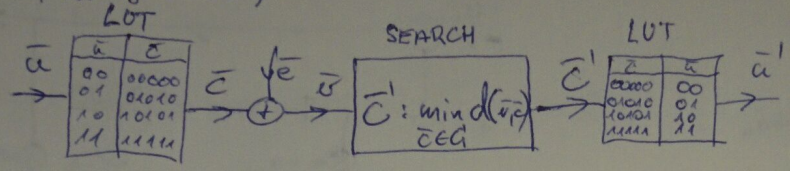
INFORÓD VIZSGA

(general coding scheme:)



Error correcting by repeater:
- drop in data speed: $\frac{1}{N}$
- $\frac{k}{n}$: price of detection

G_{opt} : $\max_{G} d_{min}$ $\qquad$ $d_{min} : \min_{\substack{\bar{c}\bar{c}' \in G \\ \bar{c} \neq \bar{c}'}} d(\bar{c}, \bar{c}')$

Error detection : $d_{min} - 1 = \ell$, $d_{min} \leq n - k + 1$: singleton bound

Error correction : $t = \left\lfloor \frac{d_{min} - 1}{2} \right\rfloor$,

MDS codes = Minimum Distance Separable : G_{opt} : $d_{min} = n - k + 1$

Hamming codes : $2^{n-k} = n+1$

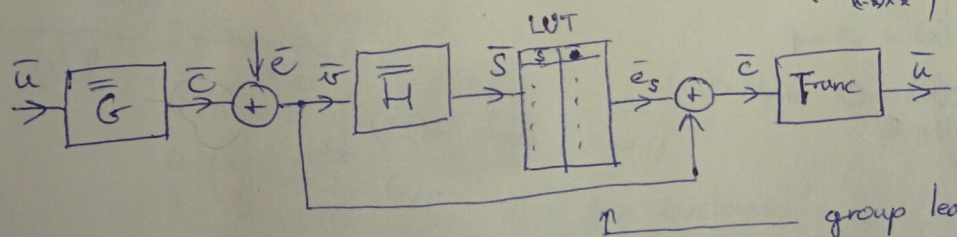
Binary linear codes : $\bar{c} = \bar{u}\,\overline{\overline{G}}_{k \times n}$

Systematic codes : $\bar{c} = (\bar{u}, \bar{p})$ (message, parity) , $\overline{\overline{G}}_{k \times n} = \left(\overline{\overline{I}}_{k \times k}, \overline{\overline{B}}_{k \times (n-k)}\right)$

$\bar{c} \xrightarrow{\text{Trunc}} \bar{u}$

↳ parity check matrix : $\overline{\overline{H}}_{(n-k) \times n}$: $\overline{\overline{H}}\bar{c}^T = \bar{0}^T$, $\Rightarrow \overline{\overline{H}}\overline{\overline{G}}^T = \overline{\overline{0}}$

$\overline{\overline{H}} = \left(\overline{\overline{B}}^T_{(n-k) \times k}, \overline{\overline{I}}_{(n-k) \times (n-k)}\right)$

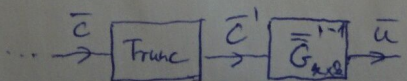


group leader : a legnagyobb valószínűségű hibavektor

C(3,1) : Hamming code + MDS code

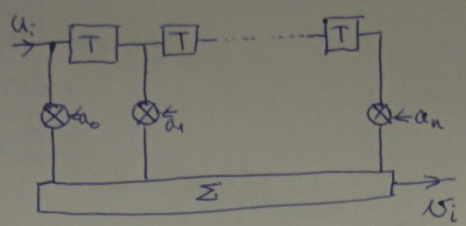
Reed-Solomon (RS) codes : q : prime , $n = q - 1$, $2t = n - k$ + MDS code over $GF(q)$ $\exists \alpha$ (primitive element)

$$\overline{\overline{G}}_{k \times n} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{k-1} & \alpha^{2(k-1)} & \cdots & \alpha^{(k-1)(n-1)} \end{pmatrix} , \quad \overline{\overline{H}}_{(n-k) \times n} = \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{n-k} & \alpha^{2(n-k)} & \cdots & \alpha^{(n-k)(n-1)} \end{pmatrix}$$



