DEKÓDOVÁNÍ PŘIJATÉ ZNAČKY JE VLASTNĚ ROZHODOVÁNÍ O TOM, ZDA JE (PŘIJATÁ) n-TICE PRVKŮ ZADANÉ MNOŽINY n-TIC, KTERÉ PŘEDSTAVUJÍ KOMBINACE, OPRAVOVANÉ NA JEDNU KONKRÉTNÍ KÓDOVOU ZNAČKU.

ÚLOHY TYPU „JE x PRVKEM MNOŽINY M?" ALE UMÍME ZA URČITÝCH PŘEDPOKLADŮ ŘEŠIT EFEKTIVNĚJI, NEŽ POROVNÁVÁNÍM SE VŠEMI PRVKY MNOŽINY M.

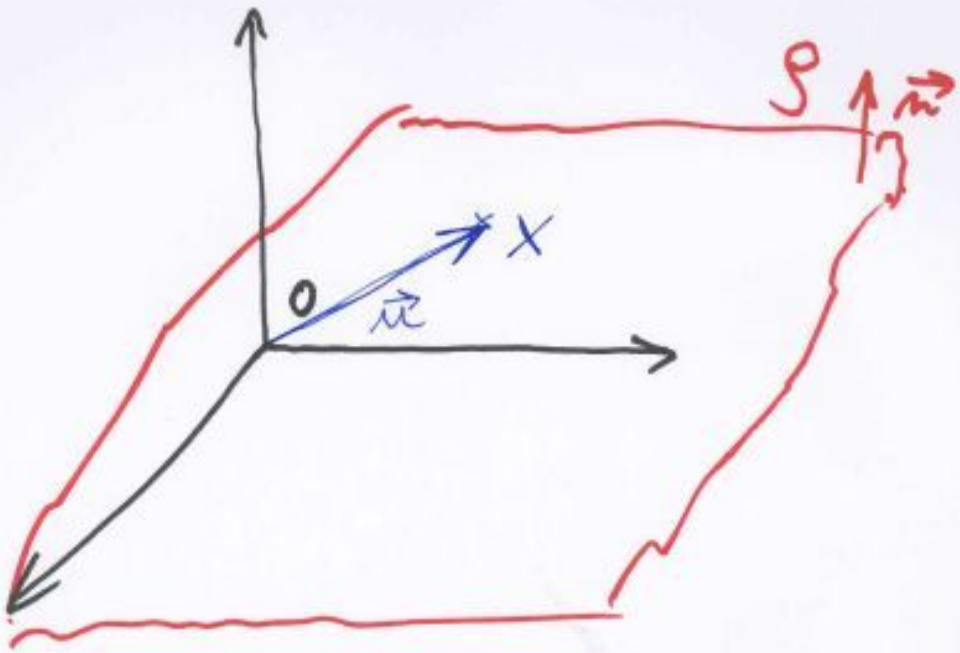
PŘ. Z GEOMETRIE (MOTIVACE):

DÁNA ROVINA ϱ PROCHÁZEJÍCÍ POČÁTKEM SOUŘADNÉ SOUSTAVY.

JE DÁN BOD $X = (x_1, x_2, x_3)$.

JAK ROZHODNEME, ZDA PLATÍ

$$X \overset{?}{\in} \varrho$$



$\vec{n}$ NORMÁLOVÝ VEKTOR ROVINY ρ
(VEKTOR KOLMÝ NA VŠECHNY VEKTORY LEŽÍCÍ V ROVINĚ ρ)

$\vec{x}$ VEKTOR S POČÁTEČNÍM BODEM V POČÁTKU SOUŘADNICOVÉHO SYSTÉMU A KONCOVÝM BODEM X

$\vec{n} \cdot \vec{u} = 0 \iff$ VEKTOR $\vec{u}$ JE SMĚROVÝM VEKTOREM ROVINY ρ, TJ.

BOD X LEŽÍ V ROVINĚ ρ

ZOBECNĚNÍ GEOMETRICKÉ ÚVAHY:

ROVINA ϱ JE LINEÁRNÍ PROSTOR DIMENZE 2 (JE PODPROSTOREM PROSTORU $\mathbb{R}^3$).

K TOMUTO LINEÁRNÍMU PODPROSTORU EXISTUJE LINEÁRNÍ PROSTOR $\varrho^\perp$ DIMENZE JEDNA, KTERÝ JE K NĚMU ORTOGONÁLNÍ ($\varrho^\perp$ JE PODPROSTOREM $\mathbb{R}^3$).

