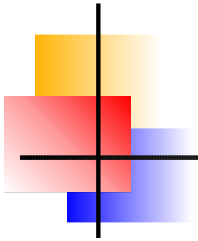
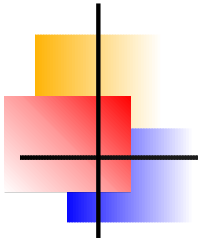


Lineárne kódy

Stanislav Palúch

Fakulta riadenia a informatiky, Žilinská univerzita

23. apríla 2021



Grupa

Grupa je množina G spolu s binárnou operáciou . priraďujúcou každým dvom prvkom $a \in G$, $b \in G$ prvok $a.b$ (krátko len ab) tak, že platí:

(i) $\forall a, b \in G \; ab \in G$

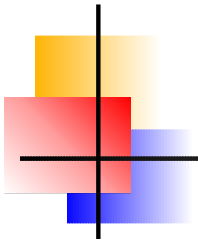
(ii) $\forall a, b, c \in G \; (ab)c = a(bc)$ – asociatívny zákon

(iii) $\exists 1 \in G \; \forall a \in G \quad 1a = a1 = a$ – existencia neutrálneho prvku

(iv) $\forall a \in G \; \exists a^{-1} \in G \quad aa^{-1} = a^{-1}a = 1$ – pre každý prvok grupy existuje inverzný prvok.

Grupa G je komutatívna, ak platí $\forall a, b \in G \; ab = ba$. V tomto prípade sa zvykne grupová operácia zapisovať aditívne, t. j. $a + b$ namiesto $a.b$ a neutrálny prvok sa pri aditívnom zápise označuje ako 0.

Inverzný prvok k prvku a sa v komutatívnom prípade nazýva opačný prvok a označuje sa $-a$.



Teleso

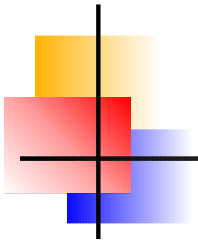
Teleso je množina T obsahujúca (okrem iných prvkov) prvky 0 a 1 spolu s binárnymi operáciami $+$ a $.$ takými, že platí:

(i) Množina T spolu s binárnou operáciou $+$ je komutatívna grupa s neutrálnym prvkom 0.

(ii) Množina $T - \{0\}$ spolu s binárnou operáciou $.$ je komutatívna grupa s neutrálnym prvkom 1.

(iii) $\forall a, b, c \in G \quad a(b + c) = ab + ac$ – platí distributívny zákon

Vlastnosti telesa si možno lepšie uvedomíme, ak (i), (ii), (iii) definície rozpíšeme na jednotlivé konkrétne podmienky, ktoré musí teleso spĺňať:



Teleso

Teleso je množina T obsahujúca (okrem iných prvkov) prvky 0 a 1 spolu s binárnymi operáciami $+$ a $.$ takými, že platí:

(T1) $\forall a, b \in T \; a + b \in T, \; ab \in T$.

(T2) $\forall a, b, c \in T \; a + (b + c) = (a + b) + c, \; a(bc) = (ab)c$ – platia asociatívne zákony.

(T3) $\forall a, b \in T \; a + b = b + a, \; ab = ba$ – platia komutatívne zákony.

(T4) $\forall a, b, c \in T \; a(b + c) = ab + ac$ – platí distributívny zákon.

(T5) $\forall a \in T \; a + 0 = a, \; a.1 = a$ – 0 je neutrálny prvok vzhľadom k operácii „+“, 1 je neutrálny prvok vzhľadom k operácii „.“.

(T6) $\forall a \in T \; \exists(-a) \in T \; a + (-a) = 0$ – ku každému prvku T existuje opačný prvok.

(T7) $\forall a \in T, \; a \neq 0 \; \exists a^{-1} \in T \; a.a^{-1} = 1$ – ku každému nenulovému prvku T existuje inverzný prvok.

Komutatívny okruh s jednotkou

Komutatívny okruh s jednotkou je množina R taká, že $0 \in R$, $1 \in R$ spolu s operáciami $+$ a $.$, v ktorej platia (T1) až (T6).

Príklad

Množina celých čísel spolu s operáciami $+$ a $.$ je komutatívnym okruhom s jednotkou.

Príklad

Faktorový okruh modulo p. *Majme množinu $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$. Na množine $\mathbb{Z}_p$ definujeme operácie $\oplus$, $\otimes$ nasledujúcim spôsobom*

$$a \oplus b = (a + b) \mod p \qquad a \otimes b = (ab) \mod p,$$

kde $n \mod p$ je zvyšok po celočíselnom delení čísla n číslom p. Ľahko sa dá ukázať, že pre ľubovoľné prirodzené číslo $p > 1$ je $\mathbb{Z}_p$ spolu s operáciami $\oplus$, $\otimes$ komutatívnym okruhom s jednotkou, t. j. spĺňa požiadavky (T1) až (T6).

Priklad – okruh $\mathbb{Z}_6$

Príklad

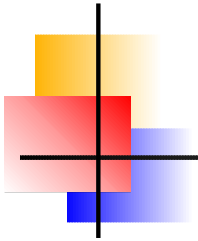
Okruh $\mathbb{Z}_6$ *bude mať nasledujúce tabuľky pre operácie sčítania a násobenia:*

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	5

.	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Podľa vyššie uvedených tabuliek je $5.5 = 1$, *t. j. inverzným prvkom prvku* 5 *je prvok* 5. *Prvky* 2, 3, 4 *vôbec nemajú inverzný prvok. Podmienka (T7) v* $\mathbb{Z}_6$ *nie je splnená –* $\mathbb{Z}_6$ *nie je telesom.*

Pre potreby kódovania budú výhodné také faktorové okruhy $\mathbb{Z}$, ktoré sú telesami.



Priklad – okruh $\mathbb{Z}_6$

Veta

Faktorový okruh $\mathbb{Z}_p$ je telesom práve vtedy, keď p je prvočíslo.

Lineárne priestory nad telesom T.

Nech T je teleso. Lineárnym priestorom nad telesom T je množina $\mathcal{L}$ spolu s binárnou operáciou $+$ (sčítanie) a skalárnou operáciou . (skalárne násobenie) takými, že platí

(L1) $\forall \mathbf{u}, \mathbf{v} \in \mathcal{L}$ a $\forall t \in T \quad u + v \in \mathcal{L}$, $t.\mathbf{u} \in \mathcal{L}$.

(L2) $\forall \mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathcal{L} \qquad \mathbf{u} + (\mathbf{v} + \mathbf{w}) = (\mathbf{u} + \mathbf{v}) + \mathbf{w}$.

(L3) $\forall \mathbf{u}, \mathbf{v} \in \mathcal{L} \qquad \mathbf{u} + \mathbf{b} = \mathbf{b} + \mathbf{u}$.

(L4) $\exists \mathbf{o} \in \mathcal{L}$ také, že $\forall \mathbf{u} \in \mathcal{L} \quad \mathbf{u} + \mathbf{o} = \mathbf{u}$

(L5) $\forall \mathbf{u} \in \mathcal{L} \quad \exists (-\mathbf{u}) \in \mathcal{L}$ také, že $\mathbf{u} + (-\mathbf{u}) = \mathbf{o}$

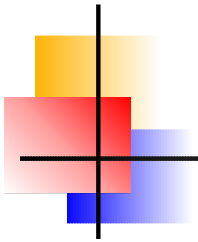
(L6) $\forall \mathbf{u}, \mathbf{v} \in \mathcal{L}$ a $\forall t \in T \quad t.(\mathbf{u} + \mathbf{v}) = t.\mathbf{u} + t.\mathbf{v}$

(L7) $\forall \mathbf{u} \in \mathcal{L}$ a $\forall s, t \in T \quad (s.t)\mathbf{u} = s.(t.\mathbf{u})$

(L8) $\forall \mathbf{u} \in \mathcal{L}$ a $\forall s, t \in T \quad (s + t)\mathbf{u} = s.\mathbf{u} + t.\mathbf{u}$

(L9) $\forall \mathbf{u} \in \mathcal{L} \quad 1.u = u$.

Požiadavky (L1) až (L5) sú ekvivalentné s požiadavkou, aby $(\mathcal{L}, +)$ bola komutatívna grupa s neutrálnym prvkom $\mathbf{o}$. Pre lineárne priestory sa používa synonymum **vektorové priestory**, ich prvky sa volajú **vektory**.



Lineárne priestory nad telesom T.

Vektory $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n$ sa nazývajú **lineárne nezávislé**, ak zo vzťahu $\sum_{i=1}^{n} t_i \mathbf{u}_i = \mathbf{o}$ vyplýva $t_i = 0$ pre $i = 1, 2, \ldots, n$.

Hovoríme, že lineárny priestor $\mathcal{L}$ je **konečne dimenzionálny**, ak existuje také prirodzené číslo k, že každá $k+1$ prvková množina vektorov z $\mathcal{L}$ je lineárne závislá.

V konečne dimenzionálnom priestore majú všetky maximálne lineárne nezávislé množiny vektorov rovnakú mohutnosť.

Mohutnosť n maximálnej lineárne nezávislej podmnožiny $\mathcal{L}$ sa nazýva **dimenzia** lineárneho priestoru $\mathcal{Z}$ – v tomto prípade hovoríme, že priestor je n-dimenzionálny.

Báza konečne dimenzionálneho lineárneho priestoru je ľubovoľná maximálna lineárne nezávislá množina jeho vektorov.

Aritmetický lineárny priestor nad telesom T.

Aritmetický lineárny priestor T^n nad telesom T je priestor n-prvkových postupností typu $\mathbf{u} = u_1 u_2 \dots u_n$, kde $u_i \in T$ a kde je sčítanie a skalárne násobenie definované nasledovne:
Nech $\mathbf{u} = u_1 u_2 \dots u_n$, $\mathbf{v} = v_1 v_2 \dots v_n$, $t \in T$.
Potom

$$\mathbf{u} + \mathbf{v} = (u_1 + v_1)(u_2 + v_2) \dots (u_n + v_n) \qquad t.\mathbf{u} = (tu_1)(tu_2) \dots (tu_n).$$

Skalárny súčin vektorov $\mathbf{u} \in T^n$, $\mathbf{v} \in T^n$ je definovaný nasledovne

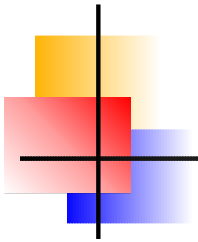
$$\mathbf{u} * \mathbf{v} = u_1 v_1 + u_2 v_2 + \dots + u_n v_n$$

Hovoríme, že vektory $\mathbf{u}$, $\mathbf{v}$ sú **ortogonálne**, ak $\mathbf{u} * \mathbf{v} = 0$.

Dôležitosť priestoru T^n vyplýva z nasledujúcej vety:

Veta

Každý n-dimenzionálny vektorový priestor nad telesom T je izomorfný s priestorom T^n.



Význam aritmetického lineárneho priestoru T^n

V teórii lineárnych kódov sa vychádza z toho, že na kódovej abecede sú dané operácie $+$ a $.$, s ktorými je táto abeceda konečným telesom.

Potom sa na množinu všetkých n-znakových slov v kódovej abecede možno pozerať ako na n-dimenzionálny lineárny priestor.

Jediné konečné telesá sú telesá typu $\mathbb{Z}_p$ pre p prvočíslo a tzv. Galoisove polia typu $GF(p^n)$, kde p je prvočíslo s počtom prvkov p^n.

Mohutnosť kódovej abecedy je pre takéto úvahy obmedzená na čísla typu p^n, kde p je prvočíslo, t. j. 2,3,4,5,7,8,9,11,13,16,17. . . , ale nemôže byť 6,10,12,14,15 lebo tieto čísla nie sú mocninami prvočísel.

Tieto obmedzenia však nie sú tragické, pretože najdôležitejšou kódovou abecedou je binárna abeceda, pre abecedy s väčším počtom znakov použijeme najbližšie teleso s väčším počtom prvkov s tým, že niektoré z nich na reprezentáciu znakov abecedy A nevyužijeme.

Definícia

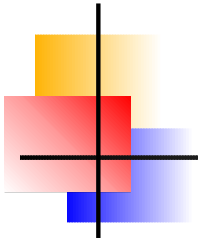
Kód $\mathcal{K}$ sa nazýva **lineárny** (n, k)**-kód**, *ak je podpriestorom dimenzie k lineárneho priestoru A^n, t. j. ak* $\dim(\mathcal{K}) = k$, *a pre ľubovoľné* $\mathbf{a}, \mathbf{b} \in \mathcal{K}$ *a ľubovoľné $c \in A$ je*

$$\mathbf{a} + \mathbf{b} \in \mathcal{K}, \qquad c.\mathbf{a} \in \mathcal{K}.$$

Lineárny (n, k)-kód ako k-dimenzionálny podpriestor priestoru A^n musí mať k-prvkovú bázu $\mathbf{B} = \{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k\}$. Potom každé kódové slovo $\mathbf{a} \in A^n$ má jednoznačné vyjadrenie

$$\mathbf{a} = a_1\mathbf{b}_1 + a_2\mathbf{b}_2 + \cdots + a_k\mathbf{b}_k, \tag{1}$$

kde $a_1, a_2, \ldots, a_n$ sú súradnice vektora $\mathbf{a}$ v báze $\mathbf{B}$. Ak $|A| = p$, potom na mieste každého a_i môže stáť p rôznych čísel, z čoho vyplýva, že existuje p^k rôznych k-tic $a_1, a_2, \ldots, a_k$, dosadením ktorých do (1) dostaneme p^k rôznych kódových slov kódu $\mathcal{K}$. Lineárny (n, k)-kód má teda p^k slov.



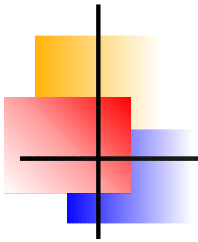
Lineárne kódy

Zobrazenie $\phi : A^k \to A^n$ definované

$$\forall(a_1 a_2 \dots a_k) \in A^k \quad \phi(a_1 a_2 \dots a_k) = a_1\mathbf{b}_1 + a_2\mathbf{b}_2 + \cdots + a_k\mathbf{b}_k.$$

Zobrazenie ϕ je vzájomne jednoznačné zobrazenie $A^k \leftrightarrow \mathcal{K}$ a teda podľa definície má lineárny (n, k)-kód $\mathcal{K}$ k informačných a $n - k$ kontrolných znakov.

Zobrazenie ϕ je kódovanie informačných znakov.



