DK spracovanie 2014

$\bar{A}\cdot\bar{x}=\bar{B}$

výslednej mat.

násobenie matíc
1. musí mať toľko stĺpcov koľko druhá riadkov

umocňovať sa dajú len štvorcové matice
$m=n$ $\quad \bar{A}\cdot\bar{A}=\bar{A}^2$
$\bar{A}^2\cdot A=\bar{A}^3$

hodnosť mat. = počet jej LN riadkov

LZ je ak sa dá aspoň jeden riadok vyjadriť ako LK ostatných

char. pol. matice
$p(\lambda)=\det(\lambda I-A)$
I = 1ková mat. $\quad p(\lambda)=\det(A-\lambda I)$

vlastné čísla matice sú korene char. pol. (sú to tie lambdy)

$\boxed{LN \text{ ak } \det\neq 0}$ $\quad \boxed{LZ \text{ ak } \det=0}$

$\Delta mat \Rightarrow \det(A)=\prod diag.(A)$

ak sa $\det(A)\neq 0 \;\exists A^{-1}$

$(A|I)\sim \dots ERO \dots \sim (I|A^{-1})$

$\bar{A}\cdot\bar{A}^{-1}=\bar{A}^{-1}\cdot\bar{A}=I$

$$x_{1,2}=\frac{-b\pm\sqrt{b^2-4ac}}{2a}$$

Crammerovo pravidlo

$a_1x+b_1y+c_1z=d_1$
$a_2x+b_2y+c_2z=d_2$
$a_3x+b_3y+c_3z=d_3$

$$D=\begin{vmatrix}a_1&b_1&c_1\\a_2&b_2&c_2\\a_3&b_3&c_3\end{vmatrix}\qquad D_x=\dots\qquad D_y=\begin{vmatrix}a_1&d_1&c_1\\a_2&d_2&c_2\\a_3&d_3&c_3\end{vmatrix}$$

$$x=\frac{D_x}{D}\quad y=\frac{D_y}{D}\quad z=\frac{D_z}{D}$$

vektory sú LN ak,
$a_1\bar{v}_1+a_2\bar{v}_2\neq 0$
$a_1=0$ a $a_2=0$

Pr. $\bar{v}_1=(1;1;2;1)$
$\bar{v}_2=(1;2;0;1)$

1.) $a_1+a_2=0$
2.) $a_1+2a_2=0$
3.) $2a_1=0$
4.) $a_1+a_2=0$

teda sú LN

Signály RZ; NRZ
UP; BP

NRZ – L (level) [1 +V ; 0 −V]
– M (mark) [1 zmena ; 0 nemení]
– S (space) [0 zmena ; 1 bez zmeny]

RZ – 1 +V na 1/2 intervalu 0 nič [UP]
– 1 — 〃 —— 0 −V na 1/2 [BP]

RZ-AMI – 1 mení polaritu ; 0 nič

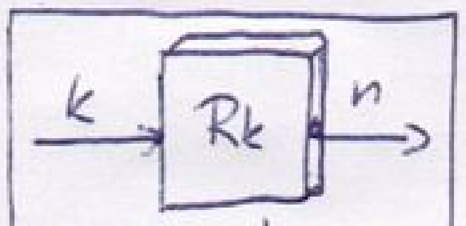
Manchaster – Bi-Ø-L – strieda polaritu
1 v prvej 1/2
0 v druhej 1/2

Bi-Ø-M → 1 ⎍ → 0 ⊔ (alternuje asi)

dicode NRZ → prechody 01 a 10 mena polarity inak nič

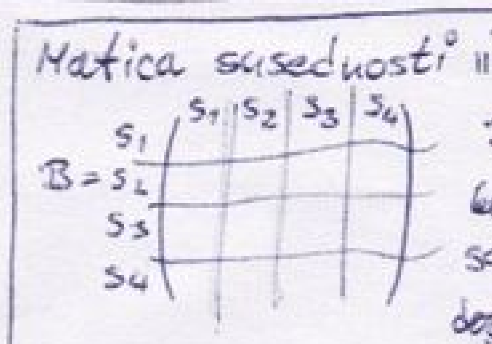
dicode RZ → —〃— po dobu 1/2 intervalu

0 ↑ 1 ↓



$Rk=\frac{k}{n}\leq 1$

Matica susednosti „B^n"



B^n definuje koľkými spôsobmi sa na „n" krokov dostanem zo stavu do stavu

na GF(q) $\quad$ q = počet prvkov {0;1;…;q−1}
$x\oplus y=(x+y)\bmod q$
$x\odot y=(x\cdot y)\bmod q$

Kapacita kanála

$C'=\log_2(\max(root(\underbrace{\det(\lambda I-B)}_{p(\lambda)})))\quad \frac{bit}{symbol}$ $\sim$ $C'=\log_2(\lambda ma$

Prenosová rýchlosť

$R_p=R_m\cdot C'\left[\frac{bit}{s}\right]$
modul. rých.