ϱ ... PROSTOR VŠECH VEKTORŮ KOMPLANÁRNÍCH S DANOU ROVINOU.

$\varrho^\perp$ ... PROSTOR VŠECH VEKTORŮ KOLMÝCH K DANÉ ROVINĚ.

$\vec{u} \in \varrho \iff$ JE ORTOGONÁLNÍ NA VŠECHNY PRVKY $\varrho^\perp \iff$ JE ORTOGONÁLNÍ NA VŠECHNY PRVKY BÁZE $\varrho^\perp$, STAČÍ TEDY SPOČÍTAT JEDINÝ SKALÁRNÍ SOUČIN $\vec{u} \cdot \vec{u}$

PŘ ρ : ROVINA OS X A Y

BÁZOVÉ VEKTORY : $e_1 = (1,0,0)$

$e_2 = (0,1,0)$

$\rho^\perp$: $e_1^\perp = (0,0,1)$

$X = [5,3,0]$ $\vec{u} = (5,3,0)$

$\vec{u} \cdot \vec{m} = 5 \cdot 0 + 3 \cdot 0 + 1 \cdot 0 = 0$

$\Rightarrow X \in \rho$

$Y = [5,3,1]$ $\vec{v} = (5,3,1)$

$\vec{v} \cdot \vec{m} = 5 \cdot 0 + 3 \cdot 0 + 1 \cdot 1 = 1$

$\Rightarrow Y \notin \rho$

ZÁVĚR : BEZPEČNOSTNÍ KÓDY BUDEME KONSTRUOVAT JAKO LINEÁRNÍ PROSTORY. ALE NE NAD TĚLESEM REÁLNÝCH ČÍSEL R.

MUSÍME SE NAUČIT VYTVOŘIT TĚLESO Z KONEČNÉ ABECEDY KÓDU T.

TĚLESO JE MNOŽINA T SPOLU SE DVĚMA OPERACEMI $+$ A $\cdot$ TAKOVÝMI, ŽE PLATÍ:

1) $\forall a,b \in T \quad \exists a+b \in T \quad \exists a \cdot b \in T$

2) $\forall a,b,c \in T \quad (a+b)+c = a+(b+c)$

$(a \cdot b) \cdot c = a \cdot (bc)$

3) $\forall a,b \in T \quad a+b = b+a$

$a \cdot b = b \cdot a$

4) $\forall a,b,c \in T \quad a \cdot (b+c) = a \cdot b + a \cdot c$

5) $\exists\, 0 \in T : \quad a+0 = a \quad \forall a \in T$

$\exists\, 1 \in T : \quad a \cdot 1 = a \quad \forall a \in T$

6) $\forall a \in T \quad \exists -a : a+(-a) = 0$

7) $\forall a \in T \; a \neq 0 \quad \exists a^{-1} : a \cdot a^{-1} = 1$

LINEÁRNÍ PROSTOR NAD TĚLESEM T JE MNOŽINA L SPOLU S OPERACEMI $+$ (SČÍTÁNÍ) A $\cdot$ (NÁSOBENÍ SKALÁREM) TAKOVÝMI, ŽE PLATÍ:

1) $\forall a,b \in L \quad \exists\, a+b \in L$ TAKOVÝ, ŽE

$$a+b = b+a \qquad \forall a,b \in L$$

$$(a+b)+c = a+(b+c) \qquad \forall a,b,c \in L$$

$$\exists\, 0 \in L : \quad a+0 = a \qquad \forall a \in L$$

$$\forall a \in L \;\exists\, -a \in L : \quad a+(-a) = 0$$

2) $\forall a \in L \quad \forall \lambda \in T \quad \exists\, \lambda \cdot a \in L$

3) $\forall a,b \in L \quad \forall \alpha, \lambda \in T$ PLATÍ

$$\lambda \cdot (a+b) = \lambda a + \lambda b$$

$$(\alpha\lambda)a = \alpha \cdot (\lambda a)$$

$$(\alpha+\lambda)a = \alpha a + \lambda a$$

$$1 \cdot a = a$$

TĚLESO $\{0,1\}$

OPERACE

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

OVĚŘENÍ VLASTNOSTÍ TĚLESA:

