



Bevezetés az algebra 2

BMETE91AM37



Alkalmazások

H607 – 2017-05-10



Wetttl Ferenc

ALGEBRA TANSZÉK

Kombinatorika

Kombinatorika

Fisher-egyenlőtlenség

- D Tekintsük a v -elemű P halmaz részhalmazainak egy halmazát. E részhalmazokat **blokkoknak** nevezzük, míg P elemeit pontoknak. Azt mondjuk, hogy e blokkok **2-struktúrát** alkotnak, ha P bármely két pontja pontosan $\lambda > 0$ számú blokkban van, és van legalább egy nem triviális blokk a rendszerben, azaz amelynek legalább 2 pontja van, de nem tartalmazza P összes pontját.
- T **Fisher-egyenlőtlenség**: Bármely 2-struktúra blokkjainak száma legalább annyi, mint pontjaié, azaz $b \geq v$.

B Jelöljék a 2-struktúra pontjait az 1-től v -ig terjedő egészek, a j -edik blokkot B_j ($j = 1, 2, \dots, b$). Illeszkedési mátrixa \mathbf{M} , ahol

$$m_{ij} = \begin{cases} 1, & \text{ha } i \in B_j, \\ 0, & \text{egyébként.} \end{cases}$$

$$\mathbf{A} = \mathbf{M}\mathbf{M}^T = \begin{bmatrix} r_1 & \lambda & \dots & \lambda \\ \lambda & r_2 & \dots & \lambda \\ \vdots & \vdots & \ddots & \vdots \\ \lambda & \lambda & \dots & r_v \end{bmatrix} = \lambda \mathbf{J}_v + \text{diag}(r_1 - \lambda, r_2 - \lambda, \dots, r_v - \lambda),$$

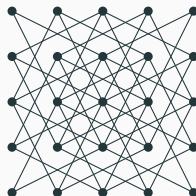
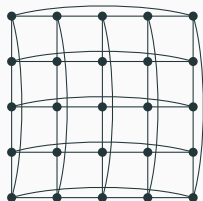
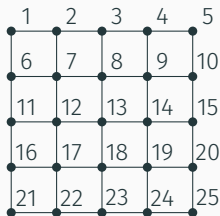
ahol \mathbf{J}_v a csupa 1-esből álló $v \times v$ -es mátrix, és r_i az i pont foka.

- A \mathbf{J}_v pozitív szemidefinit, ugyanis szimmetrikus és ha $\mathbf{0} \neq \mathbf{x} \in \mathbb{R}^v$ tetszőleges, akkor $\mathbf{x}^T \mathbf{J}_v \mathbf{x} = \sum_{i,j} x_i x_j = (\sum_i x_i)^2 \geq 0$.
- $\text{diag}(r_1 - \lambda, r_2 - \lambda, \dots, r_v - \lambda)$ poz.def, mert $r_i > \lambda$. ($r_i = \lambda$ esetén $\forall j \neq i$ pontra az i -t tartalmazó blokkok tartalmazzák j -t is, vagyis nem létezne nem triviális blokk.)
- Pozitív definit + pozitív szemidefinit = pozitív definit $\rightsquigarrow \mathbf{A}$ invertálható, rangja $v \rightsquigarrow \mathbf{M}_{v \times b}$ rangja $v \rightsquigarrow b \geq v$.

Kombinatorika

Lámpácskás játék

- m lámpák egyúttal kapcsolók is, megnyomásukra megváltozik a saját és bizonyos „szomszédai” állapota is.
- „XL25” 1983, Mérő László, „Lights Out!” 90-es évek
 - „Button Madness”, a szomszédtság a határon átnyúlik (tórusz),
 - „Gamze”, ahol a lámpák rombuszalakban vannak elhelyezve,
 - „Lights Out 2000”, a lámpáknak három állapotuk van (kikapcsolt, piros, zöld),
 - „Lights Out Cube”, a lámpák egy $3 \times 3 \times 3$ -as kocka oldalain vannak,
 - „Orbix”, ahol a lámpák egy dodekaéder csúcsaira vannak helyezve,
 - „Merlin”, 70-es évek 3×3 -as táblán