Nutná podm. ∃ transl. kódu
$Rk\leq C'$; $Rk\leq 1$

Postačujúca podm. ∃ translačného kódu
suma každého riadku B matice musí byť väčšia alebo rovná, alebo kým to neplatí po vyčiarknutí ľubovoľ. riadku a prísl. stĺpca.

$$\sum_j b_{ij}^n\geq 2^k$$

i = informačný vektor (slovo)
– vstupná postupnosť
– má „k" symbolov

c – inf. slovo
– má „n" symbolov

2^k – je počet kódových slov

w_H – váha slova
– počet nenul. prvkov

d_H – ham. vzdialenosť
$d_H(\bar{u};\bar{v})=w(u+v)$

G – gen. mat. (rozmer $k\times n$)

H – kontrolná matica ($(n-k)\times n$)

m = nadbytočnosť ($m=n-k$)

r, v – prijaté slovo

t – počet opraviteľných chýb

$\bar{e}$ – chybové vektory

q – počet prvkov poľa

$g(x)$ – gen. polynóm

$p(x)$ – prvky poľa

r – počet prvkov vo vektore

LBK
LK kódových slov je kódové slovo
$i_1+i_2=k_3 \qquad c_1+c_2=c_3$

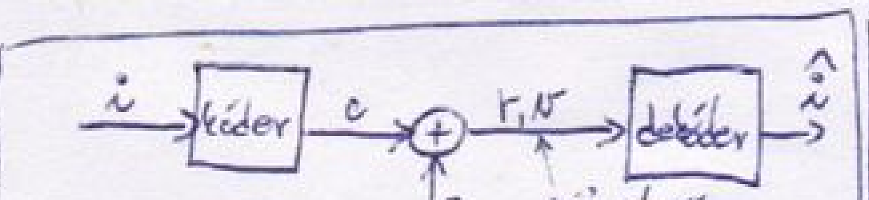
$c=i\cdot G$
$G\cdot H=0$ (princíp ortogon.)
$S=v\cdot H^T$
$S=e\cdot H^T$ $\}$ $\hat{c}=\hat{e}+v$

Syst. tvar LBK
$G=(I_{k\times k}|P)$ $\qquad H=(P^T|I_{n-k})$
paritná mat.

$SumB^n=\begin{pmatrix}\\ \\ \\ \end{pmatrix}\geq$
R

syndrómová tabuľka
počet jej riadkov

$$\sum_{\tau=1}^{t_{kor.}}\binom{n}{\tau}=\frac{n!}{\tau!\cdot(n-\tau)!}$$



$v=c\oplus e$

$v\cdot H^T=(c+e)\cdot H^T=c\cdot H^T+e\cdot H^T=S$

$G\cdot H^T=0\Rightarrow e\cdot H^T=0$

t korekčné
$t_{kor.}=\left\lfloor\frac{d_{min}-1}{2}\right\rfloor$

t detekčné
$t_{det.}=d_{min}-1$

$$\bar{G}_{4x7}=\begin{pmatrix}g_1\\g_2\\g_3\\g_4\end{pmatrix}=\begin{pmatrix} & & \\ & & \end{pmatrix}$$
syst. tvar

$\bar{G}_S=(I_K|P_{(k;n-k)})$ $\Rightarrow \bar{G}_{S(I_k|P_{k\times(n-k)})}\rightarrow P\rightarrow P^T\rightarrow H_{(P^T|I_{n-k})}$ $\quad \bar{G}_{k\times}$

$\bar{G}_S\cdot H^T=0 \qquad G\cdot\bar{H}^T=0$

$\sum\bar{c}=0$

LBK kódovanie

nesyst. $c(x) = i(x) \cdot g(x)$

$\bar{c} = \bar{i} \cdot \bar{G}$

$$\bar{G} = \begin{pmatrix} 1&1&0&0&0&1&0 \\ 0&1&1&1&0&1&0 \\ 0&0&0&1&1&1&0 \\ 0&1&0&1&0&0&1 \end{pmatrix} \cdot \overset{\bar{i}}{\begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}} = \bar{c}$$

syst.