1) DEFINOVÁNO TABULKOU

2)

a	b	c	$(a+b)+c$	$a+(b+c)$	$(ab)c$	$a(bc)$
0	0	0	$0+0=0$	$0+0=0$	0	0
0	1	0	$1+0=1$	$0+1=1$	0	0
0	1	1	$1+1=0$	$0+0=0$	0	0
1	0	0	$1+0=1$	$1+0=1$	0	0
1	0	1	$1+1=0$	$1+1=0$	0	0
1	1	0	$0+0=0$	$1+1=0$	0	0
1	1	1	$0+1=1$	$1+0=1$	1	1
0	0	1	$0+1=1$	$0+1=1$	0	0

3) ZŘEJMÉ Z TABULEK (SYMETRICKÉ)

4) LZE OVĚŘIT PODOBNĚ JAKO U 2)

5) $0 \neq 0$, $1 \neq 1$

6) OPAČNÝ PRVEK K 1 JE 1

K 0 JE 0

7) INVERZNÍ PRVEK K 1 JE 1

ZAVEDEME-LI OPERACI ODEČÍTÁNÍ JAKO PŘIČÍTÁNÍ OPAČNÉHO PRVKU JE VZHLEDEM K G $-1 = 1$, TEDY ODEČÍTÁNÍ JE TOTÉŽ CO PŘIČÍTÁNÍ.

PO ZAVEDENÍ OPERACÍ NAD ZNAKOVÁNÍ MŮŽEME KÓDY POPISOVAT ROVNICEMI:

KÓD ÚPLNÉ KONTROLY PARITY:

$$n_0 + n_2 + \dots + n_n = 0$$

TJ. SUDÝ POČET JEDNIČEK

OPAKOVACÍ KÓD:

$$n_1 + n_2 = 0$$
$$n_1 + n_3 = 0$$
$$\vdots$$
$$n_1 + n_n = 0$$

TJ. $n_1 = n_2$, $n_1 = n_3$, $\dots$, $n_1 = n_n$

ŘEŠENÍ ROVNICE POPISUJÍCÍ KÓD CELKOVÉ KONTROLY PARITY:

MNOŽINA VŠECH ZNAČEK SE SUDÝM POČTEM JEDNIČEK.

ŘEŠENÍ SOUSTAVY ROVNIC POPISUJÍCÍ OPAKOVACÍ KÓD:

$\{00\ldots00, 11\ldots11\}$

PŘ: „KOKTAVÝ KÓD" DÉLKY 6
(KAŽDÝ ZNAK SE V NĚM DVAKRÁT OPAKUJE)

NAPŘ 001111
110011 atd.

ROVNICE KOKTAVÉHO KÓDU:

$$v_1 + v_2 = 0$$
$$v_3 + v_4 = 0$$
$$v_5 + v_6 = 0$$

OBA KÓDY JSOU POPSÁNY SOUSTAVAMI HOMOGENNÍCH LINEÁRNÍCH ROVNIC O n NEZNÁMÝCH. (V PRVNÍ SOUSTAVĚ JE 1 ROVNICE VE DRUHÉ JE $n-1$ ROVNIC).

ŘEŠENÍM (LIBOVOLNÉ) HOMOGENNÍ SOUSTAVY LINEÁRNÍCH ROVNIC JE LINEÁRNÍ PROSTOR, KTERÝ JE PODPROSTOREM T^n.

SOUČET DVOU ŘEŠENÍ $u + w$ JE TAKÉ ŘEŠENÍM.

LIBOVOLNÝ SKALÁRNÍ NÁSOBEK ŘEŠENÍ $\lambda . u$ JE TAKÉ ŘEŠENÍM.

ODLIŠNOSTI OPROTI LINEÁRNÍM PROSTORŮM NAD R:

1) LINEÁRNÍ PROSTOR NAD T JE KONEČNÝ.

2) Z $u + u = 0$ NEVYPLÝVÁ $u = 0$.

PŘ: $(001100) + (001100) = (000000)$

BINÁRNÍ KÓD K SE NAZÝVÁ LINEÁRNÍ KÓD, JESTLIŽE JE PODPROSTOREM LINEÁRNÍHO PROSTORU $\{0,1\}^n$, TJ. JESTLIŽE SOUČET DVOU KÓDOVÝCH SLOV JE KÓDOVÉ SLOVO.
JE-LI K PODPROSTOREM DIMENZE k, HLUVÍME O LINEÁRNÍM (n,k) KÓDU.