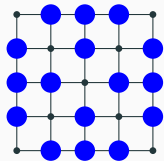


Illeszkedési mátrix

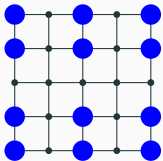
$$A = \begin{bmatrix} 110001000000000000000000 \\ 111000100000000000000000 \\ 011100010000000000000000 \\ 001110001000000000000000 \\ 000110000100000000000000 \\ 100001100010000000000000 \\ 010001110001000000000000 \\ 001000111000100000000000 \\ 000100011100010000000000 \\ 000010001100001000000000 \\ 000001000011000100000000 \\ 000000100011100010000000 \\ 000000001000111000100000 \\ 000000000100011000010000 \\ 000000000010001100001000 \\ 000000000001000011000100 \\ 000000000000100011100010 \\ 0000000000000010001110001 \\ 0000000000000000100001100 \\ 00000000000000000010001110 \\ 000000000000000000010001110 \\ 000000000000000000001000111 \\ 0000000000000000000001000111 \\ 00000000000000000000001000111 \end{bmatrix}$$

- Egy gomb páros sokszori megnyomása olyan, mintha egyszer sem nyomtuk volna meg, míg páratlan sokszori megnyomása egy nyomással ekvivalens. Eszerint a nyomások számát modulo 2 számolhatjuk, vagyis \mathbb{F}_2 elemeivel.
- Másrészt a fenti mátrix is tekinthető \mathbb{F}_2 fölöttinek, melynek i -edik oszlopa azt adja meg, hogy az i jelű gomb megnyomására mely lámpák állapota változik meg.
- Jelölje $\mathbf{x} \in \mathbb{F}_2^{25}$ azt a vektort, melynek x_i koordinátája 1, ha az i gombot páratlan sokszor nyomtuk meg, és 0, ha páros sokszor. \mathbf{Ax} azt a vektort adja eredményül, melynek i -edik koordinátája akkor 1, ha az i gomb állapota az \mathbf{x} vektor szerinti gombok megnyomása után megváltozik, és akkor 0, ha nem.
- Ha kezdetben a lámpák állapotát egy \mathbf{b} vektor írja le ($b_i = 1$, ha az i lámpa ég, $b_i = 0$, ha nem), akkor a lámpák pontosan akkor kapcsolhatók le, ha van olyan \mathbf{x} vektor, melyre $\mathbf{Ax} = \mathbf{b}$.

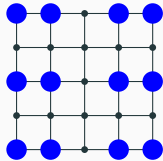
- Ezek tehát azok a minták, melyek gombjainak megnyomása nem változtatja meg a a lámpák állapotát:



az u vektor

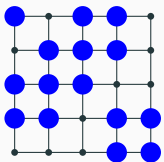


a v vektor

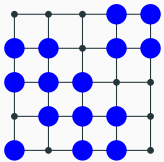


az $u + v$ vektor

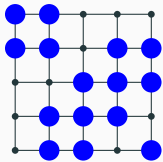
- A megoldások egyikéhez a nulltér fenti elemeit hozzáadva megkapjuk az összes megoldást:



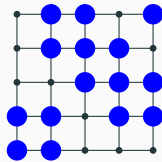
x



$x + u$



$x + v$



$x + u + v$

Kombinatorika

Gráfok

Á Egy egyszerű G gráf adjacencia (szomszédsági) mátrixát jelölje \mathbf{A}_G .
Ekkor

1. $\text{trace}(\mathbf{A}_G) = 0$
2. \mathbf{A}_G szimmetrikus 2×2 -es minorainak összege $= -|E(G)|$
3. \mathbf{A}_G szimmetrikus 3×3 -as minorainak összege $= 2 \times$ háromszögek száma.
4. Ha $d(i, j) = k$ (a két pont távolsága G -ben), akkor $\mathbf{I}, \mathbf{A}_G, \dots, \mathbf{A}_G^k$ lineárisan függetlenek.

B 1. A főátlóban 0-k vannak.