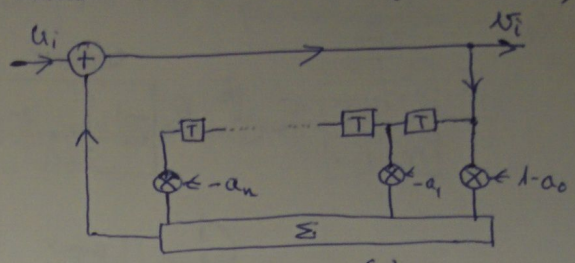
↳ any number of errors can be corrected

Linear Feed Forward Shift Register: (LFFSR)



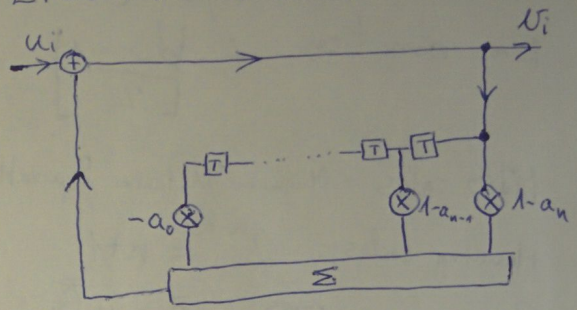
$$v(x) = a(x) \cdot u(x)$$

Linear Feed Back Shift Register: (LFBSR)



$$v(x) = \frac{u(x)}{a(x)}$$

LFBSR with remainder: (LFBSR wr)



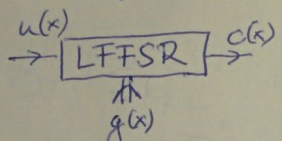
$$u(x) = v(x) \cdot a(x) + r(x)$$

Cyclic linear codes:

$$c'(x) = x \cdot c(x) \bmod (x^n - 1)$$

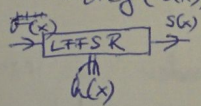
↳ generator polinom: $g(x)$

- $\deg(g(x)) = n-k$
- $g_{n-k} = 1$
- $\forall c(x) = a(x) \cdot g(x)$
- $g(x) \mid x^n - 1$



↳ parity check polinom: $h(x)$

- $g(x) \cdot h(x) = x^n - 1$
- $h(x) \cdot c(x) = 0 \bmod (x^n - 1)$
- $\deg(h(x)) = k$



RS codes are cyclic

$$\Downarrow$$

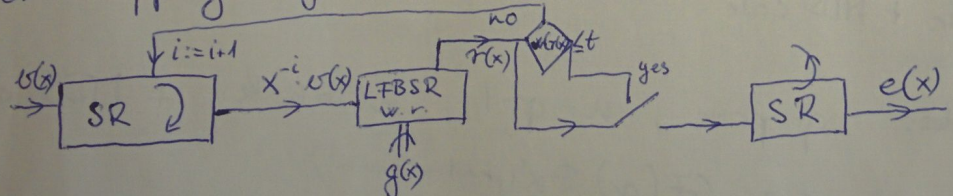
$$x^n - 1 = \underbrace{\prod_{i=1}^{n-k} (x - \alpha^i)}_{g(x)} \cdot \underbrace{\prod_{i=n-k+1}^{n} (x - \alpha^i)}_{h(x)}$$

over $GF(2^m)$:

$$g(x) = \prod_{i=1}^{n-k} (x - y^i)$$

$$h(x) = \prod_{i=n-k+1}^{n} (x - y^i)$$

Error Trapping Algorithm: (ETA)



- 3 shift regiszter (x hatvánnyal eltolás, maradékos osztás, x hatványával visszatolás)
- switch (a $w(r(x)) \leq t$ feltétel ellenőrzésére)