PŘ.: KÓD CELKOVÉ KONTROLY PARITY DÉLKY n MÁ DIMENZI $k = n-1$.

BÁZE: $b_1 = 1000\ldots01$
$b_2 = 0100\ldots01$
$\vdots$
$b_{n-1} = 00\ldots011$

JE TO $(n,n-1)$ KÓD

OPAKOVACÍ KÓD DÉLKY n MÁ DIMENZI 1.

BÁZE: $b_1 = 111\ldots11$

JE TO $(n,1)$ KÓD

„KOKTAVÝ KÓD" DÉLKY 6 NA DIMENZI 3.

BÁZE: $b_1 = 110000$ JE TO

$b_2 = 001100$ (6,3)

$b_3 = 000011$ KÓD.

KAŽDÝ PRVEK LINEÁRNÍHO KÓDU LZE VYJÁDŘIT JAKO LINEÁRNÍ KOMBINACI PRVKŮ BÁZE:

$$v = u_1 b_1 + u_2 b_2 + \dots + u_k b_k$$

k-TICE $u_1 u_2 \dots u_k$ PŘEDSTAVUJE LIBOVOLNĚ VOLITELNÉ INFORMAČNÍ ZNAKY.

VZTAH PRO VÝPOČET v PŘEDSTAVUJE KÓDOVÁNÍ INFORMAČNÍCH ZNAKŮ

$$\varphi : \{0,1\}^k \to K$$

DEFINOVANÉ PŘEDPISEM

$$\varphi(u_1 u_2 \dots u_k) = u_1 b_1 + u_2 b_2 + \dots + u_k b_k$$

JE-LI BINÁRNÍ KÓD POPSÁN SOUSTAVOU HOMOGENNÍCH KONTROLNÍCH ROVNIC, NAZÝVÁME MATICI H TÉTO SOUSTAVY **KONTROLNÍ MATICÍ**.

SLOVO $v_1 v_2 \dots v_n$ JE KÓDOVÉ, PRÁVĚ KDYŽ SPLŇUJE SOUSTAVU ROVNIC

$$H \cdot \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

UMÍSTÍME-LI k PRVKŮ BÁZE KÓDU DO MATICE G

$$G = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_k \end{bmatrix}$$

ZÍSKÁME **GENEROVACÍ MATICI KÓDU.**

OBECNÁ TEORIE LINEÁRNÍCH KÓDŮ

LZE ÚVAHY, KTERÉ BYLY PREZENTOVÁNY PRO BINÁRNÍ KÓDY, ZOBECNIT I PRO KÓDOVÉ ABECEDY S JINÝM POČTEM PRVKŮ?

ZKUSÍME NADEFINOVAT OPERACE $\oplus$ A $\odot$ NAD ABECEDAMI $\{0,1,2\}$ ($p-1$) A $\{0,1,2,3\}$ ($p-1$):

$\oplus$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\odot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

OPERACE DEFINUJEME TAKTO:

$$a \oplus b = \begin{cases} a+b, & \text{pokud } a+b \leq p-1 \\ a+b-p, & \text{pokud } a+b \geq p \end{cases}$$

$$a \odot b = ab - kp, \quad k = 0,1,2,\ldots$$

KDE k VOLÍME TAK, ABY

$ab - kp$ BYLO JEDNO Z ČÍSEL $0,1,\ldots,p-1$

DÁ SE UKÁZAT, ŽE TAKTO DEFINOVANÉ OPERACE SPLŇUJÍ VLASTNOSTI TĚLESA.

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\odot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

PROTOŽE SE V TABULCE OPERACE VE SLOUPCI (ŘÁDKU) 2 NIKDE NEVYSKYTUJE 1, ZNAMENÁ TO, ŽE K PRVKU 2 NEEXISTUJE INVERZNÍ PRVEK.
TO ZNAMENÁ, ŽE OPERACE NAD $\{0,1,2,3\}$ NESPLŇUJÍ VLASTNOSTI TĚLESA.

PROTOŽE JINÉ OPERACE NAD MNOŽINAMI $\{0,1\}$, $\{0,1,2\}$ A $\{0,1,2,3\}$ NADEFINOVALI STEJNÝM ZPŮSOBEM, NAD PRVNÍMI DVĚMA MNOŽINAMI SPLŇUJÍ VLASTNOSTI TĚLESA.