2. Az i -edik és j -edik sorok kerszteződésében lévő ilyen minor pontosan akkor nem a zérusmátrix, ha i és j indexű pontok össze vannak kötve G -ben, ekkor viszont a minor $|\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}| = -1$.

3.
$$\begin{vmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{vmatrix} = 2$$

Hibajavító kódok

Hibajelző és hibajavító kódok

D Hamming-távolság: $d_H(\mathbf{x}, \mathbf{y}) = |\{i : x_i \neq y_i\}|$

P $d_H(01001110, 01101100) = 2$

m ez metrika

Alappéldák: egyszerű hibajelző és hibajavító kódok

- P Ismétlődő kód:** a kódábécé tetszőleges, és a kód álljon azokból az n -hosszú kódszavakból, melyek minden koordinátája azonos. E kód legföljebb $n - 1$ hibát jelez, és $\lfloor \frac{n-1}{2} \rfloor$ hibát javít.
- P Paritásellenőrző kód:** $(n - 1)$ -hosszú \mathbf{b} bitvektorhoz még egy bitet csatolunk, melynek értéke 1, ha \mathbf{b} -ben páratlan sok bit egyenlő 1-gyel, egyébként 0, akkor olyan n -hosszú vektort kapunk, melyben páros sok 1-es van.

A paritásellenőrző kód 1-hibajelző, de jelez minden olyan hibát, melyben páratlan sok koordináta változik meg.

- P Nullösszegű kód:** \mathbb{Z}_m^n összes olyan $\mathbf{v} = (v_1, v_2, \dots, v_n)$ vektorából álló kód, melyekre $v_1 + v_2 + \dots + v_n = 0$, azaz melyekre $\mathbf{1} \cdot \mathbf{v} = 0$.

Hamming-kód

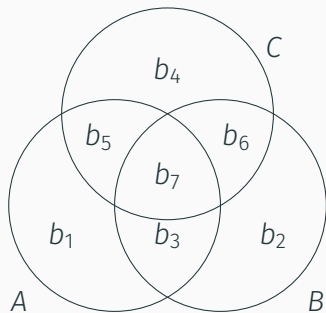
- P bináris, 7-hosszú, mely egy 4-hosszú üzenethez három paritásbitet ad. A kódolandó üzenet $b_3b_5b_6b_7$, a kód $\mathbf{b} = b_1b_2b_3b_4b_5b_6b_7$, a b_1, b_2, b_4 paritásbitekre fennállnak:

$$b_1 + b_3 + b_5 + b_7 = 0$$

$$b_2 + b_3 + b_6 + b_7 = 0$$

$$b_4 + b_5 + b_6 + b_7 = 0$$

- Á A kód \mathbb{F}_2^7 16 vektorából áll, 2-hibajelző, és 1-hibajavító. \mathbb{F}_2^7 minden vektora vagy kódvektor, vagy egyetlen koordináta megváltoztatásával azzá tehető!
- J Bináris $[7, 4, 3]_2$ Hamming-kód
- Á A fenti Hamming-kód perfekt, azaz a kódszavak köré emelt – Hamming-távolságban mérve – 1-sugarú gömbök hézagtalanul és átfedés nélkül lefedik az \mathbb{F}_2^7 teret.



HF 7 halálraítélt körben ül, mindegyikük fején egy véletlenül kiválasztott piros vagy fekete sapka. Mindenki látja a többiek sapkáját, de a sajátját senki. Semmi módon nem kommunikálhatnak egymással. Egy idő után egyszerre mindegyiküknek tippelnie kell a saját sapkája színére. Három válasz lehetséges: „nem tudom”, „fekete”, „piros”. Ha senki nem találja el, vagy csak egy is akad, aki téved, mind meghalnak, egyébként mind megmenekülnek. Javasoljunk olyan eljárást, amivel a legnagyobb eséllyel menekülhetnek?