Entrophy: $H(x) := \sum_x p(x) \cdot \mathrm{ld} \frac{1}{p(x)}$, $0 \leq H(x) \leq \mathrm{ld}\, N$, N: szimbólumok száma

Átlagos kódszóhossz: $L = \sum_x p(x) \cdot \ell(x)$, Dataspeed $= L \cdot f_s$

C_{opt} : $\min_C L$: • unique decoding $\sum_x 2^{-\ell(x)} \leq 1 \Rightarrow$ binary tree
• given $p(x) \overset{?}{\rightarrow} \ell(x)$

Shannon-Fano coding:

$$\ell(x) = \left\lceil \mathrm{ld} \frac{1}{p(x)} \right\rceil \Rightarrow H(x) \leq L_{SF} \leq H(x) + 1$$

Haffman coding:

↳ if $p_i > p_j$ then $l_i < l_j$

↳ if $p_1 > p_2 \dots > p_{N-1} > p_N \rightarrow \ell_{N-1} = \ell_N$

• megvalósítás: binary tree : útvonal $\cong \ell(x)$

~~Lempel-Ziv Lenten-Zipff~~ (LZ 78): Distribution-free data compression

1.) Parsing } (make a dictionary)
2.) Ranking }
3.) ToBinary
4.) Decryption (with dictionary)

Mobile systems,

1G - FDMA (Frequency Division Multiple Access):

↳ a sávszélességet osztjuk ablakokra felhasználónként $M = \frac{B}{b} = \frac{\text{sávszélesség}}{\text{ablak méret}}$, M: felhasználók száma

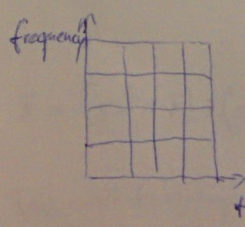
2G - TDMA (Time Division MA):

↳ az idő ablakokra van felosztva, az ablak szét van osztva a felhasználók közt

$$M = \frac{T_{frame}}{T_{chip}} = \frac{f_{chip}}{f_{frame}} \quad , \quad T_{frame} = T_{sample}$$

3G - CDMA/FH (Code DMA / Frequency Hopping):

↳ bináris egymásra ugrott kódok $\Rightarrow$ több felhasználó kódolt tartalmát ~~egy~~ a Multiple Access System egy "kártyán" tudja tárolni, mégha ütközés is van



$M \sim \mathcal{O}(N^2)$

3G - CDMA/DS (Direct Sequence)

↳ $s_i(t)$: signature signal

$$M \leq N = \frac{f_c}{f_s} \quad : \text{chip hossza}$$

Csatorna kapacitás

$$C = \left(\frac{k}{n} =\right) ldN - H(\bar{r}) \quad , \left(\text{def: a küldendő információ és a ténylegesen elküldött információ hányadosa}\right)$$

$$C_{BSC} = 1 - H(P_b) = 1 - P_b \cdot ld\frac{1}{P_b} - (1-P_b)\cdot ld\frac{1}{(1-P_b)} \quad , \; C_{BSC} = 0 \text{, ha } P_b = 0.5$$

$$C = \max_{p(x)} I(X,Y) \underset{\text{symmetric channel esetén}}{=} \max_{p(x)} (H(Y) - H(Y|X)) = ldN - H(\bar{r})$$

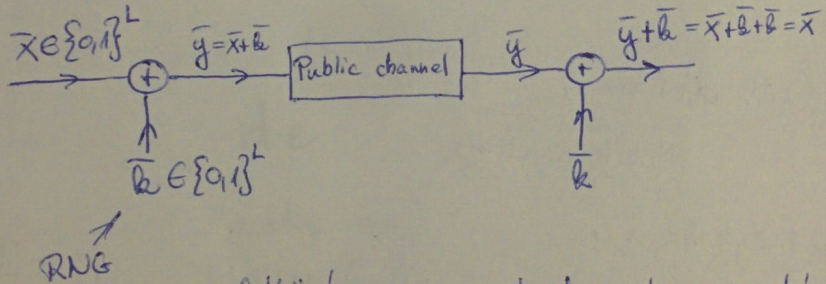
$\bar{r}$: $\bar{\bar{P}}$-nek egy oszlopának az entrópiája

channel matrix: $\bar{\bar{P}}$: • az oszlopok feltételes eloszlások
• az oszlopok egymás permutációi

$$P_{ij} = P(Y = y_i \mid X = x_j)$$

Cryptography

OTP (One Time Pad):