TĚLESA Z_p

PRO KAŽDÉ **PRVOČÍSLO** p DEFINUJEME NA MNOŽINĚ $\{0, 1, \dots, p-1\}$ OPERACE $\oplus$ A $\odot$ TAKTO:

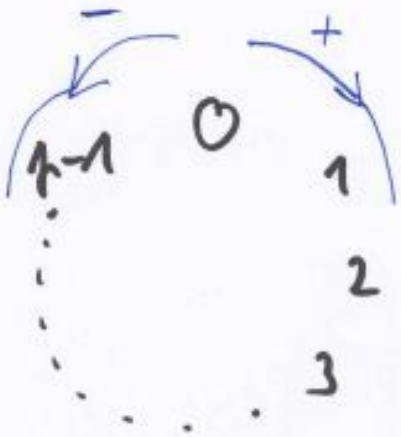
$$a \oplus b = \begin{cases} a+b, & \text{JE-LI } a+b \leq p-1 \\ a+b-p, & \text{JE-LI } a+b \geq p \end{cases}$$

$$a \odot b = ab - k.p, \quad k = 0, 1, 2, \dots$$

KDE k VOLÍME TAK, ABY $ab - kp$ BYLO NĚKTERÝM Z ČÍSEL $\{0, 1, \dots, p-1\}$

PRO KAŽDÉ PRVOČÍSLO TAKTO DEFINOVANÉ OPERACE SPLŇUJÍ VLASTNOSTI TĚLESA, Z_p JE TEDY TĚLESEM.

ILUSTRACE:



ZÁVĚR: EXISTUJÍ TĚLESA O p PRVCÍCH, KDE p JE PRVOČÍSLO.

LZE DOKÁZAT, ŽE EXISTUJÍ I TĚLESA O p^n PRVCÍCH, KDE p JE PRVOČÍSLO A n JE $1, 2, 3, \ldots$ (GALOISOVA TĚLESA).

LINEÁRNÍM KÓDEM ROZUMÍME LINEÁRNÍ PODPROSTOR K PROSTORU T^n (KDE T JE KONEČNÉ TĚLESO).

JE-LI DIMENZE KÓDU k, HLUVÍME O LINEÁRNÍM (n, k) KÓDU.

POKUD $k = 0$ NEBO $k = n$, HOVOŘÍME O TRIVIÁLNÍM KÓDU.

p-ZNAKOVÝ (n, k) KÓD MÁ p^k KÓDOVÝCH SLOV.

GENERUJÍCÍ MATICE G LINEÁRNÍHO (n, k) KÓDU $(k \neq 0)$ JE MATICE TYPU k/n S TĚMITO VLASTNOSTMI:

a) KAŽDÝ ŘÁDEK MATICE JE KÓDOVÝM SLOVEM

b) ŘÁDKY JSOU LINEÁRNĚ NEZÁVISLÉ

c) KAŽDÉ KÓDOVÉ SLOVO JE LINEÁRNÍ KOMBINACÍ ŘÁDKŮ MATICE G.

$$G = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_K \end{bmatrix} = \underbrace{\begin{bmatrix} \quad \end{bmatrix}}_{n} \Big\} k$$

KAŽDÉ KÓDOVÉ SLOVO JE JEDNOZNAČNĚ URČENO SUMÍ SOUČINŮ ČETNÍ V DANÉ BÁZI.

$$\varphi(u_1 u_2 \ldots u_K) = u_1 b_1 + u_2 b_2 + \ldots + u_k b_K =$$

$$= G^T \cdot u \qquad \text{KDE } u \text{ JE SLOUPEC TYPU } k/1$$

OBVYKLÉ ZNAČENÍ:

u .... $k/1$ ... INFORMAČNÍ ČÁST

v .... $n/1$ ... KÓDOVÁ ZNAČKA

G ..... k/n ... GENEROVACÍ MATICE

$v = G^T \cdot u$ ... KÓDOVÁNÍ INFORMAČNÍ ČÁSTI

$n/1$ n/k $k/1$

PŘ. GENEROVACÍCH MATIC BINÁRNÍCH KÓDŮ

PARITNÍ KÓD $G = \begin{bmatrix} 1\,0\,0 \ldots 0\,0\,1 \\ 0\,1\,0 \ldots 0\,0\,1 \\ \vdots \\ 0\,0\,0 \ldots 0\,1\,1 \end{bmatrix}$

OPAKOVACÍ KÓD $G = [1\,1 \ldots\ldots 1\,1]$

„KONTROLNÍ KÓD" $G = \begin{bmatrix} 1\,1\,0\,0\,0\,0 \\ 0\,0\,1\,1\,0\,0 \\ 0\,0\,0\,0\,1\,1 \end{bmatrix}$

PŘÍKLAD TROJKOVÉHO KÓDU ($T = \{0,1,2\}$)
DÉLKY 6.