P 4-hosszú ternér $[4, 2, 3]_3$ Hamming-kód Az \mathbb{F}_3^4 tér összes $(a, b, a + b, a - b)$ alakú vektorának halmaza egy 1-hibajavító, 3-kódtávolságú kód. (kódtávolság = $\min d_H(\mathbf{u}, \mathbf{v})$, ha $\mathbf{u} \neq \mathbf{v}$)

B \mathbb{F}_3 -ban $-1 = 2$, tehát $a - b = a + 2b$

az $a, b, a + b, a - b$ értékek közül bármely kettő egyértelműen megadja a másik kettőt is. Például az

$$a + b = x$$

$$a - b = y$$

egyenletrendszer egyértelműen megoldható a -ra és b -re

\rightsquigarrow a kódtávolság legalább 3, de pl $d(0000, 0112) = 3$, ezért a kód 1-hibajavító.

Hibajavító kódok

Lineáris kódok

- D** Az \mathbb{F}_q test fölött értelmezett $\mathcal{C} \subseteq \mathbb{F}_q^n$ kódot **lineáris** $[n, k]_q$ -kódnak nevezzük, ha \mathcal{C} az \mathbb{F}_q^n vektortér egy k -dimenziós altere. Szokás az $[n, k, d]_q$ jelölés használata a d -távolságú lineáris kódra.
- Á** Az eddig ismertetett kódok mind lineárisak.
- B** ismétlő kód $[n, 1, n]_q$ -kód, a paritásellenőrző kód $[n, n - 1, 2]_2$ -kód, a nullösszegű kód $[n, n - 1, 2]_q$ -kód, a bináris Hamming-kód $[7, 4, 3]_2$ -kód, a ternér Hamming-kód $[4, 2, 3]_3$ -kód.

Generátormátrix

D $\mathcal{C} \leq \mathbb{F}_q^n$ k -dimenziós lineáris altér, kódolás $\mathbb{F}_q^k \rightarrow \mathcal{C} \leq \mathbb{F}_q^n$. Legyen $\mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_k$ a \mathcal{C} egy bázisa. Egy tetszőleges $\mathbf{x} \in \mathbb{F}_q^k$ vektor (üzenet) $\mathbf{c} \in \mathcal{C}$ kódja legyen $\mathbf{c} = x_1\mathbf{g}_1 + x_2\mathbf{g}_2 + \dots + x_k\mathbf{g}_k$, azaz

$$\mathbf{c} = \mathbf{xG},$$

ahol a $k \times n$ -es \mathbf{G} mátrix – az úgynevezett **generátormátrix** – sorvektorai \mathcal{C} bázisának elemei.

P **Ismétlő kód.** Így $\mathbf{G} = [1 \ 1 \ \dots \ 1]$.

P **Paritásellenőrző kód, nullösszegű kód.**

$(a_1, \dots, a_{n-1}) \in \mathbb{F}_q^{n-1} \mapsto (a_1, \dots, a_{n-1}, -\sum_{i=1}^{n-1} a_i) \in \mathbb{F}_q^n$ mátrixa

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & \dots & 0 & -1 \\ 0 & 1 & \dots & 0 & -1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -1 \end{bmatrix}$$

P $[7, 4, 3]_2$ Hamming-kód. Az $\mathbb{F}_2^4 \rightarrow \mathbb{F}_2^7 : (b_3, b_5, b_6, b_7) \mapsto (b_1, \dots, b_7)$, ahol $b_1 = b_3 + b_5 + b_7$, $b_2 = b_3 + b_6 + b_7$, $b_4 = b_5 + b_6 + b_7$ leképezés mátrixa

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

Például az $\mathbf{x} = (0, 1, 1, 0)$ üzenet kódja

$$\begin{aligned} \mathbf{c} = \mathbf{xG} &= \begin{bmatrix} 0 & 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 \end{bmatrix} \end{aligned}$$

P Ternér $[4, 2, 3]_3$ Hamming-kód. A

$\mathbb{F}_3^2 \rightarrow \mathbb{F}_3^4 : (a, b) \mapsto (a, b, a + b, a + 2b)$ leképezés mátrixa

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

D A \mathcal{C} kód **duálisán** a

$$\mathcal{C}^\perp = \{ \mathbf{v} \in \mathbb{F}_q^n : \mathbf{v} \cdot \mathbf{c} = 0 \text{ minden } \mathbf{c} \in \mathcal{C} \text{ kódot} \}$$

kódszóra értjük, mely egy lineáris kód. A \mathcal{C}^\perp kód \mathbf{H} generátormátrixát a \mathcal{C} kód **ellenőrző mátrixának** nevezzük. (Használatos még a *paritásmátrix* vagy a paritásellenőrző mátrix elnevezés is, bár paritásról csak a $q = 2$ esetben van szó.)