Dohoda o maticových zápisoch

Slová – t. j. vektory $\mathbf{a} \in A^n$ – budeme v maticových zápisoch vždy považovať za **stĺpcové matice**, t. j. ak $\mathbf{a} = a_1 a_2 \ldots a_k$ sa vyskytne v maticovom zápise, budeme predpokladať, že

$$\mathbf{a} = \begin{bmatrix} a_1 \\ a_2 \\ \ldots \\ a_k \end{bmatrix} .$$

Ak budeme potrebovať vektor $\mathbf{a}$ v tvare jednoriadkovej matice, zapíšeme ho ako transponovanú maticu $\mathbf{a}^T$, t. j.

$$\mathbf{a}^T = \begin{bmatrix} a_1 & a_2 & \ldots & a_k \end{bmatrix} .$$

Skalárny súčin dvoch vektorov $\mathbf{u}$, $\mathbf{v} \in A^n$ môžeme považovať za súčin matíc a zapísať ako $\mathbf{u}^T.\mathbf{v}$.

Definícia

Nech $\mathcal{K}$ je lineárny (n, k)-kód, nech $\mathbf{B} = \{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k\}$ je ľubovoľná báza kódu $\mathcal{K}$. Nech $\mathbf{b}_i = (b_{i1}\ b_{i2} \ldots b_{in})^T$ pre $i = 1, 2, \ldots, k$. Potom matica

$$\mathbf{G} = \begin{bmatrix} \mathbf{b}_1^T \\ \mathbf{b}_2^T \\ \ldots \\ \mathbf{b}_k^T \end{bmatrix} = \begin{bmatrix} b_{11} & b_{12} & \ldots & b_{1n} \\ b_{21} & b_{22} & \ldots & b_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ b_{k1} & b_{k2} & \ldots & b_{kn} \end{bmatrix} \tag{2}$$

typu $(k \times n)$ sa nazýva **generujúca matica kódu $\mathcal{K}$.**

Poznámka

Podľa tejto definície je generujúcou maticou kódu $\mathcal{K}$ každá matica, ktorej

a) *každý riadok je kódovým slovom,*

b) *riadky sú lineárne nezávislé, takže hodnosť matice $\mathbf{G}$ sa rovná k,*

c) *každé kódové slovo je lineárnou kombináciou riadkov matice.*

Generujúca matica

Ak teda z matice $\mathbf{G}$ vytvoríme ekvivalentnými riadkovými úpravami ekvivalentnú maticu $\mathbf{G}'$, potom aj matica $\mathbf{G}'$ je generujúcou maticou kódu $\mathcal{K}$.

Poznámka

Nech má lineárny (n, k)-kód pre bázu $\mathbf{B} = \{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k\}$ generujúcu maticu (19). Ak má slovo $\mathbf{a} = a_1 a_2 \ldots a_n$ súradnice $u_1, u_2, \ldots, u_k$ v báze $\mathbf{B}$, potom

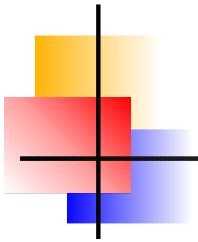
$$\mathbf{a}^T = u_1\mathbf{b}_1^T + u_2\mathbf{b}_2^T + \cdots + u_k\mathbf{b}_k^T = \begin{bmatrix} u_1 & u_2 & \ldots & u_k \end{bmatrix} . \begin{bmatrix} \mathbf{b}_1^T \\ \mathbf{b}_2^T \\ \ldots \\ \mathbf{b}_k^T \end{bmatrix},$$

alebo po rozpísaní vektorov $\mathbf{b}_i^T$ podrobnejšie

$$\begin{bmatrix} a_1 & a_2 & \ldots & a_n \end{bmatrix} = \begin{bmatrix} u_1 & u_2 & \ldots & u_k \end{bmatrix} . \begin{bmatrix} b_{11} & b_{12} & \ldots & b_{1n} \\ b_{21} & b_{22} & \ldots & b_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ b_{k1} & b_{k2} & \ldots & b_{kn} \end{bmatrix},$$

alebo krátko

$$\mathbf{a}^T = \mathbf{u}^T . \mathbf{G} .$$



Príklady lineárnych kódov

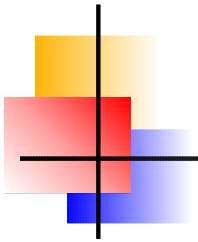
Príklady lineárnych kódov.

a) Binárny kód dĺžky 4 s kontrolou parity – lineárny $(4, 3)$-kód:
$\mathcal{K} \subset A^4, \quad A = \{0, 1\}:$ $0000, \quad 0011, \quad 0101, \quad 0110$
$1001, \quad 1010, \quad 1100, \quad 1111$
Báza: $B = \{0011, 0101, 1001\}$.

$$\text{Generujúca matica} \quad \mathbf{G} = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

b) Ternárny opakovací kód dĺžky 5 – lineárny $(5, 1)$-kód :
$\mathcal{K} \subset A^5, \quad A = \{0, 1, 2\}:$ $00000, 11111, 22222$
Báza: $\{11111\}$.

$$\text{Generujúca matica} \quad \mathbf{G} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$



Príklady lineárnych kódov

c) Binárny zdvojovací kód dĺžky 6 – lineárny $(6, 3)$-kód :

$\mathcal{K} \subset A^6, \quad A = \{0, 1\}$: 000000, 000011, 001100, 001111
110000, 110011, 111100, 111111

Báza: $\{000011, 001100, 110000\}$.

Generujúca matica $\mathbf{G} = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$

d) Dekadický kód dĺžky n s kontrolnou číslicou modulo 10 nie je lineárnym kódom, lebo neexistuje konečné teleso s počtom prvkov 10.

Definícia

Hovoríme, že dva blokové kódy $\mathcal{K}$, $\mathcal{K}'$ dĺžky n sú **ekvivalentné**, *ak existuje permutácia π množiny $\{1, 2, \ldots, n\}$ taká, že platí*

$$\forall a_1 a_2 \ldots a_n \in A^n \quad a_1 a_2 \ldots a_n \in \mathcal{K} \quad \text{práve vtedy, keď} \quad a_{\pi[1]} a_{\pi[2]} \ldots a_{\pi[n]} \in \mathcal{K}' .$$

Podľa definície je blokový kód $\mathcal{K}$ s k informačnými a $n - k$ kontrolnými znakmi systematický, ak ku každému $a_1 a_2 \ldots a_k \in A^k$ existuje práve jedno kódové slovo $\mathbf{a} \in \mathcal{K}$ s prefixom $a_1 a_2 \ldots a_k \in A^k$.

Ako sme už ukázali, lineárny (n, k)-kód je kódom s k informačnými a $n - k$ kontrolnými znakmi, avšak nemusí byť systematický.

Zdvojovací kód je $n = 2k$ je lineárny kód, ktorý nie je systematický, ak $k > 1$. Stačí však zmeniť poradie znakov v slove $a_1 a_2, \ldots a_n$ – dať najprv znaky na nepárnych miestach a potom znaky na párnych miestach a takto získaný nový kód je už systematický.

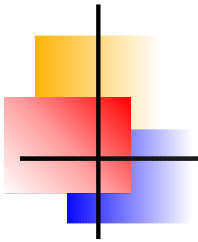
Toto sa dá urobiť s každým lineárnym (n, k)-kódom.

Veta

Lineárny (n, k)-kód $\mathcal{K}$ je systematický práve vtedy, keď k nemu existuje generujúca matica $\mathbf{G}$ *typu:*

$$\mathbf{G} = \left[\begin{array}{c|c} \mathbf{E} & \mathbf{B} \end{array} \right] = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 & b_{11} & b_{12} & \dots & h_{1n-k} \\ 0 & 1 & 0 & \dots & 0 & b_{21} & b_{22} & \dots & b_{2n-k} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & b_{k1} & h_{k2} & \dots & h_{kn-k} \end{bmatrix} . \quad (3)$$

Dôkaz.
Nech (3) je generujúcou maticou pre kód $\mathcal{K}$. Nech $\mathbf{u} = u_1, u_2, \dots u_k$ sú súradnice slova $\mathbf{a} = a_1 a_2 \dots a_n \in \mathcal{K}$ v báze, ktorú tvoria riadky generujúcej matice $\mathbf{G}$.
Potom podľa je $\mathbf{a}^T = \mathbf{b}^T.\mathbf{G}$.



Lineárne kódy

Špeciálne pre $\mathbf{u} = a_1 a_2 \ldots a_k$ je

$$\mathbf{u}^T.\mathbf{G} = \begin{bmatrix} a_1 & a_2 & \ldots & a_k \end{bmatrix}. \begin{bmatrix} 1 & 0 & 0 & \ldots & 0 & b_{11} & b_{12} & \ldots & b_{1n-k} \\ 0 & 1 & 0 & \ldots & 0 & b_{21} & b_{22} & \ldots & b_{2n-k} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 1 & b_{k1} & b_{k2} & \ldots & b_{kn-k} \end{bmatrix} =$$

$$= \begin{bmatrix} a_1 & a_2 & \ldots & a_k & v_{k+1} & \ldots & v_n \end{bmatrix},$$

kde v_{k+i} je jednoznačne určené vzťahom:

$$v_{k+i} = \begin{bmatrix} a_1 & a_2 & \ldots & a_k \end{bmatrix}. \begin{bmatrix} b_{1i} \\ b_{2i} \\ \ldots \\ b_{ki} \end{bmatrix}.$$

Pre každé $a_1 a_2 \ldots a_k \in A^k$ existuje práve jedno slovo kódu $\mathcal{K}$ s prefixom $a_1 a_2 \ldots a_k$. Kód $\mathcal{K}$ je teda systematický.

Lineárne kódy

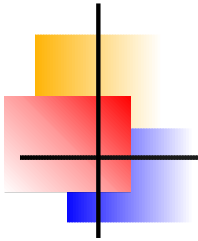
Nech je kód $\mathcal{K}$ systematický. Ak sú prvé k stĺpce generujúcej matice $\mathbf{G}$ lineárne nezávislé, riadkovými ekvivalentnými úpravami ju môžeme previesť na ekvivalentnú maticu $\mathbf{G}'$ v tvare $\mathbf{G}' = \left[\begin{array}{c|c} \mathbf{E} & \mathbf{B} \end{array}\right]$, ktorá je tiež generujúcou maticou kódu $\mathcal{K}$.

Nech teda prvé k stĺpce generujúcej matice $\mathbf{G}$ systematického kódu $\mathcal{K}$ nie sú lineárne závislé. Potom ju môžeme ekvivalentnými riadkovými úpravami transformovať na ekvivalentný tvar

$$\mathbf{G}' = \left[\begin{array}{ccccc|ccccc} d_{11} & d_{12} & d_{13} & \dots & d_{1k} & d_{1(k+1)} & d_{1(k+2)} & \dots & d_{1n} \\ d_{21} & d_{22} & d_{23} & \dots & d_{2k} & d_{2(k+1)} & d_{2(k+2)} & \dots & d_{2n} \\ \multicolumn{5}{c|}{\dots\dots\dots\dots\dots} & \multicolumn{4}{c}{\dots\dots\dots\dots\dots} \\ d_{(k-1)1} & d_{(k-1)2} & d_{(k-1)3} & \dots & d_{(k-1)k} & d_{(k-1)(k+1)} & d_{(k-1)(k+2)} & \dots & d_{(k-1)n} \\ 0 & 0 & 0 & \dots & 0 & d_{k(k+1)} & d_{k(k+2)} & \dots & d_{kn} \end{array}\right]$$

Matica $\mathbf{G}'$ má hodnosť k, pretože je ekvivalentná s maticou $\mathbf{G}$, ktorá mala k lineárne nezávislých riadkov. Pre $\mathbf{u}, \mathbf{v} \in A^k$ také, že $\mathbf{u} \neq \mathbf{v}$ je $\mathbf{u}^T.\mathbf{G}' \neq \mathbf{v}^T.\mathbf{G}'$. Všimnime si, že prvých k súradníc vektora $\mathbf{u}^T.\mathbf{G}$ nezávisí na k-tej súradnici vektora $\mathbf{u}$, z čoho vyplýva, že existuje niekoľko kódových slov kódu $\mathcal{K}$ s rovnakým prefixom a teda kód $\mathcal{K}$ nie je systematický.

Z predpokladu, že prvé k stĺpce generujúcej matice sú závislé, sme dostali spor. □



Dôsledok. Lineárny (n, k)-kód $\mathcal{K}$ je systematický práve vtedy, keď jeho ľubovoľná generujúca matica $\mathbf{G}$ má prvé k stĺpce lineárne nezávislé.

Veta

Každý lineárny (n, k)-kód $\mathcal{K}$ je ekvivalentný so systematickým lineárnym kódom.

Kontrolná matica lineárneho kódu

Definícia

Kontrolná matica lineárneho kódu $\mathcal{K}$ *je taká matica* $\mathbf{H}$ *prvkov kódovej abecedy A, pre ktorú platí: Slovo* $\mathbf{v} = v_1 v_2 \dots v_n$ *je kódové práve vtedy, keď*

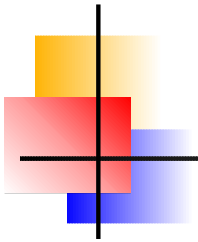
$$\mathbf{H}.\mathbf{v} = \begin{bmatrix} h_{11} & h_{12} & \dots & h_{1n} \\ h_{21} & h_{22} & \dots & h_{2n} \\ \dots & \dots & \dots & \dots \\ h_{m1} & h_{m2} & \dots & h_{mn} \end{bmatrix} . \begin{bmatrix} v_1 \\ v_2 \\ \dots \\ v_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \dots \\ 0 \end{bmatrix} = \mathbf{o} \ . \tag{4}$$

Stručnejšie: $\mathbf{v} \in \mathcal{K}$ *práve vtedy, keď* $\mathbf{H}.\mathbf{v} = \mathbf{o}$.

Majme lineárny (n, k)-kód $\mathcal{K}$ s generujúcou maticou

$$\mathbf{G} = \begin{bmatrix} \mathbf{b}_1^T \\ \mathbf{b}_2^T \\ \dots \\ \mathbf{b}_k^T \end{bmatrix} = \begin{bmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \dots & \dots & \dots & \dots \\ b_{k1} & b_{k2} & \dots & b_{kn} \end{bmatrix} \tag{5}$$

typu $(k \times n)$. Aká má byť kontrolná matica kódu $\mathcal{K}$ t. j. matica $\mathbf{H}$ taká, že $\mathbf{H}.\mathbf{u} = \mathbf{o}$ práve vtedy, keď $\mathbf{u} \in \mathcal{K}$?



Kontrolná matica lineárneho kódu

Prvé, čo o matici $\mathbf{H}$ vieme povedať, je, že má mať n stĺpcov (už len preto, aby $\mathbf{H}.\mathbf{u}$ bolo definované pre $\mathbf{u} \in A^n$).

Množina všetkých $\mathbf{u} \in A^n$ takých, že $\mathbf{H}.\mathbf{u} = \mathbf{o}$ je podpriestor priestoru A^n dimenzie rovnej $n - \dim(\mathbf{H}) = \dim(\mathcal{K}) = k$, odkiaľ $\dim(\mathbf{H}) = n - k$.
Stačí teda hľadať maticu $\mathbf{H}$ ako maticu typu $((n-k) \times n)$ s $n-k$ lineárne nezávislými riadkami.