$\bar{c} = \bar{i} \cdot \bar{G}_S$

$$\bar{G}_S = \begin{pmatrix} 1&0&0&0&1&0&1 \\ 0&1&0&0&1&1&1 \\ 0&0&1&0&0&1&1 \\ 0&0&0&1&1&1&0 \end{pmatrix} \cdot \overset{i}{\begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}} = \bar{c}$$

LBK dekódovanie

synd. tab. ①

$\bar{e}$	$\bar{s} = \bar{e} \cdot H^T$
+ kombinácie	
1000000	101
0100000	011
⋮	⋮

② syndrómy prij. slov: $\bar{s} = \bar{v} \cdot H^T$

③ $\hat{c} = \hat{e} + \bar{v}$

Syndróm všeobecne

$\bar{s} = \bar{v} \cdot H^T = e \cdot H^T$

synd. prij. slova — synd. do tabuľky

$GF(2^2)$ — binar, 2miestne

Cyklické kódy

- podmnožina lbk
- sú definované gen. pol. $g(x)$
- cyklické, lebo ich definuje posun

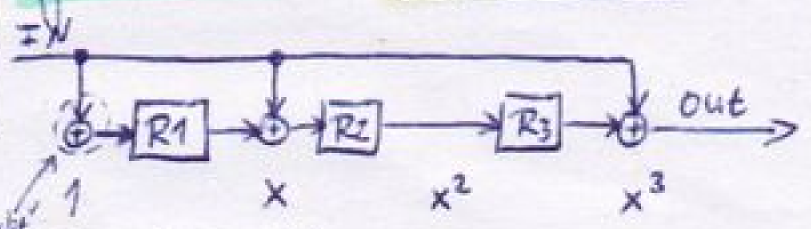
„$\cdot x$" „$\div x$"

$v(x) \cdot \bmod g(x) = (c(x)+e(x)) \bmod g(x) = \underbrace{c(x) \bmod g(x)}_{0 \text{ inak } c(x) \text{ nie je kód. slovo}} + e(x) \bmod g(x) = s(x)$

HW realizácia cyklických kódov

počet reg. = st. $g(x)$

$g(x) = x^3 + x + 1$ nesystematicky



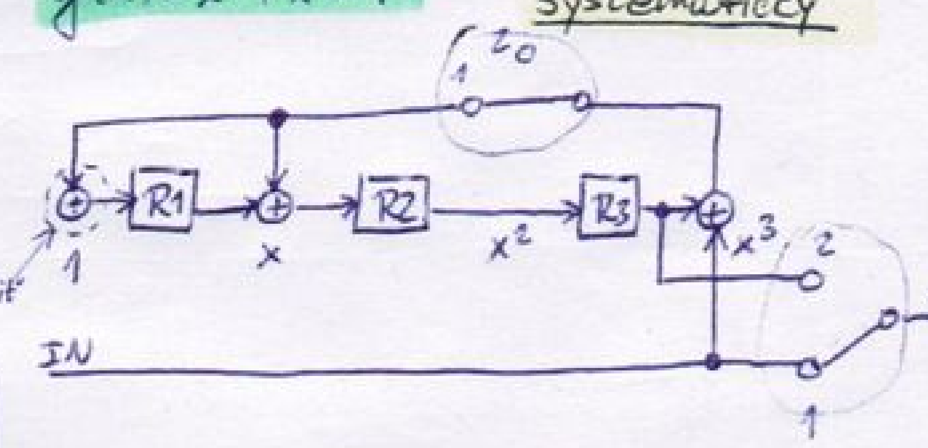
$R_1(t) = IN(t)$

$R2(t) = IN(t) + R1(t-1)$

$R3(t) = R2(t-1)$

$Out(t) = R3(t-1) + IN(t)$

$g(x) = x^3 + x + 1$ systematicky



$R_1(t) = R3(t-1) + IN(t)$

$R2(t) = \underbrace{R3(t-1) + IN(t)}_{R1(t)} + R1(t-1)$

$R3(t) = R2(t-1)$

$Out(t) =$ IN(t) / R3(t-1) (switch)

Cyklické kódy kódovanie

nesyst.