T Ha \mathcal{C} egy lineáris $[n, k]$ -kód, akkor

1. $\mathcal{C}^\perp = \{ \mathbf{v} \in \mathbb{F}_q^n : \mathbf{v}\mathbf{G}^\top = \mathbf{0} \},$

2. \mathcal{C}^\perp egy $[n, n - k]$ -kód,

3. $\mathcal{C}^{\perp\perp} := (\mathcal{C}^\perp)^\perp = \mathcal{C},$

4. $\mathcal{C} = \{ \mathbf{c} \in \mathbb{F}_q^n : \mathbf{c}\mathbf{H}^\top = \mathbf{0} \},$

5. $\mathbf{G}\mathbf{H}^\top = \mathbf{0}_{k \times (n-k)}, \mathbf{H}\mathbf{G}^\top = \mathbf{0}_{(n-k) \times k},$

6. ha $\mathbf{G} = [\mathbf{I}_k | \mathbf{A}]$ a \mathcal{C} kód standard alakú generátormátrixa, akkor ellenőrző mátrixa $\mathbf{H} = [-\mathbf{A}^\top | \mathbf{I}_{n-k}]$.

B 1. \checkmark (\mathcal{C}^\perp megegyezik \mathbf{G}^\top bal magterével) \rightsquigarrow

2. $\dim(\mathcal{C}^\perp) + k = n$, azaz $\dim(\mathcal{C}^\perp) = n - k$.

3. Ezt az érvelést megismételve $\mathcal{C}^{\perp\perp}$ -re: $\mathcal{C}^{\perp\perp}$ egy $[n, k]$ -kód. E kód tartalmazza \mathcal{C} -t, és dimenziójuk megegyezik, így $\mathcal{C}^{\perp\perp} = \mathcal{C}$.

4. következik 1.-ből

5. $\forall \mathbf{x} \in \mathbb{F}_q^k$ vektorra $\mathbf{x}\mathbf{G} \in \mathcal{C}$, azaz $\mathbf{x}\mathbf{G}\mathbf{H}^\top = \mathbf{0} \rightsquigarrow \mathbf{G}\mathbf{H}^\top = \mathbf{0}$

6. $\mathbf{G}\mathbf{H}^\top = \mathbf{0}$, így bármely $\mathbf{c} = \mathbf{x}\mathbf{G}$ kódszóra $\mathbf{c}\mathbf{H}^\top = \mathbf{x}\mathbf{G}\mathbf{H}^\top = \mathbf{x}\mathbf{0} = \mathbf{0}$, tehát \mathbf{H} valóban ellenőrző mátrix, mivel sorai lin. ftlenek.

Hibajavító kódok

Hamming kód

A Hamming kód konstrukciója

D A \mathbf{H} oszlopai között \mathbb{F}_q^r minden nemnulla vektorának pontosan egy nem nulla konstansszorososa szerepeljen (mint a projektív koordináták). Azt a kódot, melynek a \mathbf{H} mátrix az ellenőrző mátrixa, r paraméterű \mathbb{F}_q feletti $H_{r,q}$ **Hamming-kódnak**, duálisát $S_{r,q}$ **szimplex kódnak** nevezzük.

T A $H_{r,q}$ Hamming-kód

$$\left[\frac{q^r - 1}{q - 1}, \frac{q^r - 1}{q - 1} - r, 3 \right]_q$$

paraméterű perfekt kód, a $H_{2,q}$ kód $q > 2$ esetén $[q + 1, q - 1, 3]_q$ paraméterű.

B A Hamming-kód paraméterei a definícióból adódnak, $d = 3$, mert \mathbf{H} -ban bármely két oszlop független, de van három összefüggő. A kód perfektsége egyszerű számolással adódik.