Nech $\mathbf{h}^T$ je riadok matice $\mathbf{H}$.
Potom pre každé kódové slovo $\mathbf{u} \in \mathcal{K}$ musí byť

$$\mathbf{u}^T.\mathbf{h} = u_1 h_1 + u_2 h_2 + \cdots + u_n h_n = 0 \ . \tag{6}$$

Mohli by sme teda zostaviť sústavu $p^k = |\mathcal{K}|$ lineárnych rovníc typu (26), kde by $\mathbf{u}$ prebiehalo všetky kódové slová kódu $\mathcal{K}$.
Takýto systém lineárnych rovníc by však obsahoval príliš veľa lineárne závislých rovníc.

Kontrolná matica lineárneho kódu

Stačí totiž,

$$\mathbf{u}^T.\mathbf{h} = u_1h_1 + u_2h_2 + \cdots + u_nh_n = 0 \ .$$

platilo pre všetky prvky bázy podpriestoru $\mathcal{K}$, potom bude (26) platiť aj pre všetky prvky podpriestoru $\mathcal{K}$.
Pre $\mathbf{h}$ možno zostaviť túto sústavu lineárnych rovníc:

$$\left.\begin{array}{rcl} \mathbf{b}_1^T.\mathbf{h} & = & 0 \\ \mathbf{b}_2^T.\mathbf{h} & = & 0 \\ \cdots & & \\ \mathbf{b}^T.\mathbf{h} & = & 0 \end{array}\right\},$$

čo sa dá v maticovom tvare zapísať

$$\mathbf{G}.\mathbf{h} = \mathbf{o} \ . \tag{7}$$

Keďže dimenzia matice $\mathbf{G}$ je k, množina všetkých riešení sústavy (7) je podpriestor dimenzie $(n-k)$ a preto možno nájsť $(n-k)$ lineárne nezávislých riešení sústavy (7) $\mathbf{h}_1, \mathbf{h}_2, \ldots, \mathbf{h}_{n-k}$, ktoré budú riadkami hľadanej kontrolnej matice $\mathbf{H}$, t. j.

$$\mathbf{H} = \begin{bmatrix} \mathbf{h}_1^T \\ \mathbf{h}_2^T \\ \cdots \\ \mathbf{h}_{n-k}^T \end{bmatrix} .$$

Kontrolná matica lineárneho kódu

Všimnime si, že

$$\mathbf{G}.\mathbf{H}^T = \begin{bmatrix} \mathbf{b}_1^T \\ \mathbf{b}_2^T \\ \dots \\ \mathbf{b}_k^T \end{bmatrix}_{k\times n} \begin{bmatrix} \mathbf{h}_1 & \mathbf{h}_2 & \dots & \mathbf{h}_{n-k} \end{bmatrix}_{n\times(n-k)} = \begin{bmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 \end{bmatrix}_{k\times(n-k)} .$$

Majme maticu $\mathbf{H}$ typu $((n-k)\times n)$ dimenzie $\dim(\mathbf{H}) = (n-k)$ pre ktorú platí $\mathbf{G}.\mathbf{H}^T = \mathbf{O}_{k\times(n-k)}$, kde $\mathbf{O}_{k\times(n-k)}$ je nulová matica typu $(k\times(n-k))$.

Označme $\mathcal{N} \subseteq A^n$ priestor všetkých riešení rovnice $\mathbf{H}\mathbf{u} = \mathbf{o}$.
Keďže pre všetky prvky bázy kódu $\mathcal{K}$ platí $\mathbf{H}.\mathbf{b}_i = \mathbf{o}$, $i = 1, 2, \dots k$,
platí aj pre ľubovoľné kódové slovo $\mathbf{u} \in \mathcal{K}$, $\mathbf{u} = \sum_{i=1}^{k} u_i\mathbf{b}_i$:

$$\mathbf{H}.\mathbf{u} = \mathbf{H}.\sum_{i=1}^{k} u_i\mathbf{b}_i = \sum_{i=1}^{k} \mathbf{H}.(u_i\mathbf{b}_i) = \sum_{i=1}^{k} u_i(\mathbf{H}.\mathbf{b}_i) = \sum_{i=1}^{k} u_i.\mathbf{o} = \mathbf{o} .$$

Máme teda $\mathcal{K} \subseteq \mathcal{N}$. Pretože $\dim(\mathbf{H}) = (n-k)$, $\dim(\mathcal{N})$ sa rovná
$n - \dim(\mathbf{H}) = k$.
Keďže $\mathcal{K} \subseteq \mathcal{N}$ je báza $\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_k$ bázou priestoru $\mathcal{N}$, a teda $\mathcal{K} = \mathcal{N}$.

Veta

Nech $\mathcal{K}$ je lineárny (n, k)-kód s generujúcou maticou $\mathbf{G}$ typu $(k \times n)$. Potom matica $\mathbf{H}$ typu $((n-k) \times n)$ je kontrolnou maticou kódu $\mathcal{K}$ práve vtedy, keď

$$\dim(\mathbf{H}) = (n-k) \quad a \quad \mathbf{G}.\mathbf{H}^T = \mathbf{O}_{k\times(n-k)}, \tag{8}$$

kde $\mathbf{O}_{k\times(n-k)}$ je nulová matica typu $(k \times (n-k))$.

Veta

Lineárny (n, k)-kód $\mathcal{K}$ s generujúcou maticou $\mathbf{G} = \left[\ \mathbf{E}_{k\times k} \mid \mathbf{B}\ \right]$ má kontrolnú maticu $\mathbf{H} = \left[\ -\mathbf{B}^T \mid \mathbf{E}_{(n-k)\times(n-k)}\ \right]$.

Dôkaz. Označme $m = n - k$. Potom môžeme matice $\mathbf{G}$, $\mathbf{H}$ rozpísať nasledovne:

$$\mathbf{G} = \begin{bmatrix} \mathbf{b}_1^T \\ \mathbf{b}_2^T \\ \dots \\ \mathbf{b}_p^T \\ \dots \\ \mathbf{b}_k^T \end{bmatrix} = \left[\begin{array}{cccccc|cccccc} 1 & 0 & \dots & 0 & \dots & 0 & b_{11} & b_{12} & \dots & b_{1q} & \dots & b_{1m} \\ 0 & 1 & \dots & 0 & \dots & 0 & b_{21} & b_{22} & \dots & b_{1q} & \dots & b_{2m} \\ \dots & & & & & & & & & & & \\ 0 & 0 & \dots & 1 & \dots & 0 & b_{p1} & b_{p2} & \dots & b_{pq} & \dots & b_{pm} \\ \dots & & & & & & & & & & & \\ 0 & 0 & \dots & 0 & \dots & 1 & b_{k1} & b_{k2} & \dots & b_{kq} & \dots & b_{km} \end{array}\right],$$

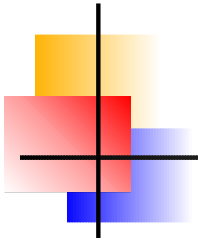
$$\mathbf{H} = \begin{bmatrix} \mathbf{h}_1^T \\ \mathbf{h}_2^T \\ \dots \\ \mathbf{h}_q^T \\ \dots \\ \mathbf{h}_m^T \end{bmatrix} = \left[\begin{array}{cccccc|cccccc} -b_{11} & -b_{21} & \dots & -b_{p1} & \dots & -b_{k1} & 1 & 0 & \dots & 0 & \dots & 0 \\ -b_{12} & -b_{22} & \dots & -b_{p2} & \dots & -b_{k2} & 0 & 1 & \dots & 0 & \dots & 0 \\ \dots & & & & & & & & & & & \\ -b_{1q} & -b_{2q} & \dots & -b_{pq} & \dots & -b_{kq} & 0 & 0 & \dots & 1 & \dots & 0 \\ \dots & & & & & & & & & & & \\ -b_{1m} & -b_{2m} & \dots & -b_{pm} & \dots & -b_{km} & 0 & 0 & \dots & 0 & \dots & 1 \end{array}\right].$$

Pre $\mathbf{b}_p$, $\mathbf{h}_q$ platí

$$\begin{array}{rcl} \mathbf{b}_p^T & = & [\ 0 \quad 0 \quad \dots \quad 1 \quad \dots \quad 0 \quad b_{p1} \quad b_{p2} \quad \dots \quad b_{pq} \quad \dots \quad b_{pm}\ ] \\ \mathbf{h}_q^T & = & [\ -b_{1q} \quad -b_{2q} \quad \dots \quad -b_{pq} \quad \dots \quad -b_{kq} \quad 0 \quad 0 \quad \dots \quad 1 \quad \dots \quad 0\ ] \end{array}$$

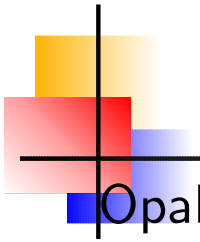
a preto je $\mathbf{b}_p^T.\mathbf{h}_q = (-b_{pq} + b_{pq}) = 0$ pre každé $p,\ q \in \{1, 2, \dots, n\}$, z čoho

$$\mathbf{G}.\mathbf{H}^T = \mathbf{O}_{k \times (n-k)}.$$



Lineárne kódy

Keďže matica $\mathbf{H}$ s $m = n - k$ riadkami obsahuje jednotkovú podmaticu $\mathbf{E}_{(n-k)\times(n-k)}$, je $\dim(H) = n - k$.
Preto je $\mathbf{H}$ kontrolnou maticou kódu $\mathcal{K}$.



Lineárne kódy a objavovanie chýb

Opakovanie:
Kód $\mathcal{K}$ objavuje t-násobné jednoduché chyby, ak pri zmene ľubovoľných t znakov ľubovoľného kódového slova $\mathbf{u}$ vznikne nekódové slovo.

Mechanizmus vzniku niekoľkonásobnej chyby modelujeme v teórii lineárnych kódov tak, ako keby sa k vyslanému slovu

$$\mathbf{v} = v_1 v_2 \dots v_n$$

behom prenosu pripočítalo slovo

$$\mathbf{e} = e_1 e_2 \dots e_n.$$

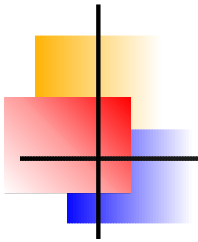
Potom namiesto slova $\mathbf{v}$ prijmeme slovo

$$\mathbf{w} = w_1 w_2 \dots w_n,$$

pre ktoré platí

$$\mathbf{w} = \mathbf{v} + \mathbf{e}.$$

Slovo $\mathbf{e}$ nazývame **chybové slovo**.



Lineárne kódy a objavovanie chýb

Definícia

Hovoríme, že lineárny kód $\mathcal{K}$ **objavuje chybové slovo e**, *ak pre každé kódové slovo* **v** *je slovo* $\mathbf{v} + \mathbf{e}$ *nekódovým slovom.*

Definícia

Hammingova váha $\|\mathbf{a}\|$ slova $\mathbf{a} \in A^n$ *je počet nenulových znakov slova* **a**.

Veta

Každý binárny lineárny kód obsahuje buď len slová párnej váhy, alebo má rovnaký počet slov párnej a nepárnej váhy.

Dôkaz.
Ak existuje kódové slovo $\mathbf{v}$ nepárnej váhy, fixujme ho a definujme zobrazenie $f : \mathcal{K} \to \mathcal{K}$ predpisom

$$f(\mathbf{w}) = \mathbf{w} + \mathbf{v} \ .$$

Je ihneď vidieť, že f je vzájomne jednoznačné zobrazenie $\mathcal{K}$ na $\mathcal{K}$ priraďujúce každému slovu párnej váhy slovo nepárnej váhy a naopak. Z toho už vyplýva, že počet slov párnej váhy sa rovná počtu slov nepárnej váhy. □

Opakovanie.
Minimálna vzdialenosť $\Delta(\mathcal{K})$ blokového kódu $\mathcal{K}$ bola definovaná ako minimum z Hammingových vzdialeností všetkých dvojíc nerovnakých slov kódu $\mathcal{K}$.
Ak totiž $d = \Delta(\mathcal{K})$, kód $\mathcal{K}$ objavuje všetky $(d-1)$-násobné chyby a opravuje všetky t-násobné chyby pre $t < \frac{d}{2}$.

Veta

Pre lineárny kód $\mathcal{K}$ sa minimálna vzdialenosť kódu $\Delta(\mathcal{K})$ rovná minimu z Hammingových váh všetkých nenulových slov kódu $\mathcal{K}$, t. j.

$$\Delta(\mathcal{K}) = \min_{\mathbf{u}\in\mathcal{K},\mathbf{u}\neq\mathbf{o}}\{\|\mathbf{u}\|\} .$$

Dôkaz.
1. Majme $\mathbf{u},\ \mathbf{v} \in \mathcal{K}$ také, že $d(\mathbf{u},\mathbf{v}) = \Delta(\mathcal{K})$.
Nech $\mathbf{w} = \mathbf{u} - \mathbf{v}$.
Slovo $\mathbf{w}$ má práve toľko nenulových znakov, v koľkých znakoch sa líšia slová $\mathbf{u},\ \mathbf{v}$, preto je

$$\min_{\mathbf{u}\in\mathcal{K},\mathbf{u}\neq\mathbf{o}}\{\|\mathbf{u}\|\} \leq \|\mathbf{w}\| = d(\mathbf{u},\mathbf{v}) = \Delta(\mathcal{K}) . \tag{9}$$

2. Vezmime $\mathbf{w} \in \mathcal{K}$ také, že $\|w\| = \min_{\mathbf{u}\in\mathcal{K},\mathbf{u}\neq\mathbf{o}}\{\|\mathbf{u}\|\}$. Potom

$$\Delta(\mathcal{K}) \leq d(\mathbf{o},\mathbf{v}) = \|\mathbf{w}\| \leq \min_{\mathbf{u}\in\mathcal{K},\mathbf{u}\neq\mathbf{o}}\{\|\mathbf{u}\|\} . \tag{10}$$

Vzťahy (9) a (10) už dávajú tvrdenie vety. □

Veta

Nech $\mathcal{K}$ je lineárny kód s kontrolnou maticou $\mathbf{H}$. Nech d je minimum z počtu lineárne závislých stĺpcov[a] kontrolnej matice $\mathbf{H}$.
Potom pre minimálnu vzdialenosť $\Delta(\mathcal{K})$ kódu $\mathcal{K}$ platí

$$d = \Delta(\mathcal{K}) \ .$$

[a] V kontrolnej matici $\mathbf{H}$ existuje d lineárne závislých stĺpcov, ale každých $d-1$ stĺpcov kontrolnej matice je už lineárne nezávislých.

Dôkaz. Podľa predchádzajúcej vety sa $\Delta(\mathcal{K})$ rovná minimálnej váhe nenulového kódového slova.