$c(x) = i(x) \cdot g(x)$

syst.

① $i(x) \cdot x^{st.g(x)} \Leftrightarrow i(x) \cdot x^{n-k}$

② $Q(x) = i(x) \cdot x^{st.(g(x))} \cdot \bmod g(x)$

③ $c(x) = i(x) \cdot x^{st(g(x))} + Q(x)$

Cyklické kódy dekódovanie

① vytvorím synd. tab.

e	$e(x)$	$s(x) = e(x) \cdot \bmod g(x)$
1 …	x^6	x^2+1
1 …	x^5	
1 …	x^4	x^2+x+1
⋮	⋮	⋮

② nájdem syndróm slova

$s(x) = v(x) \cdot \bmod g(x)$

③ nájdem synd. v tabuľke

④ $c(x) = v(x) + e(x)$

Konečné polia $GF(p^r)$

$P(x)$ - generátor poľa

r - počet prvkov vo vektoroch

$P(x)$ musí byť ireducibilný, keď ho delí $x^n + 1$; kde $n = 2^r - 1$. n - najmenšie celé číslo, pre kt. to platí

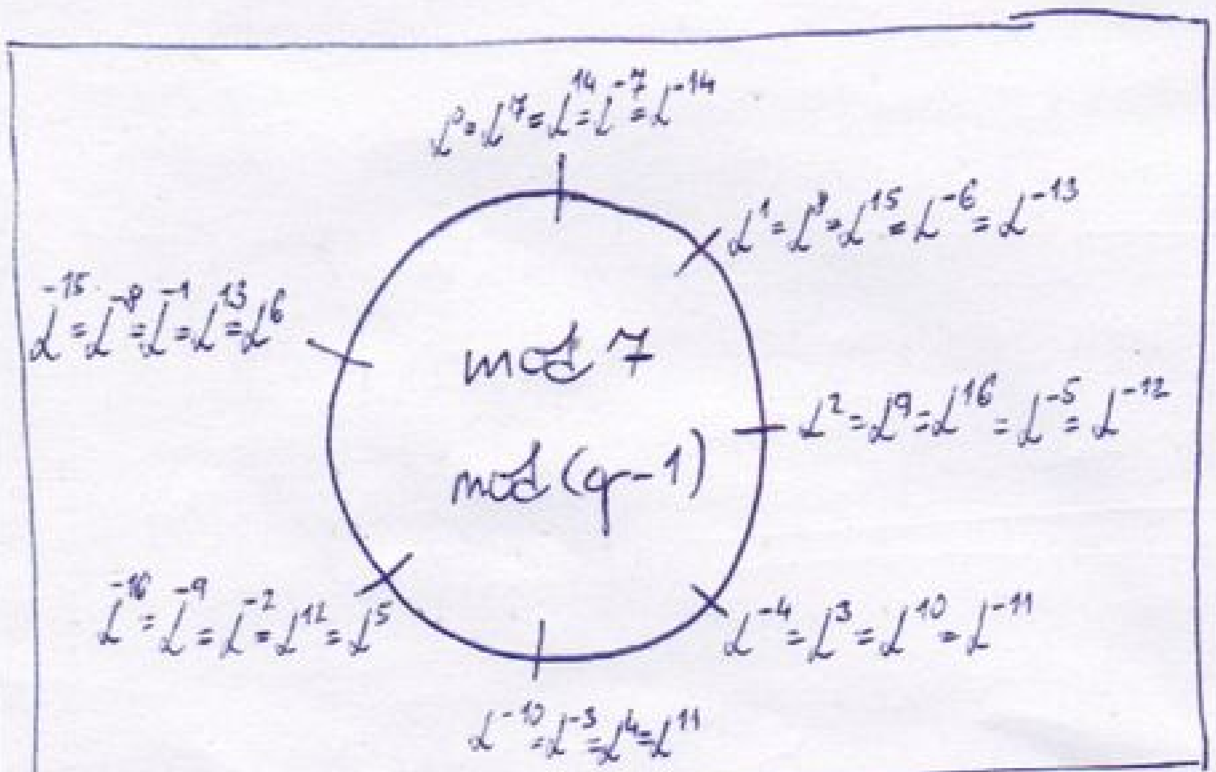
$r = st.\ p(x)$

$\alpha^i \odot \alpha^j = \alpha^{(i+j) \bmod (2^r - 1)}$

$\alpha^i + \alpha^j$ = zrátam binárne (polynomiálne)

$\alpha^i - \alpha^j = \alpha^i + \alpha^j$ (rátam bin.; pol.)

