Construction of an optimal code with the given distance (difficult).

3. Implementation of error detecting / correcting networks.

Error Correcting Codes.

Geometrical Interpretation.

Error correction :



v', v'' - fault - free output ; $v', v'' \in \mathcal{V}$

e', e'' - errors ; $\| e' \|, \| e'' \| \leq \ell$

w', w'' - faulty outputs

ℓ- multiplicity of errors.

For error correction spheres must not intersect $\Leftrightarrow$ $d(v', v'') \geq 2\ell + 1$

$$\boxed{d(\mathcal{V}) \geq 2\ell + 1}$$

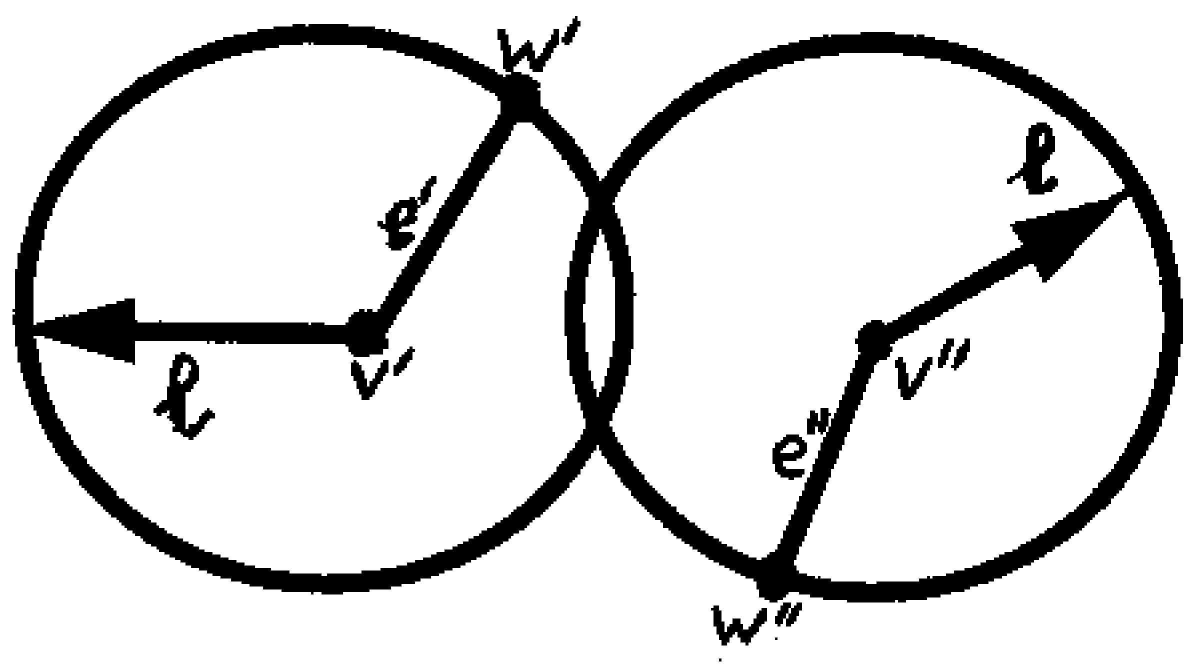
Error Detection :

$v', v'' \in U$

e' , e'' - errors ; $\| e' \|$, $\| e'' \| \leq \ell$

$w' = v' \oplus e'$

$w'' = v'' \oplus e''$



Any sphere doesn't contain a center of another one $\Leftrightarrow$ $d(v', v'') \geq \ell + 1$

$$\boxed{d(V) \geq \ell + 1}$$

Set of all vectors at the distance exactly (up to) e from any given vector y is the Hamming sphere (ball) with radius e and center y.

the size of a ball with radius e

$$V(e) = \sum_{i=1}^{e} \binom{n}{i} (q-1)^{i}$$

the size of a sphere with radius e

$$S(e) = \binom{n}{e} (q-1)^{e}$$

$$\frac{S(e)}{V(e)} \simeq 1$$ skin effect for large n.

∴ Code V is <u>linear</u> (systematic)
if for $v_1, v_2 \in V \Rightarrow v_1 \oplus v_2 \in V$

∴ one-dimensional parity checks,
two-dimensional parity checks and
Hamming codes are linear, BCH is linear
RM codes are linear.

∴ Code is <u>cyclic</u> if a cyclic shift
of a codeword is another codeword.