Nech d je minimum počtu lineárne závislých stĺpcov kontrolnej matice $\mathbf{H}$.

Označme $\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_n$ stĺpce kontrolnej matice $\mathbf{H}$, t. j.

$$\mathbf{H} = \left[\begin{array}{cccc} \mathbf{c}_1 & \mathbf{c}_2 & \ldots & \mathbf{c}_n \end{array} \right].$$

Nech $\mathbf{u} \in \mathcal{K}$ je nenulové slovo s najmenšou Hammingovou váhou

$$\|\mathbf{u}\| = t = \Delta(\mathcal{K}).$$

Slovo $\mathbf{u}$ má na miestach $i_1, i_2, \ldots, i_t$ znaky $u_{i_1}, u_{i_2}, \ldots, u_{i_t}$ a na ostatných miestach znak 0, t. j.

$$\mathbf{u}^T = \left[\, 0 \;\; 0 \;\; \ldots \;\; 0 \;\; u_{i_1} \;\; 0 \;\; \ldots \;\; 0 \;\; u_{i_2} \;\; 0 \;\; \ldots \;\; \ldots \;\; 0 \;\; u_{i_t} \;\; 0 \;\; \ldots \;\; 0 \;\; 0 \,\right].$$

Pretože $\mathbf{u}$ je kódové slovo, je $\mathbf{Hu} = \mathbf{o}$, t. j.

$$\mathbf{Hu} = \sum_{i=1}^{n} u_i.\mathbf{c}_i = u_{i_1}\mathbf{c}_{i_1} + u_{i_2}\mathbf{c}_{i_2} + \cdots + u_{i_t}\mathbf{u}_{i_t} = \mathbf{o}\ . \qquad (11)$$

Pretože všetky koeficienty u_{i_j} sú nenulové, sú stĺpce $\mathbf{c}_{i_1}, \mathbf{c}_{i_2}, \ldots, \mathbf{c}_{i_t}$ lineárne závislé, a preto

$$d \leq t = \Delta(\mathcal{K})\ . \qquad (12)$$

Majme d lineárne závislých stĺpcov $\mathbf{c}_{i_1}, \mathbf{c}_{i_2}, \ldots, \mathbf{c}_{i_d}$. Potom existujú čísla $u_{i_1}, u_{i_2}, \ldots, u_{i_d}$ také, že aspoň jedno z nich je nenulové a

$$u_{i_1}\mathbf{c}_{i_1} + u_{i_2}\mathbf{c}_{i_2} + \cdots + u_{i_d}\mathbf{c}_{i_d} = \mathbf{o} \ .$$

Definujme slovo $\mathbf{u}$ také, že na miestach $i_1, i_2, \ldots, i_d$ bude mať znaky $u_{i_1}, u_{i_2}, \ldots, u_{i_d}$ a na ostatných miestach znak 0, t. j.

$$\mathbf{u}^T = \left[\, 0 \;\; 0 \;\; \ldots \;\; 0 \;\; u_{i_1} \;\; 0 \;\; \ldots \;\; 0 \;\; u_{i_2} \;\; 0 \;\; \ldots \;\; \ldots \;\; 0 \;\; u_{i_t} \;\; 0 \;\; \ldots \;\; 0 \;\; 0 \,\right].$$

Potom

$$\mathbf{Hu} = \sum_{i=1}^{n} u_i.\mathbf{c}_i = u_{i_1}\mathbf{c}_{i_1} + u_{i_2}\mathbf{c}_{i_2} + \cdots + u_{i_t}\mathbf{c}_{i_d} = \mathbf{o} \ , \qquad (13)$$

a teda $\mathbf{u}$ je nenulovým kódovým slovom, pre ktorého Hammingovu váhu platí $\|\mathbf{u}\| \leq d$ a teda

$$\Delta(\mathcal{K}) \leq d \ .$$

Posledná nerovnosť spolu s (12) už dáva požadované tvrdenie vety. □

Veta

Lineárny kód objavuje t-násobné chyby práve vtedy, keď každých t stĺpcov kontrolnej matice je lineárne nezávislých.

Dôkaz.
Označme $d = \Delta(\mathcal{K})$.
Podľa predchádzajúcej vety existuje v kontrolnej matici $\mathbf{H}$ kódu $\mathcal{K}$ d lineárne závislých stĺpcov, a pre každé $t < d$ je ľubovoľných t stĺpcov matice $\mathbf{H}$ lineárne nezávislých.

1.
Ak kód $\mathcal{K}$ objavuje t-násobné chyby, potom musí byť $t < d$, a podľa vety 9 je každých t stĺpcov matice $\mathbf{H}$ lineárne nezávislých.

2.
Ak je každých t stĺpcov matice $\mathbf{H}$ lineárne nezávislých, potom je $t < d$, a preto kód $\mathcal{K}$ objavuje t chýb. □

Definícia

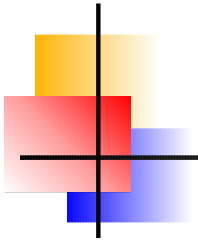
Nech $\mathbf{H}$ *je kontrolná matica lineárneho kódu* $\mathcal{K}$,
nech $\mathbf{v} = v_1 v_2 \dots v_n \in A^n$ *je ľubovoľné slovo abecedy* A *dĺžky* n.
Syndróm slova $\mathbf{v}$ *je slovo* $\mathbf{s} = s_1 s_2 \dots s_n$, *pre ktoré platí*

$$\mathbf{H}.\begin{bmatrix} v_1 \\ v_2 \\ \dots \\ v_n \end{bmatrix} = \begin{bmatrix} s_1 \\ s_2 \\ \dots \\ s_n \end{bmatrix}, \qquad \textit{skrátene} \quad \mathbf{H}.\mathbf{v} = \mathbf{s}\ .$$

Ak teda prijmeme slovo $\mathbf{w}$, vypočítame jeho syndróm $\mathbf{s} = \mathbf{Hw}$, a ak $\mathbf{s} \neq \mathbf{o}$, vieme, že došlo k chybe.
Vyslané slovo $\mathbf{v}$, prijaté slovo $\mathbf{w} = \mathbf{v} + \mathbf{e}$.

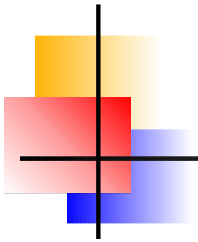
$$\mathbf{Hw} = \mathbf{H}(\mathbf{v} + \mathbf{e}) = \mathbf{Hv} + \mathbf{He} = \mathbf{o} + \mathbf{He} = \mathbf{He}\ .$$

Syndróm prijatého slova $\mathbf{w} = \mathbf{v} + \mathbf{e}$ je rovnaký, ako syndróm chybového slova $\mathbf{e}$.



Lineárne kódy a objavovanie chýb

Kód $\mathcal{K}$ je podpriestor práve všetkých riešení rovnice $\mathbf{H} = \mathbf{o}$.
Rovnica $\mathbf{He} = \mathbf{s}$ má množinu všetkých riešení v tvare $\mathbf{e} + \mathbf{k}$, kde $\mathbf{k} \in \mathcal{K}$.
Túto množinu budeme v ďalšom označovať ako $\mathbf{e} + \mathcal{K}$.



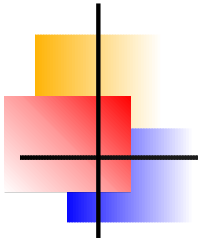
Štandardné dekódovanie

Opakovanie.
Dekódovanie je funkcia δ, ktorá ma za definičný obor A^n alebo jeho časť obsahujúcu kód $\mathcal{K}$, a ktorá každému slovu zo svojho definičného oboru priraďuje kódové slovo, pričom je δ na $\mathcal{K}$ identitou – kódovému slovu $\mathbf{a} \in \mathcal{K}$ priraďuje $\delta(\mathbf{a}) = \mathbf{a}$.

Definícia

Hovoríme, že **lineárny kód** $\mathcal{K}$ **pri dekódovaní** δ **opravuje chybové slovo e**, *ak pre všetky* $\mathbf{v} \in \mathcal{K}$ *platí:*

$$\delta(\mathbf{e} + \mathbf{v}) = \mathbf{v} \ .$$



Štandardné dekódovanie

Definícia

Nech $\mathcal{K} \subseteq A^n$ je lineárny kód s kódovou abecedou A. Pre každé slovo $\mathbf{e} \in A^n$ definujeme

$$\mathbf{e} + \mathcal{K} = \{\mathbf{e} + \mathbf{v} \mid \mathbf{v} \in \mathcal{K}\} \ .$$

Množina $\mathbf{e} + \mathcal{K}$ sa volá **trieda slova e podľa kódu** $\mathcal{K}$.

Štandardné dekódovanie

Veta

Nech $\mathcal{K} \subseteq A^n$ je lineárny (n, k)-kód s kódovou abecedou A, $|A| = p$. Pre ľubovoľné slová $\mathbf{e}, \mathbf{e}' \in A^n$ platí

(i) *Ak $\mathbf{e} - \mathbf{e}'$ je kódové slovo, potom $\mathbf{e} + \mathcal{K} = \mathbf{e}' + \mathcal{K}$.*

(ii) *Ak $\mathbf{e} - \mathbf{e}'$ nie je kódové slovo, potom $\mathbf{e} + \mathcal{K}$, $\mathbf{e}' + \mathcal{K}$ sú disjunktné.*

(iii) *Počet slov každej triedy sa rovná počtu kódových slov, t. j. $|\mathbf{e} + \mathcal{K}| = |\mathcal{K}| = p^k$ a počet všetkých tried je p^{n-k}.*

Dôkaz.
(i) Nech $(\mathbf{e} - \mathbf{e}') \in \mathcal{K}$, nech $\mathbf{a} \in \mathbf{e} + \mathcal{K}$.
Potom $\mathbf{a} = \mathbf{e} + \mathbf{v}$ pre nejaké $\mathbf{v} \in \mathcal{K}$.
$\mathbf{a} = \mathbf{e} + \mathbf{v} - (\mathbf{e} - \mathbf{e}') = \mathbf{e}' + \mathbf{v}$
$\mathbf{v} \in \mathcal{K}$, a teda $(\mathbf{e} + \mathbf{v}) \in (\mathbf{e} + \mathcal{K})$. Položme $\mathbf{u} = \mathbf{v} + (\mathbf{e} - \mathbf{e}')$. Pretože $\mathcal{K}$ je lineárny priestor a $(\mathbf{e} - \mathbf{e}') \in \mathcal{K}$, je aj $\mathbf{u} \in \mathcal{K}$, a teda $(\mathbf{e}' + \mathbf{u}) \in (\mathbf{e}' + \mathcal{K})$.
Ale $\mathbf{e}' + \mathbf{u} = \mathbf{e}' + \mathbf{v} + (\mathbf{e} - \mathbf{e}') = \mathbf{e} + \mathbf{v}$. Preto je $(\mathbf{e} + \mathbf{v}) \in (\mathbf{e}' + \mathcal{K})$.
Ukázali sme, že $(\mathbf{e} + \mathcal{K}) \subseteq (\mathbf{e}' + \mathcal{K})$. Analogicky sa ukáže aj opačná inklúzia, a teda $(\mathbf{e} + \mathcal{K}) = (\mathbf{e}' + \mathcal{K})$.

Štandardné dekódovanie

Ak prijmeme nekódové slovo, chceme mu priradiť kódové slovo, ktorého pokazením toto slovo pravdepodobne vzniklo (zase za predpokladov, že počet chýb neprekročil hodnotu t).

Na to slúži dekódovanie δ definované ako funkcia, ktorá ma za definičný obor A^n alebo jeho časť obsahujúcu kód $\mathcal{K}$, a ktorá každému slovu zo svojho definičného oboru priraďuje kódové slovo, pričom je δ na $\mathcal{K}$ identitou – kódovému slovu $\mathbf{a} \in \mathcal{K}$ priraďuje $\delta(\mathbf{a}) = \mathbf{a}$.

Ak bolo vyslané slovo $\mathbf{v}$ a došlo k chybe vyjadrenej slovom $\mathbf{e}$, prijmeme slovo $\mathbf{e} + \mathbf{v}$. Ak $\delta(\mathbf{e} + \mathbf{v}) = \mathbf{v}$, dekódovali sme správne.

Definícia

Hovoríme, že **lineárny kód $\mathcal{K}$ pri dekódovaní δ opravuje chybové slovo $\mathbf{e}$**, *ak pre všetky* $\mathbf{v} \in \mathcal{K}$ *platí:*

$$\delta(\mathbf{e} + \mathbf{v}) = \mathbf{v} \ .$$

Štandardné dekódovanie

Ak prijmeme nekódové slovo, chceme mu priradiť kódové slovo, ktorého pokazením toto slovo pravdepodobne vzniklo (zase za predpokladov, že počet chýb neprekročil hodnotu t).

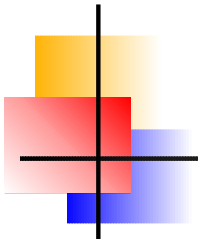
Na to slúži dekódovanie δ definované ako funkcia, ktorá ma za definičný obor A^n alebo jeho časť obsahujúcu kód $\mathcal{K}$, a ktorá každému slovu zo svojho definičného oboru priraďuje kódové slovo, pričom je δ na $\mathcal{K}$ identitou – kódovému slovu $\mathbf{a} \in \mathcal{K}$ priraďuje $\delta(\mathbf{a}) = \mathbf{a}$.

Ak bolo vyslané slovo $\mathbf{v}$ a došlo k chybe vyjadrenej slovom $\mathbf{e}$, prijmeme slovo $\mathbf{e} + \mathbf{v}$. Ak $\delta(\mathbf{e} + \mathbf{v}) = \mathbf{v}$, dekódovali sme správne.

Definícia

Hovoríme, že **lineárny kód** $\mathcal{K}$ **pri dekódovaní** δ **opravuje chybové slovo** $\mathbf{e}$, *ak pre všetky* $\mathbf{v} \in \mathcal{K}$ *platí:*

$$\delta(\mathbf{e} + \mathbf{v}) = \mathbf{v} \ .$$



Štandardné dekódovanie

Definícia

Štandardné dekódovanie.
Definujeme úplné dekódovanie $\delta : A^n \to \mathcal{K}$ *nasledovne:*

Z každej triedy podľa $\mathcal{K}$ *vyberieme jedného reprezentanta triedy tak, aby jeho váha bola v danej triede minimálna.*
(Výber reprezentanta podľa kritéria minimálnej váhy nemusí byť jednoznačný – v tom prípade sa musíme rozhodnúť pre jedného s minimálnou váhou).