$\alpha^i \div \alpha^j = \alpha^{(i-j)} \bmod (q-1)$



Generovanie prvkov poľa

$\alpha^{-\infty}; \alpha^0; \dots$

pre. GF(8)

$\alpha^r = \alpha^6 = \max.$

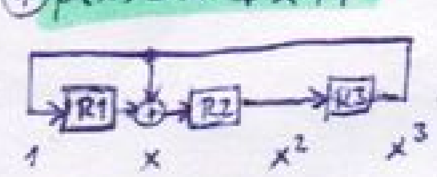
$r = q - 2$

1, x, x^2, ⋮ — $\cdot x \bmod (px)$

$\alpha^{-\infty}$	0
α^0	1
α^2	x
⋮	⋮

- pomocou HW

① $p(x) = x^3 + x + 1$



$R1(t) = R3(t-1)$

$R2(t) = R3(t-1) + R1(t-1) = R1(t-1) + R1(t)$

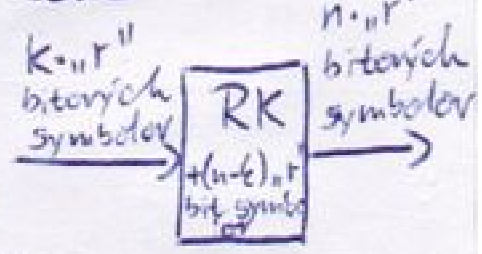
$R3(t) = R2(t-1)$

② inicujem v čase 1 čímkoľvek okrem 0,0,0, napr. 0,1,0

③ rozadím podľa $\alpha^i = x^i$, alebo $\alpha^i = x^i \bmod p(x)$

RS kódy všeobecne

$GF(q) = GF(p^r)$



$n = q - 1 = 2^r - 1$

n - dĺžka kódového slova

k - ‖ - informačného slova

$d_{min} = (n-k) + 1$ ← len RS

$t = \left\lfloor \frac{n-k}{2} \right\rfloor = \left\lfloor \frac{d_{min} - 1}{2} \right\rfloor$ ⇐ len RS počet opr. chýb

$g(x) = (x - \alpha^i)(x - \alpha^{i+1})(x - \alpha^{i+2}) \dots$ 2t po sebe idú.

$2t = n - k$ ← len RS

m - dĺžka kód. slova

$m = 2^r - 1 = st.\ g(x)$

$r = st.\ p(x)$

- je to počet bitov vstupujúcich slov

Vyšetrenie RS kódu $[n, k, d_{min}, t, r, m]$

$n = q - 1 = 2^r - 1$

$r = st.\ p(x)$

$d_{min} = (n-k) + 1$

$m = 2^r - 1 = st.\ g(x)$

$t = \left\lfloor \frac{n-k}{2} \right\rfloor = \left\lfloor \frac{d_{min} - 1}{2} \right\rfloor$

$k = k$

$n - k = 2t$

$g(x) = (x - \alpha^i)(x - \alpha^{i+1})$ $\quad g(x) = x^4 + x^3 \alpha^2 + \dots$

kódovanie RS

nesystematický

$c(x) = i(x) \cdot g(x)$

systematický

① $i(x) \cdot x^m$ $m = n - k = st.\, g(x)$

② $Q(x) = i(x) \cdot x^m \cdot \bmod g(x)$

③ $c(x) = i(x) \cdot x^m + Q(x)$

$g(x)$ má „2t" za sebou idúcich koreňov, až za nepovie inak „$i = 0$"

$i = \alpha^4 ; \alpha^1 ; \alpha^6 ; \alpha^0 ; \alpha^2$

$\bar{i}x = (\alpha^4 x^4 ; \alpha^1 x^3 ; \alpha^6 x^2 ; \alpha^0 x ; \alpha^2 x^0)$