TŘETÍ ZNAK SLOUŽÍ KE KONTROLE PRVNÍCH DVOU : $a_3 = a_1 + a_2$

ŠESTÝ ZNAK SLOUŽÍ KE KONTROLE ČTVRTÉHO A PÁTÉHO ZNAKU : $a_6 = a_4 + a_5$

ODVOZENÍ KONTROLNÍCH ROVNIC:

$$a_3 = a_1 + a_2 \Rightarrow a_1 + a_2 - a_3 = 0 \Rightarrow$$

$$\Rightarrow a_1 + a_2 + 2a_3 = 0 \quad (\text{PROTOŽE } -1 = 2)$$

ANALOGICKY $a_4 + a_5 + 2a_6 = 0$

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

INFORMAČNÍ ZNAKY — KONTROLNÍ ZNAKY

PŘIROZENÁ BÁZE — DOPOČÍTÁNÍ

EKVIVALENTNÍ KÓDY

DVA BLOKOVÉ KÓDY K a K' DÉLKY n JSOU EKVIVALENTNÍ, JESTLIŽE EXISTUJE PERMUTACE $[\pi_1, \pi_2, \ldots, \pi_n]$ ČÍSEL $1, 2, \ldots, n$ TAKOVÁ, ŽE PLATÍ $\forall\, v_1 v_2 \ldots v_n \in K$:

$$v_1 v_2 \ldots v_n \in K \iff v_{\pi_1} v_{\pi_2} \ldots v_{\pi_n} \in K'$$

JINAK ŘEČENO: KÓDOVÉ ZNAČKY SE LIŠÍ JEN POŘADÍM PRVKŮ VE ZNAČKÁCH.

GENEROVACÍ MATICE SYSTEMATICKÝCH KÓDŮ:

$$G = [I_k \vdots B] \qquad I_k \ldots \text{JEDNOTKOVÁ MATICE ŘÁDU } k$$

$$\begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} = \begin{bmatrix} 1\,0\,\ldots\,0 \\ 0\,1\,\ldots\,0 \\ \ddots\ \vdots \\ 0\,0\,\ldots\,0\,1 \\ b_{11} \\ \ddots \\ b_{n-k,\,k} \end{bmatrix}_{k \times n} \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_k \end{bmatrix} = \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_k \\ \hline v_{k+1} \\ \vdots \\ v_n \end{bmatrix}$$

KAŽDÝ LINEÁRNÍ KÓD JE EKVIVALENTNÍ SE SYSTEMATICKÝM LINEÁRNÍM KÓDEM.

JAK Z GENERUJÍCÍ MATICE G KÓDU K ZKONSTRUOVAT GENERUJÍCÍ MATICI G' SYSTEMATICKÉHO KÓDU K'?

G MÁ k LINEÁRNĚ NEZÁVISLÝCH ŘÁDKŮ, MÁ TEDY I k LINEÁRNĚ NEZÁVISLÝCH SLOUPCŮ.

POKUD JE LINEÁRNĚ NEZÁVISLÝCH PRVNÍCH k SLOUPCŮ MATICE G, ZÍSKÁME G' ELEMENTÁRNÍMI ŘÁDKOVÝMI ÚPRAVAMY. *

POKUD PRVNÍCH k SLOUPCŮ ~~MATICE~~ MATICE G NENÍ LINEÁRNĚ NEZÁVISLÝCH, MUSÍME PROVÉST TAKOVOU PERMUTACI SLOUPCŮ MATICE G, ABYCHOM ZÍSKALI NEZÁVISLÉ SLOUPCE V PRVNÍCH k POZICÍCH. ELEMENTÁRNÍMI ŘÁDKOVÝMI ÚPRAVAMI PAK ZÍSKÁME G'. *

* JINÁ BÁZE TÉHOŽ KÓDU (SPOJNÁ MNOŽINA ZÁKLADEK, JINÉ PŘEKLADY)

* JINÝ KÓD (EKVIVALENTNÍ)