Potom každé prijaté slovo $\mathbf{w} \in A^n$ *dekódujeme ako* $\mathbf{v} = \mathbf{w} - \mathbf{e}$, *kde chybové slovo* $\mathbf{e}$ *je reprezentantom triedy slova* $\mathbf{w}$, *teda*

$$\delta(\mathbf{w}) = \mathbf{w} - [\textit{reprezentant triedy } (\mathbf{w} + \mathcal{K})].$$

Štandardné dekódovanie

Príklad

Binárny $(4,3)$*-kód* $\mathcal{K}$ *celkovej parity má dve triedy*

$$\begin{aligned} 0000+\mathcal{K} &= \{0000 \quad 0011 \quad 0101 \quad 0110 \quad 1001 \quad 1010 \quad 1100 \quad 1111\} \\ 0001+\mathcal{K} &= \{0001 \quad 0010 \quad 0100 \quad 0111 \quad 1000 \quad 1011 \quad 1101 \quad 1110\} \end{aligned}$$

Trieda $0000+\mathcal{K}$ *má jednoznačného reprezentanta – slovo* 0000*.*

Trieda $0001+\mathcal{K}$ *môže mať za reprezentanta ľubovoľné zo slov* $0001,\ 0010,\ 0100,\ 1000$*.*
Podľa toho, ktoré z týchto slov vyberieme za reprezentantov, štandardné dekódovanie opraví jednu chybu, ktorá vznikne na prvom, resp. druhom, treťom alebo štvrtom mieste.

Ak vznikne chyba na inom mieste, štandardné dekódovanie nedekóduje správne.
(Pre nás to nie je prekvapujúce zistenie, lebo vieme, že kód celkovej parity má minimálnu vzdialenosť 2, a preto nemôže opravovať ani všetky jednoduché chyby.)

Štandardné dekódovanie

Veta

Štandardné dekódovanie δ opravuje práve tie chybové slová, ktoré sú reprezentantmi tried, t. j.

$$\delta(\mathbf{v}+\mathbf{e}) = \mathbf{v} \quad \textit{pre všetky } \mathbf{v} \in \mathcal{K}$$

práve vtedy, keď $\mathbf{e}$ *je reprezentantom niektorej triedy podľa kódu* $\mathcal{K}$.

Dôkaz.
Ak je $\mathbf{e}$ reprezentantom svojej triedy a $\mathbf{v} \in \mathcal{K}$, potom slovo $\mathbf{v}+\mathbf{e}$ padne do triedy $\mathbf{e}+\mathcal{K}$ a dekóduje sa ako $\delta(\mathbf{e}+\mathbf{v}) = \mathbf{e}+\mathbf{v}-\mathbf{e} = \mathbf{v}$ – podľa definície 10 dekódovanie δ opravuje chybové slovo $\mathbf{e}$.

Nech $\mathbf{e}'$ nie je reprezentantom svojej triedy, ktorá má za reprezentanta slovo $\mathbf{e} \neq \mathbf{e}'$. Platí $(\mathbf{e}-\mathbf{e}') \in \mathcal{K}$.
Nech $\mathbf{v} \in \mathcal{K}$, potom slovo $\mathbf{v}+\mathbf{e}'$ padne do triedy $\mathbf{e}+\mathcal{K}$ a dekóduje sa ako $\delta(\mathbf{v}+\mathbf{e}') = \mathbf{v}+\mathbf{e}'-\mathbf{e} \neq \mathbf{v}$.
Ak $\mathbf{e}'$ nie je reprezentantom svojej triedy, štandardné dekódovanie neopravuje slovo $\mathbf{e}'$. □

Štandardné dekódovanie

Veta

Štandardné dekódovanie δ je optimálne v tom zmysle, že neexistuje dekódovanie δ^*, ktoré by opravovalo tie isté chybové slová ako δ a navyše ešte niektoré ďalšie.

Dôkaz.
Vezmime $\mathbf{e}' \in (\mathbf{e} + \mathcal{K})$, nech $\mathbf{e}$ je reprezentantom triedy $\mathbf{e} + \mathcal{K}$, nech $\mathbf{e} \neq \mathbf{e}'$. Slovo $\mathbf{v} = \mathbf{e}' - \mathbf{e}$ je kódové a nenulové.
Ak vyšleme slovo $\mathbf{v}$ a vznikne chyba pôsobením chybového slova $\mathbf{e}$, prijmeme slovo $\mathbf{v} + \mathbf{e} = \mathbf{e}' - \mathbf{e} + \mathbf{e} = \mathbf{e}'$.

Keďže δ opravuje všetky slová, ktoré sú reprezentantami tried je $\delta(\mathbf{v} + \mathbf{e}) = \delta(\mathbf{e}') = \mathbf{v}$.

Keďže δ^* opravuje všetky slová, ktoré opravuje δ, je aj $\delta^*(\mathbf{e}') = \mathbf{v}$.

Môže dekódovanie δ^* opravovať slovo $\mathbf{e}'$? Keby áno, potom by muselo byť $\delta^*(\mathbf{o} + \mathbf{e}') = \mathbf{o}$, čo je v spore s tým, že $\delta^*(\mathbf{e}') = \mathbf{v} \neq \mathbf{o}$. □

Štandardné dekódovanie

Veta

Ak je $d = \Delta(\mathcal{K})$ minimálna vzdialenosť lineárneho kód $\mathcal{K}$, potom štandardné dekódovanie opraví všetky t-násobné chyby pre $t < \frac{d}{2}$.

Dôkaz.

Nech $\mathbf{e}$ je slovo váhy $t < \frac{d}{2}$. Hammi Nech $\mathbf{v} \in (\mathbf{e} + \mathcal{K})$, $\mathbf{v} \neq \mathbf{e}$, $\mathbf{v} = \mathbf{e} + \mathbf{u}$, $\mathbf{u} \in \mathcal{K}$.

Je $\|\mathbf{u}\| \geq d$, $\|\mathbf{e}\| = t < \frac{d}{2}$.

Preto počet nenulových znakov slova $\mathbf{v} = \mathbf{e} + \mathbf{u}$ je aspoň $d - t$ – t. j. $\|\mathbf{v}\| > d - t > t$.

Preto je každé slovo $\mathbf{e}$ s Hammingovou váhou menšou než $\frac{d}{2}$ reprezentantom niektorej triedy slov podľa kódu $\mathcal{K}$.

Keďže štandardné dekódovanie opravuje všetky chybové slová, ktoré sú reprezentantami tried, opravuje všetky chybové slová s Hammingovou váhou menšou než $\frac{d}{2}$, čo je ekvivalentné s tým, že štandardné dekódovanie opraví všetky t-násobné chyby. □

Štandardné dekódovanie

Princípom štandardného dekódovania je určenie, v ktorej triede slov podľa kódu $\mathcal{K}$ sa dekódované slovo vyskytuje.
Na to by príslušný dekódovací algoritmus musel prezrieť tzv. Slepianovu tabuľku všetkých slov dĺžky n abecedy A.

	Trieda $\mathbf{e}_1 + \mathcal{K}$	Trieda $\mathbf{e}_2 + \mathcal{K}$		Trieda $\mathbf{e}_m + \mathcal{K}$
reprezentant	$\mathbf{e_1} = \mathbf{e_1} + \mathbf{o}$	$\mathbf{e_2} = \mathbf{e_2} + \mathbf{o}$	$\ldots$	$\mathbf{e_m} = \mathbf{e_m} + \mathbf{o}$
prvky tried	$\mathbf{e_1} + \mathbf{u_1}$	$\mathbf{e_2} + \mathbf{u_1}$	$\ldots$	$\mathbf{e_m} + \mathbf{u_1}$
	$\mathbf{e_1} + \mathbf{u_2}$	$\mathbf{e_2} + \mathbf{u_2}$	$\ldots$	$\mathbf{e_m} + \mathbf{u_2}$
	$\ldots$	$\ldots$	$\ldots$	$\ldots$
	$\ldots$	$\ldots$	$\ldots$	$\ldots$
	$\ldots$	$\ldots$	$\ldots$	$\ldots$
	$\mathbf{e_1} + \mathbf{u_q}$	$\mathbf{e_2} + \mathbf{u_q}$	$\ldots$	$\mathbf{e_m} + \mathbf{u_q}$

(14)

Slepianova tabuľka, $m = p^{n-k}$, $q = |\mathcal{K}| = p^k$.

Slepianova tabuľka má p^n prvkov, ktoré v najhoršom prípade musíme prehľadať všetky. Pre bežne používané binárne kódy dĺžky 64 by to znamenalo v najhoršom prípade $2^{64} > 10^{19}$ prehľadaní.

Štandardné dekódovanie

Problém možno značne zredukovať, ak si uvedomíme, že všetky prvky triedy $\mathbf{e} + \mathcal{K}$ majú rovnaký syndróm ako jej reprezentant $\mathbf{e}$.
Je to preto, lebo pre $\mathbf{v} \in \mathcal{K}$ a kontrolnú maticu $\mathbf{H}$ kódu $\mathcal{K}$ platí:

$$\mathbf{H}.(\mathbf{e} + \mathbf{v}) = \mathbf{H}.\mathbf{e} + \mathbf{H}.\mathbf{v} = \mathbf{H}.\mathbf{e} + \mathbf{o} = \mathbf{H}.\mathbf{e} \ .$$

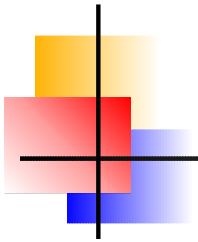
Preto namiesto Slepianovej tabuľky stačí tabuľka s dvoma riadkami, kde v prvom riadku sú reprezentanti tried $\mathbf{e_1}, \mathbf{e_2}, \ldots, \mathbf{e_m}$, $m = p^{n-k}$
a v druhom riadku sú príslušné syndrómy $\mathbf{s_1}, \mathbf{s_2}, \ldots, \mathbf{s_m}$.

reprezentant	$\mathbf{e}_1$	$\mathbf{e}_2$	$\ldots$	$\mathbf{e}_m$
syndróm	$\mathbf{s}_1$	$\mathbf{s}_2$	$\ldots$	$\mathbf{s}_m$

(15)

Teraz možno štandardný dekódovací algoritmus preformulovať nasledovne:
Pre prijaté slovo $\mathbf{w}$ vypočítame jeho syndróm $\mathbf{s} = \mathbf{H}.\mathbf{w}$. V tabuľke (15) nájdeme reprezentanta $\mathbf{e}$ triedy s rovnakým syndrómom $\mathbf{s}$ a dekódujeme

$$\delta(\mathbf{w}) = \mathbf{w} - \mathbf{e} \ .$$



Hammingove kódy

Veta

p-znakový lineárny kód opravuje jednoduché chyby práve vtedy, keď žiaden stĺpec jeho kontrolnej matice nie je skalárnym násobkom iného stĺpca.
Špeciálne binárny lineárny kód opravuje jednoduché chyby práve vtedy, keď stĺpce jeho kontrolnej matice sú nenulové a navzájom rôzne.

Dôkaz.
Vieme, že kód $\mathcal{K}$ opravuje jednoduché chyby práve vtedy, keď $\Delta(\mathcal{K}) \geq 3$, čo nastáva práve vtedy, keď ľubovoľné dva stĺpce kontrolnej matice $\mathbf{H}$ sú lineárne nezávislé.

Vo všeobecnom prípade sú dva vektory $\mathbf{u}$, $\mathbf{v}$ lineárne nezávislé práve vtedy, keď jeden nie je skalárnym násobkom druhého, čo v prípade binárnej abecedy je práve vtedy, keď sú oba vektory $\mathbf{u}$, $\mathbf{v}$ nenulové a rôzne. □

Hammingove kódy

Definícia

Binárny lineárny (n, k)-kód sa nazýva **Hammingov kód**, *ak jeho kontrolná matica* **H** *má za stĺpce všetky nenulové binárne slová dĺžky $n - k$, pričom každé z nich sa ako stĺpec matice* **H** *vyskytuje práve raz.*

Ak sa majú v matici **H** všetky nenulové binárne slová dĺžky $n - k$ vyskytovať práve raz, musí sa počet stĺpcov v tejto matici rovnať

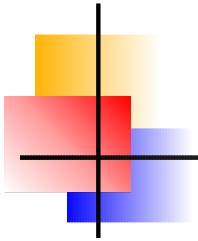
$$n = 2^{(n-k)} - 1.$$

Preto môže existovať len Hammingov (n, k)-kód pre

$$(n, k) = (3, 1),\ (7, 4),\ (15, 11),\ (31, 26), \ldots (2^m - 1, 2^m - m - 1), \ldots\ .$$

Všimnime si ešte, že informačný pomer $R = \frac{k}{n}$ s rastúcim m rýchlo rastie k 1.

Napr. $m = 6$ Hammingov $(63, 57)$-kód má informačný pomer $\frac{57}{63} > 0.9$.



Hammingove kódy

Dekódovanie Hammingovho kódu.

Predpokladajme, že stĺpce kontrolnej matice $\mathbf{H}$ sú usporiadané tak, že tvoria binárne rozvoje čísel $1, 2, \ldots, 2^{m-1}$.

Prijmeme vektor $\mathbf{w}$ a vypočítame jeho syndróm $\mathbf{s} = \mathbf{Hw}$.

Ak $\mathbf{s} = \mathbf{o}$, slovo $\mathbf{w}$ nemeníme.

Ak $\mathbf{s} \neq \mathbf{o}$, slovo $\mathbf{s}$ je binárnym rozvojom čísla i, zmeníme i-ty znak prijatého slova $\mathbf{w}$. Presnejšie

$$\delta(\mathbf{w}) = \begin{cases} \mathbf{w}, & \text{ak } \mathbf{s} = \mathbf{o} \\ \mathbf{w} - \mathbf{e_i}, & \text{ak } \mathbf{s} \text{ je binárnym rozvojom čísla } i, \end{cases} \tag{16}$$

kde $\mathbf{e}_i$ je slovo s jednotkou na mieste i.

Veta

Dekódovanie δ definované v (21) opravuje jednoduché chyby. Presnejšie: Ak sa slovo $\mathbf{w}$ líši od niektorého kódového slova $\mathbf{v}$ nanajvýš v jednom znaku, potom $\delta(\mathbf{w}) = \mathbf{v}$.

Dôkaz.
Ak $\mathbf{w} = \mathbf{v}$, potom aj $\mathbf{w}$ je kódové slovo a platí $\mathbf{Hw} = \mathbf{Hv} = \mathbf{o}$, a v tom prípade $\delta(\mathbf{w}) = \mathbf{w} = \mathbf{v}$.
Nech sa slová $\mathbf{v}$, $\mathbf{w}$ líšia práve v jednom znaku, t. j. $\mathbf{w} = \mathbf{v} + \mathbf{e_i}$, kde $\mathbf{e}_i$ je slovo s jednotkou na mieste i, $i \in \{1, 2, \ldots, n\}$. Potom

$$\mathbf{Hw} = \mathbf{H}(\mathbf{v} + \mathbf{e_i}) = \mathbf{Hv} + \mathbf{He_i} = \mathbf{He_i} \ .$$

Ale $\mathbf{He_i}$ je i-ty stĺpec matice $\mathbf{H}$ a ten je rozvojom čísla i.
Ak budeme dekódovať predpisom

$$\delta(\mathbf{w}) = \mathbf{w} - \mathbf{e_i} = \mathbf{v},$$

budeme dekódovať správne. □

Hammingove kódy

Podľa definície blokový kód $\mathcal{K}$ dĺžky n je t-perfektný, ak množina gúľ $\{G_t(\mathbf{a}) \mid \mathbf{a} \in \mathcal{K}\}$ tvorí rozklad množiny A^n všetkých slov dĺžky n.