∴ BCH codes are cyclic codes

∴ All cyclic codes are linear

Code V is <u>linear</u> iff for any

$y, z \in V \Rightarrow y \oplus z \in V$

For linear a code V $|V|$ - number of codewords $|V| = q^K$ where K is a number of information digits

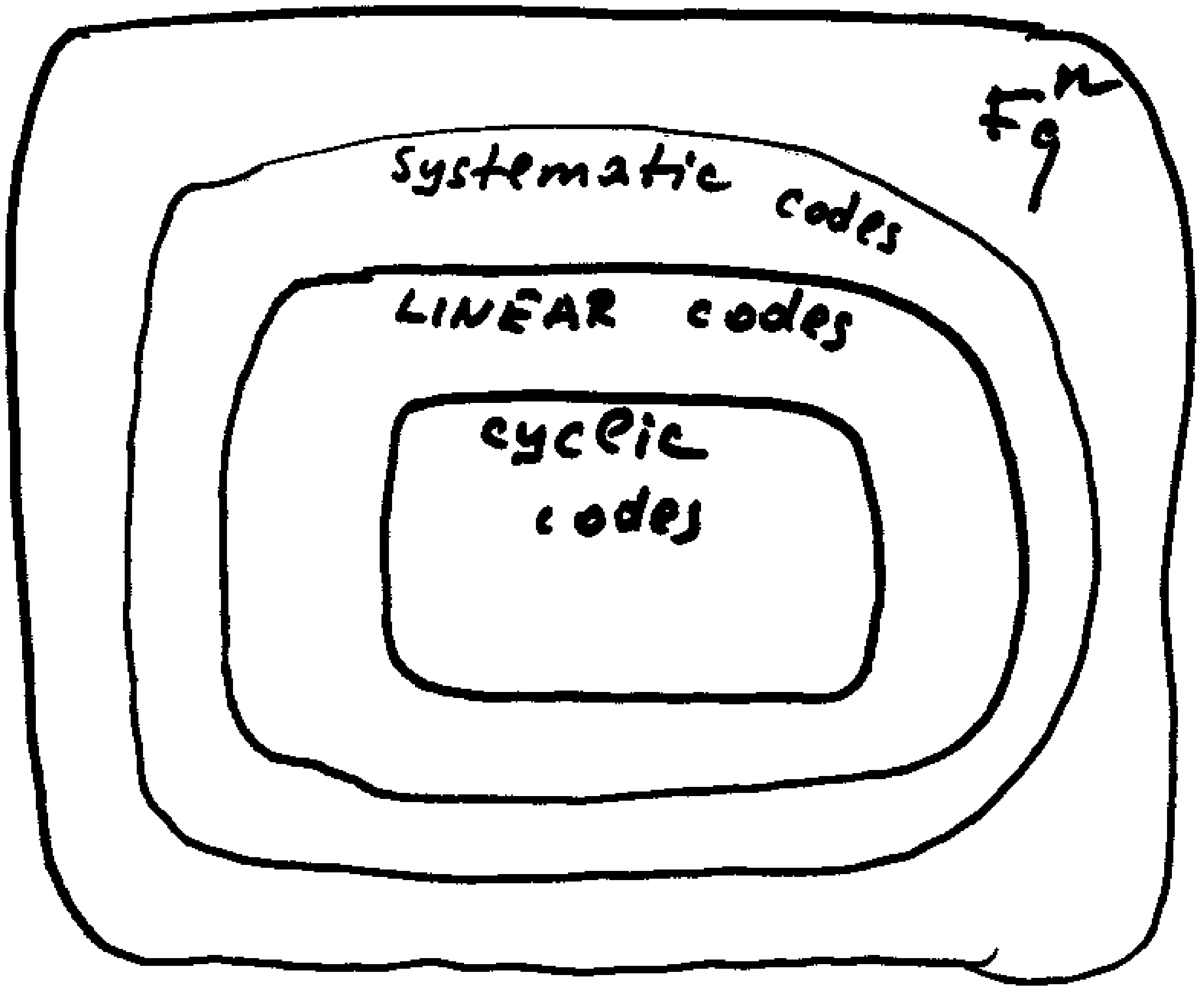
Code is <u>systematic</u> if one can distinguish between information and redundand digits

Any linear code is systematic
(Opposite is not true)

A code is cyclic iff any cyclic shift of a codeword is a codeword

If code is cyclic then it is linear

Let F_q^n set of all vectors y of length n with components y_i being b-bit vectors where $q=2^b$



Linear codes of length n with k information ~~bits~~ digits and distance d are denoted