• feltörése: az L hosszú permutációk végigpróbálása ($\mathcal{O}(2^L)$)
• hátrány: kulcsot el kell juttatni a vevő oldalra,
csak L hosszú üzenetet lehet küldeni

Perfect code:

user A : k_A , user B : k_B

1.) $A \to B$: $\bar{x} + k_A = \bar{y}$

2.) $B \to A$: $\bar{y} + k_B = \bar{z}$

3.) $A \to B$: $\bar{z} + k_A = \bar{x} + k_B = \bar{w}$

4.) B : $\bar{w} + k_B = \bar{x}$

↳ probléma : könnyen feltörhető $\bar{y}, \bar{z}, \bar{w}$ összegekként :

$$\bar{y} + \bar{z} + \bar{w} = (\bar{x} + k_A) + (\bar{x} + k_A + k_B) + (\bar{x} + k_B) = \bar{x}$$

— 6 — Csatorna kapacitás tétel III.

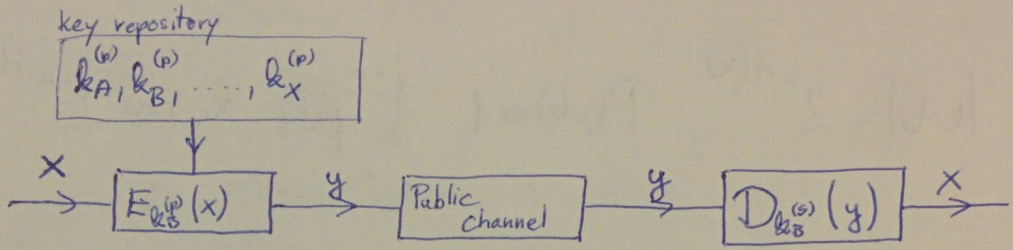
Problems to solve: 1.) commutative functions which are not addition

?.) not transmitting 3-times

Public key cryptography:

users: $A, B, \dots, X$ — p: public (key), s: secret (key)

$k_A^{(p)}$ $k_A^{(s)}$



power function: $\left(X^{k_a}\right)^{k_b} = X^{k_a \cdot k_b} = \left(X^{k_b}\right)^{k_a}$

RSA algorithm:

↳ alapja: prím faktorizáció

1.) p, q: nagy prímek, $N = p \cdot q$, $\varphi(N) = (p-1)\cdot(q-1)$

2.) $e \in \mathbb{Z}$: $1 < e < \varphi(N)$, $(e, \varphi(N)) = 1$ (legnagyobb közös osztó)

3.) d: $d \cdot e = 1 \mod \varphi(N)$, azaz $d \cdot e = 1 + k \cdot \varphi(N)$ $k \in \mathbb{Z}^+$

4.) N, e: public key

d: secret key

↳ folyamat:

kódolás { 1.) az M üzenet tördelése: $m < N$ részekre

kódolás { 2.) $c = m^e \mod N$

dekódolás 3.) $c^d = m \mod N$

Typical set:

$$\mathcal{A} = \left\{ \bar{x} = (x_1 \dots x_n) : 2^{-n H(X) - \varepsilon} \leq p(\bar{x}) \leq 2^{-n H(X) + \varepsilon} \right\}$$

↳ $P(\mathcal{A}) \geq 1 - \varepsilon$

↳ $(1-\varepsilon)\, 2^{n H(X) - \varepsilon} \leq |\mathcal{A}| \leq 2^{n H(X) + \varepsilon}$

⇒ $|\mathcal{A}| \approx 2^{n H(X)}$, $P(\mathcal{A}) \approx 1$, $p(x_1 \dots x_n) \approx 2^{-n H(X)}$