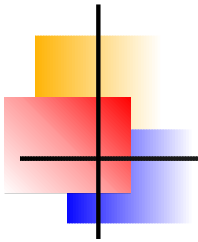
Veta

Lineárny kód je t-perfektný práve vtedy, keď množina všetkých slov váhy menšej než alebo rovnajúcej sa číslu t tvorí systém všetkých reprezentantov všetkých tried slov podľa kódu $\mathcal{K}$.

Dôkaz.
Platí: Ľubovoľné slovo $\mathbf{a} \in A^n$ môže byť reprezentantom niektorej triedy kódu $\mathcal{K}$ – totiž triedy $\mathbf{a} + \mathcal{K}$.

1.
Nech $\mathcal{K}$ je t-perfektný kód.
Na to, aby sme dokázali, že množina všetkých slov váhy menšej než alebo rovnajúcej sa číslu t tvorí systém všetkých reprezentantov všetkých tried slov podľa kódu $\mathcal{K}$ stačí ukázať dve skutočnosti, a to že

- každá trieda má reprezentanta s váhou menšou než alebo rovnajúcou sa číslu t
- ak $\mathbf{e_1}$, $\mathbf{e_2}$ sú dve slová také, že $\|\mathbf{e}_1\| \leq t$, $\|\mathbf{e}_2\| \leq t$, potom $\mathbf{e}_1 + \mathcal{K}$, $\mathbf{e}_1 + \mathcal{K}$ sú dve rôzne triedy, t. j. $\mathbf{e}_2 \notin (\mathbf{e}_1 + \mathcal{K})$



Hammingove kódy

Pretože $\mathcal{K}$ je t-perfektný lineárny kód – t. j. pre každé slovo $\mathbf{a} \in A^n$ existuje práve jedno kódové slovo $\mathbf{b} \in \mathcal{K}$ také, že $d(\mathbf{a},\ \mathbf{b}) \leq t$.

Označme $\mathbf{e} = \mathbf{a} - \mathbf{b}$.

Pretože $d(\mathbf{a},\ \mathbf{b}) \leq t$, je $\|\mathbf{e}\| \leq t$. Potom je $\mathbf{a} = \mathbf{e} + \mathbf{b}$.

Trieda $\mathbf{a} + \mathcal{K}$ má reprezentanta $\mathbf{e}$ s váhou menšou alebo rovnajúcou sa t.

Keby existovali dve slová $\mathbf{e}_1,\ \mathbf{e}_2$ také, že $\|\mathbf{e}_1\| \leq t$, $\|\mathbf{e}_2\| \leq t$ a $\mathbf{e}_2 \in (\mathbf{e}_1 + \mathcal{K})$, potom $\mathbf{e_2} - \mathbf{e_1} \in \mathcal{K}$ a $\|\mathbf{e_2} - \mathbf{e_1}\| \leq 2t$.

Z poslednej nerovnosti vyplýva pre minimálnu vzdialenosť $\Delta(\mathcal{K})$ kódu $\mathcal{K}$: $\Delta(\mathcal{K}) \leq 2t$, čo je v spore s predpokladom, že $\mathcal{K}$ opravuje t chýb.

(Vieme totiž, že kód $\mathcal{K}$ opravuje t chýb práve vtedy, keď $\Delta(\mathcal{K}) \geq 2t + 1$.)

2.

Nech množina všetkých slov váhy menšej alebo rovnej než t tvorí systém všetkých reprezentantov všetkých tried slov podľa kódu $\mathcal{K}$.

Najprv ukážeme, že $\Delta(\mathcal{K}) \geq 2t+1$.
Keby totiž existovalo $\mathbf{a} \in \mathcal{K}$ také, že $\|\mathbf{a}\| \leq 2t+1$, bolo by možné vyjadriť $\mathbf{a} = \mathbf{e_1} - \mathbf{e_2}$, kde $\|\mathbf{e}_1\| \leq t$, $\|\mathbf{e}_2\| \leq t$ a $\mathbf{e_1} \neq \mathbf{e_2}$.
Podľa (i) vety o triedach typu $(\mathbf{e}+\mathcal{K})$ by potom $(\mathbf{e}_1+\mathcal{K}) = (\mathbf{e}_2+\mathcal{K})$, čo by bolo v spore s predpokladom, že $\mathbf{e_1}$, $\mathbf{e_2}$ sú reprezentantmi rôznych tried.

Ak je teda $\Delta(\mathcal{K}) \geq 2t+1$, všetky gule $\{G_t(\mathbf{a}) \mid \mathbf{a} \in \mathcal{K}\}$ sú po dvoch disjunktné.

Teraz ukážeme, že pre každé $\mathbf{a} \in A^n$ existuje guľa $G_t(\mathbf{b})$, $\mathbf{b} \in \mathcal{K}$ taká, že $\mathbf{a} \in G_t(\mathbf{b})$.
Podľa predpokladu existuje $\mathbf{e} \in A^n$, $\|\mathbf{e}\| \leq t$ také, že $\mathbf{a} \in (\mathbf{e}+\mathcal{K})$.
Dá sa teda písať $\mathbf{a} = \mathbf{e}+\mathbf{b}$ pre nejaké $\mathbf{b} \in \mathcal{K}$.
Odtiaľ $\mathbf{a}-\mathbf{b} = \mathbf{e}$, a preto $d(\mathbf{a},\mathbf{b}) = \|(\mathbf{a}-\mathbf{b})\| = \|\mathbf{e}\| \leq t$ a teda $\mathbf{a} \in G_t(\mathbf{b})$.

Systém gúľ $\{G_t(\mathbf{a}) \mid \mathbf{a} \in \mathcal{K}\}$ tvorí rozklad množiny A^n, a preto je kód $\mathcal{K}$ t-perfektný. □

Hammingove kódy

Veta

Hammingové binárne kódy sú 1-perfektné. Každý 1-perfektný binárny lineárny kód je Hammingov.

Dôkaz.
Hammingov kód dĺžky $2^m - 1$ má m kontrolných znakov a podľa tvrdenia (iii) vety o triedach typu $(\mathbf{e} + \mathcal{K})$ má 2^m tried.
Označme $\mathbf{e}_0 = \mathbf{o}$ – nulové slovo dĺžky $2^m - 1$.
Ďalej označme pre $i = 1, 2, \ldots, 2^m - 1$

$$\mathbf{e}_i = \left[\begin{array}{ccccccc} 0 & 0 & \ldots & 0 & 1 & 0 \ldots & 0 \end{array} \right],$$

Všetky $\mathbf{e}_i$ pre $i = 1, 2, \ldots, 2^m - 1$ sú nekódové slová.
Trieda $\mathbf{e}_0 + \mathcal{K}$ je totožná s množinou kódových slov $\mathcal{K}$, a je preto rôzna od ostatných tried.
Keby boli dve triedy $\mathbf{e}_i + \mathcal{K}$, $\mathbf{e}_j + \mathcal{K}$ totožné pre $i \neq j$, potom by $\mathbf{e_i} - \mathbf{e_j} \in \mathcal{K}$, čo by znamenalo lineárnu závislosť i-teho a j-teho stĺpca kontrolnej matice kódu $\mathcal{K}$, (čo je v prípade binárneho kódu rovnosť príslušných stĺpcov).
Hammingov kód má však kontrolnú maticu, v ktorej žiadne dva stĺpce nie sú rovnaké.

Hammingove kódy

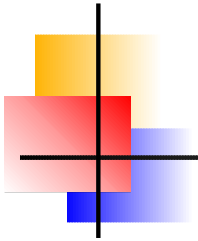
Pretože Hammingov kód $\mathcal{K}$ má 2^m tried a my sme ukázali, že všetky triedy typu $\mathbf{e}_i + \mathcal{K}$ pre $i = 0, 1, 2, \ldots, 2^m - 1$ sú rôzne (a je ich 2^m), nemôže existovať žiadna ďalšia trieda.
Množina všetkých slov dĺžky ≤ 1 tvorí systém reprezentantov všetkých tried Hammingovho kódu $\mathcal{K}$, a preto je tento kód 1-perfektný.

Majme binárny lineárny kód $\mathcal{K}$ s m kontrolnými znakmi, ktorý je 1 perfektný. Podľa tvrdenia podľa tvrdenia (iii) vety o triedach typu $(\mathbf{e} + \mathcal{K})$ kód $\mathcal{K}$ má 2^m tried.
Nech má tento kód kontrolnú maticu $\mathbf{H}$ typu $n \times m$. Podľa vety 15 musia byť všetky stĺpce matice $\mathbf{H}$ nenulové a rôzne.
Preto pre počet stĺpcov matice $\mathbf{H}$ platí $n \leq 2^m - 1$.
Pretože je kód $\mathcal{K}$ perfektný, podľa vety o t-perfektných kódoch sú všetky binárne slová dĺžky n s váhou nula alebo jedna práve všetci reprezentanti tried. Takýchto slov je $n + 1$ (nulové slovo a všetky slová typu $\mathbf{e}_i$ s práve jednou jednotkou na i-tom mieste). Je preto

$$n + 1 = 2^m,$$

čiže

$$n = 2^m - 1.$$



Hammingove kódy

Kontrolná matica kódu $\mathcal{K}$ je matica typu $(2^m - 1) \times m$ a jej stĺpce sú práve všetky rôzne binárne nenulové slová dĺžky m. $\mathcal{K}$ je teda Hammingovým kódom. □

Hammingove kódy

Definícia

Rozšírený Hammingov binárny kód *je binárny kód, ktorý vznikne rozšírením Hammingovho kódu o znak celkovej kontroly parity.*

Rozšírený Hammingov kód je $(2^m, 2^m - m - 1)$-kód všetkých slov $\mathbf{v} = v_1 v_2 \dots v_{2^m}$ takých, že $v_1 v_2 \dots v_{2^m-1}$ je kódové slovo Hammingovho kódu a $v_1 + v_2 + \dots + v_{2^m} = 0$.
Jeho minimálna váha je 4. Tento kód opravuje jednoduché chyby a objavuje trojnásobné chyby.

Poznámka

Návod, ako definovať p-znakový Hammingov kód. Je to kód s kontrolnou maticou $\mathbf{H}$ *takou, že*

(i) žiaden stĺpec nie je skalárnym násobkom iného stĺpca

(ii) každé nenulové slovo je skalárnym násobkom niektorého stĺpca matice $\mathbf{H}$.

Maticu $\mathbf{H}$ *môžeme zostaviť napríklad zo všetkých stĺpcov rovnakej dĺžky takých, ktoré majú prvý nenulový znak* 1. *Dá sa ukázať, že p-znakové Hammingové kódy majú mnohé vlastnosti rovnaké resp. analogické ako binárne Hammingové kódy. Tak napríklad všetky Hammingové kódy sú* 1*-perfektné.*

Golayov kód

Označme $\mathbf{B}$ štvorcovú maticu typu 11×11, ktorej prvý riadok obsahuje binárne slovo 11011100010 a ostatné riadky vzniknú pravými rotáciami prvého riadku, t. j.

$$\mathbf{B} = \begin{bmatrix} 1 & 1 & & 1 & 1 & 1 & & & & 1 & & \\ & 1 & 1 & & 1 & 1 & 1 & & & & 1 & \\ 1 & & 1 & 1 & & 1 & 1 & 1 & & & & \\ & 1 & & 1 & 1 & & 1 & 1 & 1 & & & \\ & & 1 & & 1 & 1 & & 1 & 1 & 1 & & \\ & & & 1 & & 1 & 1 & & 1 & 1 & 1 & \\ 1 & & & & 1 & & 1 & 1 & & 1 & 1 & \\ 1 & 1 & & & & 1 & & 1 & 1 & & 1 & \\ 1 & 1 & 1 & & & & 1 & & 1 & 1 & & \\ & 1 & 1 & 1 & & & & 1 & & 1 & 1 & \\ 1 & & 1 & 1 & 1 & & & & 1 & & 1 & \end{bmatrix}. \qquad (17)$$

Binárne slovo 11011100010 má na mieste i jednotku práve vtedy, keď je $i-1$ štvorcom modulo 11, t. j. ak $i-1 = 0^2, 1^2, 2^2, 3^2, 4^2 \equiv 5$ a $5^2 \equiv 3$. Ďalej budeme predpokladať, že matica $\mathbf{B}$ je daná vzťahom (17).

Golayov kód

Definícia

Golayov kód G_{23} *je systematický binárny kód dĺžky* 23 *s generujúcou maticou* $\mathbf{G}_{23}$ *definovanou*

$$\mathbf{G}_{23} = \left[\begin{array}{c|c} \mathbf{E}_{12\times 12} & \begin{array}{c} \mathbf{B}_{11\times 11} \\ \hline 11\ldots 11 \end{array} \end{array}\right],$$

kde $\mathbf{E}_{12\times 12}$ *je jednotková matica typu* 12×12, $\mathbf{B}_{11\times 11}$ *je štvorcová matica typu* 11×11 *definovaná v* (17).

Golayov kód G_{24} *je systematický binárny kód dĺžky* 24 *s generujúcou maticou* $\mathbf{G}_{24}$, *ktorá vznikne z matice* $\mathbf{G}_{23}$ *pridaním stĺpca* $11\ldots 10$, *t. j.*

$$\mathbf{G}_{24} = \left[\begin{array}{c|c|c} \mathbf{E}_{12\times 12} & \begin{array}{c} \mathbf{B}_{11\times 11} \\ \hline 11\ldots 11 \end{array} & \begin{array}{c} 1 \\ 1 \\ \ldots \\ 1 \\ \hline 0 \end{array} \end{array}\right]$$

Golayov kód

$$\left[\begin{array}{cccccccccccccccccccccccc}
1 & & & & & & & & & & & 1 & 1 & & 1 & 1 & 1 & & & & 1 & & 1 \\
 & 1 & & & & & & & & & & & 1 & 1 & & 1 & 1 & 1 & & & & 1 & 1 \\
 & & 1 & & & & & & & & & 1 & & 1 & 1 & & 1 & 1 & 1 & & & & 1 \\
 & & & 1 & & & & & & & & & 1 & & 1 & 1 & & 1 & 1 & 1 & & & 1 \\
 & & & & 1 & & & & & & & & & 1 & & 1 & 1 & & 1 & 1 & 1 & & 1 \\
 & & & & & 1 & & & & & & & & & 1 & & 1 & 1 & & 1 & 1 & 1 & 1 \\
 & & & & & & 1 & & & & & & & & & 1 & & 1 & 1 & & 1 & 1 & 1 & 1 \\
 & & & & & & & 1 & & & & 1 & & & & 1 & & 1 & 1 & & 1 & 1 & 1 & 1 \\
 & & & & & & & & 1 & & & 1 & 1 & & & & 1 & & 1 & 1 & & 1 & 1 & 1 \\
 & & & & & & & & & 1 & & 1 & 1 & 1 & & & & 1 & & 1 & 1 & & 1 & 1 \\
 & & & & & & & & & & 1 & & 1 & 1 & 1 & & & & 1 & & 1 & 1 & 1 & 1 \\
 & & & & & & & & & & & 1 & & 1 & 1 & 1 & & & & 1 & & 1 & 1 & 1 \\
 & & & & & & & & & & & & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 &
\end{array}\right]$$

Generujúca matica Golayovho kódu $\mathbf{G}_{24}$.