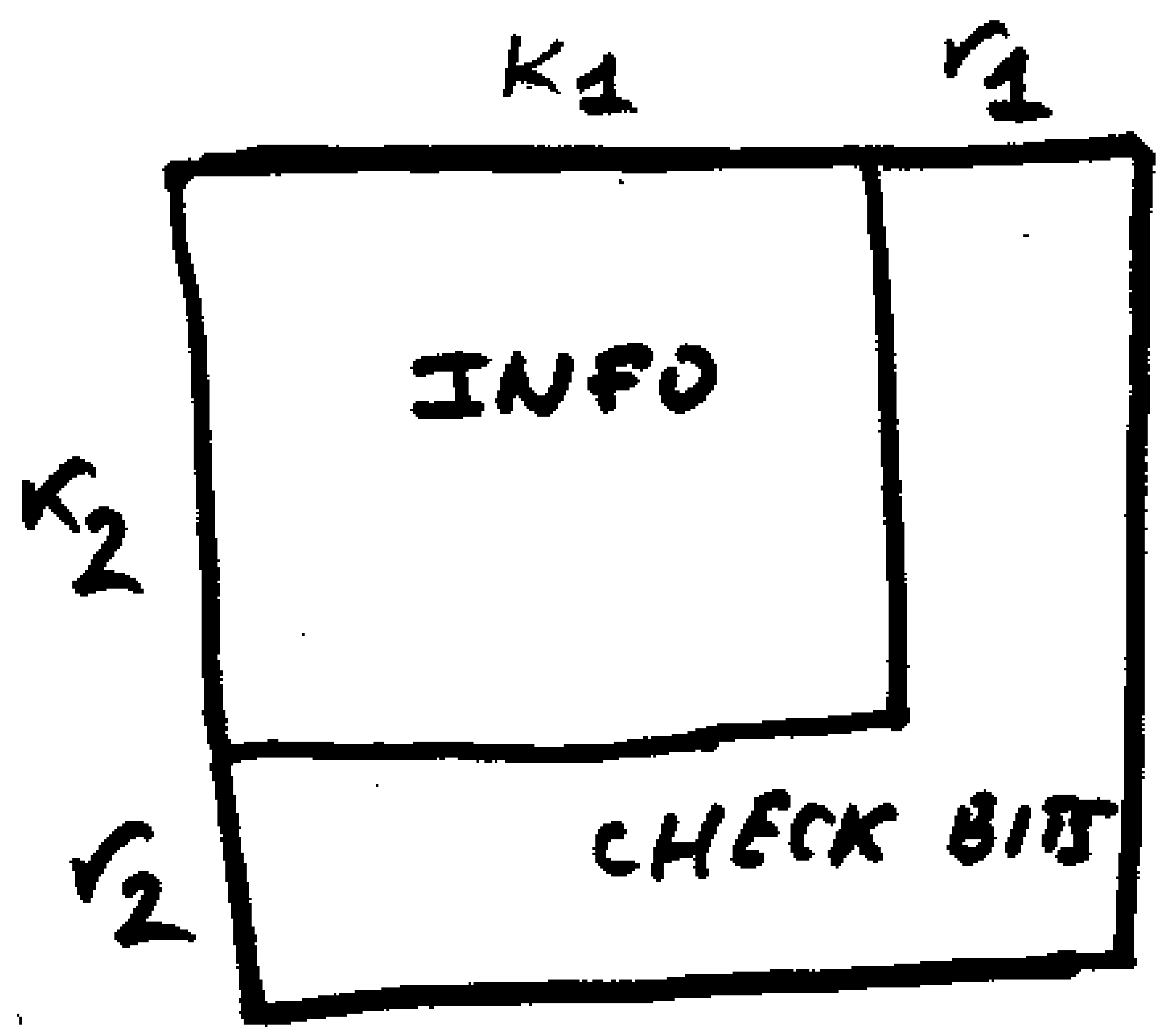
$[n, k, d]$ codes

<u>TRANSITION RATE</u> $0 < R = \frac{k}{n} < 1$

<u>DIRECT PRODUCT OF CODES</u>

V_1 : $[n_1, k_1, d_1]$ code $\qquad r_1 = n_1 - k_1$

V_2 : $[n_2, k_2, d_2]$ code $\qquad r_2 = n_2 - k_2$



$V_1 \times V_2$

$$V_1 \times V_2 \;:\; [n_1 n_2,\ \kappa_1 \cdot \kappa_2,\ d_1 d_2]$$

If $V_1 = V_2$

$$V_1^2 \;:\; [n_1^2,\ \kappa_1^2,\ d_1^2]$$

FOR $R(V_1^2) = \dfrac{\kappa_1^2}{n_1^2} = \left(R(V_1)\right)^2$