$\bar{i}x = \alpha^4 x^4 + \alpha^1 x^3 + \alpha^6 x^2 + \alpha^0 x + \alpha^2$

pomôcka

$\log_2 x \doteq 3{,}322 \cdot \log_{10} x$

dekódovanie RS

① určím parametre

② vyrátam α ($\cdot x \cdot \bmod p(x)$)

③ syndrómy $\boxed{\bar{s}_k = N(\alpha^k)}$ $k = 0, 1, \dots st\, p(x)$

④ pol. lok pre $\boxed{t=2}$

$$\left.\begin{array}{l} \text{I} \quad \bar{s}_2 + \sigma_1 \bar{s}_1 + \sigma_2 s_0 = 0 \\ \text{II} \quad \bar{s}_3 + \sigma_1 \bar{s}_2 + \sigma_2 \bar{s}_1 = 0 \end{array}\right\} \begin{array}{l} \sigma_1 = \\ \sigma_2 = \end{array}$$

⑤ dosádzam $\alpha^0 - \alpha^6$ do $\boxed{\sigma(x) = x^2 + \sigma_1 x + \sigma_2}$ kde vide 0, tam je chyba $\sigma(\alpha^2) = 0$ $x_1 = \alpha^2$

⑥ hodnota chyby

$$\bar{s}_k = \sum_{i=1}^{t} Y_i \cdot X_i^k$$

$Y_1 =$ } hodnoty
$Y_2 =$ } chyby

„$\bar{d}$" stredná dĺžka kód slova

$$\bar{d} = \sum_{i=1}^{N} p_i \cdot d_i$$

„d_{min}" dolné ohr. dĺžky kód slova

$$\bar{d} \geq d_{min} = \frac{H}{\log_2 q}$$

entropia – str. hodnota množstva informácie

$0 \leq H \leq \log_2 N$
str. hodnota

$I = -\log_2(P_i)$ [bit]
mn. infor.

$E = \sum p_i \cdot I$

$$H = E(I) = \sum_{i=1}^{N} p_i \cdot I = -\sum_{i=1}^{N} p_i \cdot \log(p_i) \left[\frac{bit}{symbol}\right]$$

$$H = -\sum_{i=1}^{N} p_i \cdot \log_2(p_i) \quad \left[\frac{bit}{symbol}\right]$$

efektívnosť kódu

$$\eta = \frac{d_{min}}{\bar{d}} \cdot 100 \ [\%] \quad = \frac{H}{\bar{d}} \cdot 100$$

disperzia

$$A^2 = \sum_{i=1}^{N} (\bar{d} - d_i)^2$$

Shenon – Fano

① zoradím od max. po min. pravd. ?

② rozdelím na pól

③ viac pravd. skupina 0, menej 1

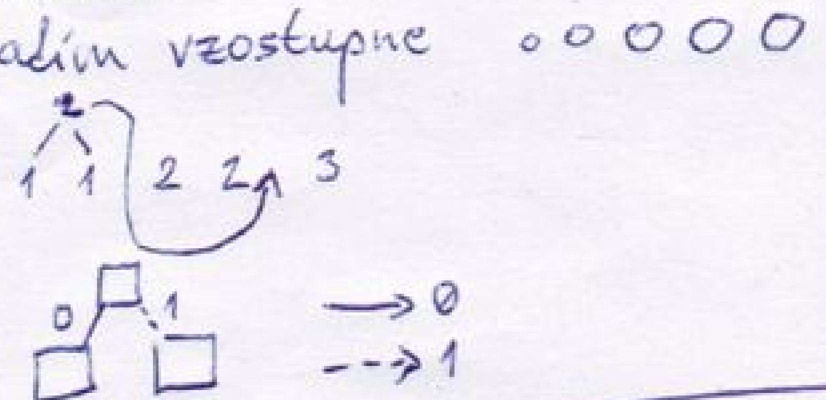
pozn – hore bude vždy väčšia suma

Huffmann

① zoradím vzostupne

②

③ → 0, --→ 1



LZ 77

N	LS
0 – N	1 – N

① inicializujem N → 0ami alebo iným znakom

② do LS vačítam postupnosť

③ adresa = pointer, dĺžka zhody, in. symbol → (x, y, z)

④ posun z LS do N

⑤ opakujem

LZ 78

(adresa ; in(symbol))

0	00	vstup	výstup
1	0	0	(0, 0) ← (0, 0)
2		01	(1, 1) → ...

ternárna sústava