Golayov kód

Vlastnosti kódov G_{24}, G_{23}.

- Počet informačných znakov kódu G_{24} je 12, počet kontrolných znakov je tiež 12.
- Kód G_{24} je samoduálny – jeho kontrolná matica je aj jeho generujúcou maticou (na to stačí overiť, že skalárny súčin ľubovoľných dvoch riadkov matice $\mathbf{G}_{24}$ sa rovná 0).
- Minimálna vzdialenosť kódu G_{24} je 8
- Kód G_{23} je $(23, 12)$-kód, ktorý je 3-perfektný.

Veta

Tietäväinen, Van Lint. *Jediné netriviálne perfektné binárne kódy sú tieto:*

a) *Hammingove kódy pre jednoduché chyby,*

b) *Golayov kód G_{23} pre trojnásobné chyby a kódy s ním ekvivalentné,*

c) *opakovacie kódy dĺžky $2t + 1$ pre t-násobné chyby, kde $t = 1, 2, 3, \ldots$.*

Golayov kód

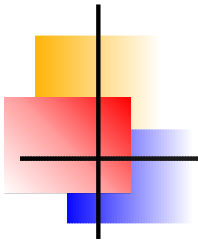
K zaujímavým ternárnym kódom patrí perfektný Golayov ternárny $(11, 6)$-kód opravujúci trojnásobné chyby.
Jeho generujúca matica je v tvare

$$\mathbf{G}_{11} = \left[\begin{array}{c|c} \mathbf{E}_{6\times 6} & \begin{array}{c} \mathbf{D}_{5\times 5} \\ \hline 11\ldots 11 \end{array} \end{array}\right],$$

kde $\mathbf{E}_{6\times 6}$ je jednotková matica typu 6×6 a kde $\mathbf{D}_{5\times 5}$ je matica, ktorej riadky tvoria všetky cyklické pravé rotácie slova 01221.

Okrem tohoto kódu (a kódov s ním ekvivalentných) sú jediné perfektné ternárne netriviálne kódy Hammingove a opakovacie kódy dĺžky $2t + 1$.

V prípade abecedy s viac ako troma znakmi sú jediné perfektné netriviálne kódy Hammingove a opakovacie kódy dĺžky $2t + 1$.



Lineárne kódy – definíca – zhrnutie

Budeme študovať n-znakový kód $\mathcal{K}$ v kódovej abeced A, t.j. $\mathcal{K} \subseteq A^n$. Jedinou možnosťou, ako detekovať alebo opravovať chyby je používať takú množiny kódových slov – kód $\mathcal{K}$, ktorá nevyužíva celé A^n,

Kódová abeceda A s operáciami $+$ a . musí byť pole (resp. teleso). Jediné konečné polia sú polia typu $\mathbb{Z}_p$, kde p je prvočíslo a Galoisove polie typu $GF(p^n)$, kde p je prvočíslo.

Množinu A^n berieme lineárny priestor, jej prvky ako n-rozmerné vektory s oepráciou sčítania po zložkách a opráciou násobenia prvkom z A tiež pozložkách.

Definícia

Kód $\mathcal{K}$ sa nazýva **lineárny** (n, k)**-kód**, *ak je podpriestorom dimenzie k lineárneho priestoru A^n, t. j. ak* $\dim(\mathcal{K}) = k$, *a pre ľubovoľné* $\mathbf{a}, \mathbf{b} \in \mathcal{K}$ *a ľubovoľné $c \in A$ je*

$$\mathbf{a} + \mathbf{b} \in \mathcal{K}, \qquad c.\mathbf{a} \in \mathcal{K}.$$

Lineárne kódy – zhrnutie

Lineárny (n, k)-kód ako k-dimenzionálny podpriestor priestoru A^n musí mať k-prvkovú bázu

$$\mathbf{B} = \{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k\}.$$

Potom každé kódové slovo $\mathbf{a} \in A^n$ má jednoznačné vyjadrenie

$$\mathbf{a} = u_1\mathbf{b}_1 + u_2\mathbf{b}_2 + \cdots + u_k\mathbf{b}_k = \Phi(u_1, u_2, \ldots, u_n), \qquad (18)$$

kde $u_1, u_2, \ldots, u_n$ sú súradnice vektora $\mathbf{a}$ v báze $\mathbf{B}$.

Ak $|A| = p$, potom na mieste každého u_i môže stáť p rôznych čísel, z čoho vyplýva, že existuje p^k rôznych k-tic $u_1, u_2, \ldots, u_k$, dosadením ktorých do (1) dostaneme p^k rôznych kódových slov kódu $\mathcal{K}$. Lineárny (n, k)-kód má teda p^k slov.

Ak $|A| = p^n$, potom počet slov lineárneho (n, k)-kódu je $(p^n)^k = p^{nk}$.

Zobrazenie (18) $\Phi(u_1, u_2, \ldots, u_k)$ je vzájomne jednoznačné zobrazenie A^k na $\mathcal{K}$, takže podľa definície má lineárny (n, k) kód $\mathcal{K}$ k informačných a $n - k$ kontrolných znakov.[1]

[1] Hovoríme, že kód $\mathcal{K}$ má k informačných a $n - k$ kontrolných znakov, ak existuje vzájomne jednoznačné zobrazenie A^k na $\mathcal{K}$.

Generujúca matica lin. kódu – zhrnutie

Nech $\mathcal{K}$ je lineárny (n, k)-kód, nech $\mathbf{B} = \{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k\}$ je ľubovoľná báza kódu $\mathcal{K}$. Nech $\mathbf{b}_i = (b_{i1}\ b_{i2} \ldots b_{in})^T$ pre $i = 1, 2, \ldots, k$. Potom matica

$$\mathbf{G} = \begin{bmatrix} \mathbf{b}_1^T \\ \mathbf{b}_2^T \\ \ldots \\ \mathbf{b}_k^T \end{bmatrix} = \begin{bmatrix} b_{11} & b_{12} & \ldots & b_{1n} \\ b_{21} & b_{22} & \ldots & b_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ b_{k1} & b_{k2} & \ldots & b_{kn} \end{bmatrix} \tag{19}$$

typu $(k \times n)$ sa nazýva **generujúca matica kódu** $\mathcal{K}$**.**
Nech má lineárny (n, k)-kód pre bázu $\mathbf{B} = \{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k\}$ generujúcu maticu (19). Ak má slovo $\mathbf{a} = a_1 a_2 \ldots a_n$ súradnice $u_1, u_2, \ldots, u_k$ v báze $\mathbf{B}$, potom

$$\mathbf{a}^T = u_1\mathbf{b}_1^T + u_2\mathbf{b}_2^T + \cdots + u_k\mathbf{b}_k^T = \begin{bmatrix} u_1 & u_2 & \ldots & u_k \end{bmatrix} . \begin{bmatrix} \mathbf{b}_1^T \\ \mathbf{b}_2^T \\ \ldots \\ \mathbf{b}_k^T \end{bmatrix},$$

alebo po rozpísaní vektorov $\mathbf{b}_i^T$ podrobnejšie

$$\begin{bmatrix} a_1 & a_2 & \ldots & a_n \end{bmatrix} = \begin{bmatrix} u_1 & u_2 & \ldots & u_k \end{bmatrix} . \begin{bmatrix} b_{11} & b_{12} & \ldots & b_{1n} \\ b_{21} & b_{22} & \ldots & b_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ b_{k1} & b_{k2} & \ldots & b_{kn} \end{bmatrix},$$

alebo krátko

$$\mathbf{a}^T = \mathbf{u}^T . \mathbf{G} .$$

Systematické lineárne kódy – zhrnutie

Lineárny (n, k)-kód $\mathcal{K}$ je systematický práve vtedy, keď jeho ľubovoľná generujúca matica $\mathbf{G}$ má prvé k stĺpce lineárne nezávislé.[2]

Každý lineárny (n, k)-kód $\mathcal{K}$ je ekvivalentný so systematickým lineárnym kódom.[3]
Lineárny (n, k)-kód $\mathcal{K}$ je systematický práve vtedy, keď k nemu existuje generujúca matica $\mathbf{G}$ typu:

$$\mathbf{G} = \left[\begin{array}{c|c} \mathbf{E} & \mathbf{B} \end{array} \right] = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 & b_{11} & b_{12} & \dots & h_{1n-k} \\ 0 & 1 & 0 & \dots & 0 & b_{21} & b_{22} & \dots & b_{2n-k} \\ & & & & & \dots & & & \\ 0 & 0 & 0 & \dots & 1 & b_{k1} & h_{k2} & \dots & h_{kn-k} \end{bmatrix} .$$

[2] Podľa definície je blokový kód $\mathcal{K}$ s k informačnými a $n-k$ kontrolnými znakmi systematický, ak ku každému $a_1 a_2 \dots a_k \in A^k$ existuje práve jedno kódové slovo $\mathbf{a} \in \mathcal{K}$ s prefixom $a_1 a_2 \dots a_k \in A^k$.

[3] Hovoríme, že dva blokové kódy $\mathcal{K}$, $\mathcal{K}'$ dĺžky n sú **ekvivalentné**, ak existuje permutácia π množiny $\{1, 2, \dots, n\}$ taká, že platí
$\forall a_1 a_2 \dots a_n \in A^n \quad a_1 a_2 \dots a_n \in \mathcal{K}$ práve vtedy, keď $a_{\pi[1]} a_{\pi[2]} \dots a_{\pi[n]} \in \mathcal{K}'$.

Kontrolná matica lineárneho kódu – zhrnutie

Kontrolná matica lineárneho kódu $\mathcal{K}$ je taká matica $\mathbf{H}$ prvkov kódovej abecedy A, pre ktorú platí: Slovo $\mathbf{v} = v_1 v_2 \dots v_n$ je kódové práve vtedy, keď

$$\mathbf{H}.\mathbf{v} = \begin{bmatrix} h_{11} & h_{12} & \dots & h_{1n} \\ h_{21} & h_{22} & \dots & h_{2n} \\ \dots & \dots & \dots & \dots \\ h_{m1} & h_{m2} & \dots & h_{mn} \end{bmatrix} . \begin{bmatrix} v_1 \\ v_2 \\ \dots \\ v_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \dots \\ 0 \end{bmatrix} = \mathbf{o} \ .$$

Stručnejšie: $\mathbf{v} \in \mathcal{K}$ práve vtedy, keď $\mathbf{H}.\mathbf{v} = \mathbf{o}$.
Generujúca matica lineárneho (n, k) kódu má dimenziu k, n stĺpcov a k riadkov, príslušná kontrolná matica lineárneho (n, k) kódu má dimenziu $m = n - k$, n stĺpcov a $m = n - k$ riadkov.

Nech $\mathcal{K}$ je lineárny (n, k)-kód s generujúcou maticou $\mathbf{G}$ typu $(k \times n)$. Potom matica $\mathbf{H}$ typu $((n - k) \times n)$ je kontrolnou maticou kódu $\mathcal{K}$ práve vtedy, keď

$$\dim(\mathbf{H}) = (n - k) \quad \text{a} \quad \mathbf{G}.\mathbf{H}^T = \mathbf{O}_{k \times (n-k)},$$

kde $\mathbf{O}_{k \times (n-k)}$ je nulová matica typu $(k \times (n - k))$.

Lineárny (n, k)-kód $\mathcal{K}$ s generujúcou maticou $\mathbf{G} = \left[\ \mathbf{E}_{k \times k} \ \middle| \ \mathbf{B} \ \right]$ má kontrolnú maticu $\mathbf{H} = \left[\ -\mathbf{B}^T \ \middle| \ \mathbf{E}_{(n-k) \times (n-k)} \ \right]$.

Minimálna vzdialenosť $\Delta\mathcal{K}$ lineárneho kódu – zhrnutie

Najdôležitejšie fakty o min. vzdialenosti lineárneho kódu.

1. Pre lineárny kód $\mathcal{K}$ sa minimálna vzdialenosť kódu $\Delta(\mathcal{K})$ rovná minimu z Hammingových váh všetkých nenulových slov kódu $\mathcal{K}$, t. j.

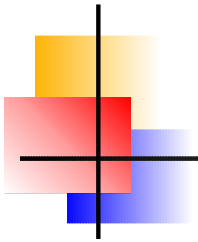
$$\Delta(\mathcal{K}) = \min_{\mathbf{u}\in\mathcal{K},\mathbf{u}\neq\mathbf{o}} \{\|\mathbf{u}\|\} \ .$$

2. Nech $\mathcal{K}$ je lineárny kód s kontrolnou maticou $\mathbf{H}$. Nech d je minimum z počtu lineárne závislých stĺpcov[4] kontrolnej matice $\mathbf{H}$. Potom pre minimálnu vzdialenosť $\Delta(\mathcal{K})$ kódu $\mathcal{K}$ platí

$$d = \Delta(\mathcal{K}) \ .$$

3. Lineárny kód objavuje t-násobné chyby práve vtedy, keď každých t stĺpcov kontrolnej matice je lineárne nezávislých.

[4] V kontrolnej matici $\mathbf{H}$ existuje d lineárne závislých stĺpcov, ale každých $d-1$ stĺpcov kontrolnej matice je už lineárne nezávislých.



Modelovanie vzniku chyby pri line. kódoch – zhrnutie

Mechanizmus vzniku niekoľkonásobnej chyby modelujeme v teórii lineárnych kódov tak, ako keby sa k vyslanému slovu

$$\mathbf{v} = v_1 v_2 \dots v_n$$

behom prenosu pripočítalo slovo

$$\mathbf{e} = e_1 e_2 \dots e_n.$$

Potom namiesto slova $\mathbf{v}$ prijmeme slovo

$$\mathbf{w} = w_1 w_2 \dots w_n,$$

pre ktoré platí

$$\mathbf{w} = \mathbf{v} + \mathbf{e}.$$

Slovo $\mathbf{e}$ nazývame **chybové slovo**.

Syndróm slova – zhrnutie

Definícia

Nech $\mathbf{H}$ *je kontrolná matica lineárneho kódu* $\mathcal{K}$,
nech $\mathbf{v} = v_1 v_2 \dots v_n \in A^n$ *je ľubovoľné slovo abecedy* A *dĺžky* n.
Syndróm slova $\mathbf{v}$ *je slovo* $\mathbf{s} = s_1 s_2 \dots s_n$, *pre ktoré platí*

$$\mathbf{H}.\begin{bmatrix} v_1 \\ v_2 \\ \dots \\ v_n \end{bmatrix} = \begin{bmatrix} s_1 \\ s_2 \\ \dots \\ s_n \end{bmatrix}, \qquad \textit{skrátene} \quad \mathbf{H}.\mathbf{v} = \mathbf{s}\ .$$

Ak teda prijmeme slovo $\mathbf{w}$, vypočítame jeho syndróm $\mathbf{s} = \mathbf{Hw}$, a ak $\mathbf{s} \neq \mathbf{o}$, vieme, že došlo k chybe.
Vyslané slovo $\mathbf{v}$, prijaté slovo $\mathbf{w} = \mathbf{v} + \mathbf{e}$.

$$\mathbf{Hw} = \mathbf{H}(\mathbf{v} + \mathbf{e}) = \mathbf{Hv} + \mathbf{He} = \mathbf{o} + \mathbf{He} = \mathbf{He}\ .$$

Syndróm prijatého slova $\mathbf{w} = \mathbf{v} + \mathbf{e}$ je rovnaký, ako syndróm chybového slova $\mathbf{e}$.

Štandardné dekódovanie – zhrnutie

Nech $\mathcal{K} \subseteq A^n$ je lineárny kód s kódovou abecedou A. Pre každé slovo $\mathbf{e} \in A^n$ definujeme

$$\mathbf{e} + \mathcal{K} = \{\mathbf{e} + \mathbf{v} \mid \mathbf{v} \in \mathcal{K}\} \ .$$

Množina $\mathbf{e} + \mathcal{K}$ sa volá **trieda slova e podľa kódu** $\mathcal{K}$.

Pre dve triedy $\mathbf{e} + \mathcal{K}$ $\mathbf{e}' + \mathcal{K}$ platí:
Ak $\mathbf{e} - \mathbf{e}' \in \mathcal{K}$, potom $\mathbf{e} + \mathcal{K} = \mathbf{e}' + \mathcal{K}$.
Ak $\mathbf{e} - \mathbf{e}' \notin \mathcal{K}$, potom sú triedy $\mathbf{e} + \mathcal{K}$, $\mathbf{e}' + \mathcal{K}$ disjunktné.
Všetky slová triedy $\mathbf{e} + \mathcal{K}$ majú rovnaký syndróm.

Hovoríme, že **lineárny kód** $\mathcal{K}$ **pri dekódovaní**[5] δ **opravuje chybové slovo e**, ak pre všetky $\mathbf{v} \in \mathcal{K}$ platí:

$$\delta(\mathbf{e} + \mathbf{v}) = \mathbf{v} \ .$$

[5] Dekódovanie je funkcia δ, ktorá ma za definičný obor A^n alebo jeho časť obsahujúcu kód $\mathcal{K}$, a ktorá každému slovu zo svojho definičného oboru priraďuje kódové slovo, pričom je δ na $\mathcal{K}$ identitou – kódovému slovu $\mathbf{a} \in \mathcal{K}$ priraďuje $\delta(\mathbf{a}) = \mathbf{a}$.

Štandardné dekódovanie – zhrnutie

Definujeme úplné dekódovanie $\delta : A^n \to \mathcal{K}$ nasledovne:
Z každej triedy podľa $\mathcal{K}$ vyberieme jedného reprezentanta triedy tak, aby jeho váha bola v danej triede minimálna.[6]
Potom každé prijaté slovo $\mathbf{w} \in A^n$ dekódujeme ako $\mathbf{v} = \mathbf{w} - \mathbf{e}$, kde chybové slovo $\mathbf{e}$ je reprezentantom triedy slova $\mathbf{w}$, teda

$$\delta(\mathbf{w}) = \mathbf{w} - [\text{reprezentant triedy } (\mathbf{w} + \mathcal{K})].$$

Štandardné dekódovanie δ opravuje práve tie chybové slová, ktoré sú reprezentantmi tried, t. j.

$$\delta(\mathbf{v} + \mathbf{e}) = \mathbf{v} \quad \text{pre všetky } \mathbf{v} \in \mathcal{K}$$

práve vtedy, keď $\mathbf{e}$ je reprezentantom niektorej triedy podľa kódu $\mathcal{K}$.

Štandardné dekódovanie δ je optimálne v tom zmysle, že neexistuje dekódovanie δ^*, ktoré by opravovalo tie isté chybové slová ako δ a navyše ešte niektoré ďalšie.

---

[6] Výber reprezentanta podľa kritéria minimálnej váhy nemusí byť jednoznačný – v tom prípade sa musíme rozhodnúť pre jedného s minimálnou váhou).

Tabuľka syndrómov tried – zhrnutie

Na dekódovanie stačí tabuľka s dvoma riadkami, kde v prvom riadku sú reprezentanti tried $\mathbf{e_1}, \mathbf{e_2}, \ldots, \mathbf{e_m}$, $m = p^{n-k}$ a v druhom riadku sú príslušné syndrómy $\mathbf{s_1}, \mathbf{s_2}, \ldots, \mathbf{s_m}$.

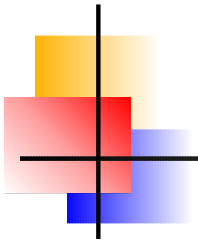
reprezentant	$\mathbf{e}_1$	$\mathbf{e}_2$	$\ldots$	$\mathbf{e}_m$
syndróm	$\mathbf{s}_1$	$\mathbf{s}_2$	$\ldots$	$\mathbf{s}_m$

(20)

Teraz možno štandardný dekódovací algoritmus preformulovať nasledovne:
Pre prijaté slovo $\mathbf{w}$ vypočítame jeho syndróm $\mathbf{s} = \mathbf{H}.\mathbf{w}$. V tabuľke (20) nájdeme reprezentanta $\mathbf{e}$ triedy s rovnakým syndrómom $\mathbf{s}$ a dekódujeme

$$\delta(\mathbf{w}) = \mathbf{w} - \mathbf{e} \ .$$

Dôležité.
Ak je $d = \Delta(\mathcal{K})$ minimálna vzdialenosť lineárneho kód $\mathcal{K}$, potom štandardné dekódovanie opraví všetky t-násobné chyby pre $t < \frac{d}{2}$.



Hammingove kódy – zhrnutie

p-znakový lineárny kód opravuje jednoduché chyby práve vtedy, keď žiaden stĺpec jeho kontrolnej matice nie je skalárnym násobkom iného stĺpca.
Špeciálne binárny lineárny kód opravuje jednoduché chyby práve vtedy, keď stĺpce jeho kontrolnej matice sú nenulové a navzájom rôzne.

Binárny lineárny (n, k)-kód sa nazýva **Hammingov kód**, ak jeho kontrolná matica **H** má za stĺpce všetky nenulové binárne slová dĺžky $n - k$, pričom každé z nich sa ako stĺpec matice **H** vyskytuje práve raz[7].

[7] Ak sa majú v matici **H** všetky nenulové binárne slová dĺžky $n - k$ vyskytovať práve raz, musí sa počet stĺpcov v tejto matici rovnať $n = 2^{(n-k)} - 1$. Preto môže existovať len Hammingov (n, k)-kód pre $(n, k) = (3, 1),\ (7, 4),\ (15, 11),\ (31, 26), \ldots (2^m - 1, 2^m - m - 1), \ldots .$
Všimnime si ešte, že informačný pomer $R = \frac{k}{n}$ s rastúcim m rýchlo rastie k 1. Napr. $m = 6$ Hammingov $(63, 57)$-kód má informačný pomer $\frac{57}{63} > 0.9$.

Dekódovanie Hammingovho kódu.

Nech že stĺpce kontrolnej matice $\mathbf{H}$ sú usporiadané tak, že tvoria binárne rozvoje čísel $1, 2, \ldots, 2^{m-1}$.

Prijmeme vektor $\mathbf{w}$ a vypočítame jeho syndróm $\mathbf{s} = \mathbf{Hw}$.

Ak $\mathbf{s} = \mathbf{o}$, slovo $\mathbf{w}$ nemeníme.

Ak $\mathbf{s} \neq \mathbf{o}$, slovo $\mathbf{s}$ je binárnym rozvojom čísla i, zmeníme i-ty znak prijatého slova $\mathbf{w}$. Presnejšie

$$\delta(\mathbf{w}) = \begin{cases} \mathbf{w}, & \text{ak } \mathbf{s} = \mathbf{o} \\ \mathbf{w} - \mathbf{e_i}, & \text{ak } \mathbf{s} \text{ je binárnym rozvojom čísla } i, \end{cases} \tag{21}$$

kde $\mathbf{e}_i$ je slovo s jednotkou na mieste i.
Dekódovanie δ definované v (21) opravuje jednoduché chyby. Presnejšie: Ak sa slovo $\mathbf{w}$ líši od niektorého kódového slova $\mathbf{v}$ nanajvýš v jednom znaku, potom $\delta(\mathbf{w}) = \mathbf{v}$.

Hammingov binárny kód (15,11) - zhrnutie

$$\begin{array}{c} \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & A & B & C & D & E & F \end{matrix} \\ \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \end{array} . \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

Súčin $\mathbf{H}.\mathbf{v} = [0,1,1,1]^T$. Číslo $(0111)_2$ v dvojkovej sústave predstavuje číslo $2+4+8=14$. Za predpokladu, že sa vyskytla len jedna chyba, táto nastala na štrnástom bite slova $\mathbf{v}$.

Generujúca matica Hammingov binárny kódu (15,11)

Toto je jedna z možných generujúcich matíc Hammingovho $(15, 11)$ kódu

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \tag{22}$$

Všimnime si, že Hammingov kód nie je systematický, to by muselo byť všetkých prvých jedenásť stĺpcov matice $\mathbf{G}$ lineárne nezávislých.
Jedenásty stĺpec je však závislý na prvých desiatich.
Desiatku prvých lineárne nezávyslých stĺpcov doplňuje na plný počet 11 až dvanásty stĺpec.

Generujúca matica Hammingovho binárny kódu (15,11)

Aby sme overili,či matica $\mathbf{G}$ z rovnice (22) je skutočne generujúcou maticou Hammingovho $(15, 11)$ kodu s kontrolnou maticou $\mathbf{H}$, treba overiť, či skutočne platí $\mathbf{G}.\mathbf{H}^T = \mathbf{0}$.

Skutočne:

$$\mathbf{G}.\mathbf{H}^T = \begin{bmatrix} 1&0&0&0&0&0&0&0&0&0&0&0&1&1&1 \\ 0&1&0&0&0&0&0&0&0&0&0&1&0&1 \\ 0&0&1&0&0&0&0&0&0&0&0&1&1&0 \\ 0&0&0&1&0&0&0&0&0&0&1&0&0&0&1 \\ 0&0&0&0&1&0&0&0&0&0&1&0&0&1&0 \\ 0&0&0&0&0&1&0&0&0&0&1&0&1&0&0 \\ 0&0&0&0&0&0&1&0&0&0&1&0&1&1&1 \\ 0&0&0&0&0&0&0&1&0&0&1&0&1&1&0 \\ 0&0&0&0&0&0&0&0&1&0&1&0&1&0&1 \\ 0&0&0&0&0&0&0&0&0&1&1&0&0&1&1 \\ 0&0&0&0&0&0&0&0&0&0&0&1&1&1&1 \end{bmatrix}_{(11\times 15)} . \begin{bmatrix} 1&0&0&0 \\ 0&1&0&0 \\ 1&1&0&0 \\ 0&0&1&0 \\ 1&0&1&0 \\ 0&1&1&0 \\ 1&1&1&0 \\ 0&0&0&1 \\ 1&0&0&1 \\ 0&1&0&1 \\ 1&1&0&1 \\ 0&0&1&1 \\ 1&0&1&1 \\ 0&1&1&1 \\ 1&1&1&1 \end{bmatrix}_{(15\times 4)} = \begin{bmatrix} 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \end{bmatrix}_{(11\times 4)} = \mathbf{0}$$

Rozšírený Hammingov kód

je binárny kód, ktorý vznikne rozšírením Hammingovho kódu o znak celkovej kontroly parity. Rozšírený Hammingov kód je $(2^m, 2^m - m - 1)$-kód všetkých slov $\mathbf{v} = v_1 v_2 \dots v_{2^m}$ takých, že $v_1 v_2 \dots v_{2^m-1}$ je kódové slovo Hammingovho kódu a $v_1 + v_2 + \cdots + v_{2^m} = 0$. Jeho minimálna váha je 4. Tento kód opravuje jednoduché chyby a objavuje trojnásobné chyby.

$$\mathbf{G}.\mathbf{H}^T = \begin{bmatrix} 1&0&0&0&0&0&0&0&0&0&0&1&1&1 \\ 0&1&0&0&0&0&0&0&0&0&1&0&1&1 \\ 0&0&1&0&0&0&0&0&0&0&1&1&0&1 \\ 0&0&0&1&0&0&0&0&0&1&0&0&0&1 \\ 0&0&0&0&1&0&0&0&0&1&0&0&1&0&1 \\ 0&0&0&0&0&1&0&0&0&1&0&1&0&0&1 \\ 0&0&0&0&0&0&1&0&0&0&1&0&1&1&1 \\ 0&0&0&0&0&0&0&1&0&0&1&0&1&1&0 \\ 0&0&0&0&0&0&0&0&1&0&1&0&1&0&1 \\ 0&0&0&0&0&0&0&0&0&1&1&0&0&1&1&0 \\ 0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&0 \end{bmatrix}_{(11\times 16)} . \begin{bmatrix} 1&0&0&0&1 \\ 0&1&0&0&1 \\ 1&1&0&0&1 \\ 0&0&1&0&1 \\ 1&0&1&0&1 \\ 0&1&1&0&1 \\ 1&1&1&0&1 \\ 0&0&0&1&1 \\ 1&0&0&1&1 \\ 0&1&0&1&1 \\ 1&1&0&1&1 \\ 0&0&1&1&1 \\ 1&0&1&1&1 \\ 0&1&1&1&1 \\ 1&1&1&1&1 \\ 0&0&0&0&1 \end{bmatrix}_{(16\times 5)} = \begin{bmatrix} 0&0&0&0&0 \\ 0&0&0&0&0 \\ 0&0&0&0&0 \\ 0&0&0&0&0 \\ 0&0&0&0&0 \\ 0&0&0&0&0 \\ 0&0&0&0&0 \\ 0&0&0&0&0 \\ 0&0&0&0&0 \\ 0&0&0&0&0 \\ 0&0&0&0&0 \end{bmatrix}_{(11\times 5)} = \mathbf{0}$$