Titokmegosztás

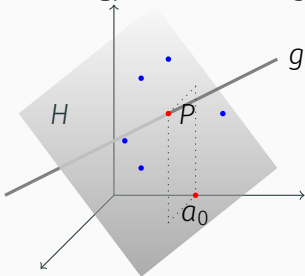
Küszöbséma interpolációs polinommal (Shamir)

n ember közül bármely k föl tudja fedni a titkot: (n, k)
küszöbséma.

Interpolációs polinommal: már volt

Geometriai konstrukció (Blakley)

- K a t -dimenziós $\mathcal{V} = \mathbb{F}_q^t$ tér egy véletlen $P = (a_0, \dots, a_{t-1})$ pontjának első koordinátája a titok. Publikálva van egy ezen a ponton átmenő g egyenes, mely nem merőleges az $\mathbf{e}_1 = (1, 0, \dots, 0)$ vektorra, így pontjainak első koordinátái végigfutnak \mathbb{F}_q elemein.
- A résztvevők megkapják egy P -n átmenő, de \mathbf{e}_1 -re nem merőleges és g -t nem tartalmazó H (affin) hipersík egy-egy általános helyzetű pontját. Így bármely t résztvevő egyértelműen föl tudja írni H egyenletét, és a g -vel való metszéspontját.



Tetszőleges részhalmazokra (Brickel)

K titok: $\mathbf{a} = (a_0, a_1, \dots, a_t) \in \mathbb{F}_q^{t+1}$ vektort első koordinátája, az $a_0 \in \mathbb{F}_q$

A p_i résztvevőhöz rendel egy $\mathbf{v}_i \in \mathbb{F}_q^t$ vektort, publikálja.

résztitok: $s_i = \mathbf{v}_i \cdot \mathbf{a} \in \mathbb{F}_q$

T Jelölje $T \subseteq P$ a résztvevők egy halmazát. A T -be tartozó résztvevők pontosan akkor tudják meghatározni a_0 -t, ha az $\mathbf{e}_1 = (1, 0, \dots, 0)$ vektor benne van a T -beli résztvevők vektorai által kifeszített altérben. Ha \mathbf{e}_1 nincs ebben az altérben, a T -beli résztvevők semmit nem tudnak meg a titokról.

B A \mathbf{V} mátrix sorai a T -beliek vektorai, és \mathbf{s} koordinátái a T -beliek résztitkai.

TFH $\mathbf{e}_1 \in \mathcal{S}(\mathbf{V}) \rightsquigarrow$ létezik olyan \mathbf{w} vektor, hogy $\mathbf{w}^T \mathbf{V} = \mathbf{e}_1^T$, így $\mathbf{w}^T \mathbf{V} \mathbf{a} = a_0$. Mivel a konstrukció szerint $\mathbf{V} \mathbf{a} = \mathbf{s}$, ezért $\mathbf{w}^T \mathbf{s} = a_0$, hisz \mathbf{w} a T -beli résztvevők által meghatározható.

TFH $\mathbf{e}_1 \notin \mathcal{S}(\mathbf{V})$. $\mathbf{V} = [\mathbf{u}_0 | \mathbf{u}_1 | \dots | \mathbf{u}_t]$. Ha $\mathbf{u}_0 \notin \text{span}(\mathbf{u}_1, \dots, \mathbf{u}_t)$, akkor van olyan \mathbf{d} vektor, hogy $\mathbf{d} \cdot \mathbf{u}_i = 0$, ha $i = 1, 2, \dots, t$, és $\mathbf{d} \cdot \mathbf{u}_0 = 1$.
 $\rightsquigarrow \mathbf{d}^T \mathbf{V} = \mathbf{e}_1$, ellentmondás $\rightsquigarrow \mathbf{u}_0 \in \text{span}(\mathbf{u}_1, \dots, \mathbf{u}_t)$, így van olyan \mathbf{w} vektor, hogy $\mathbf{V} \mathbf{w} = \mathbf{0}$, de $w_0 \neq 0$. Az ugyan igaz, hogy $\mathbf{s} = \mathbf{V} \mathbf{a}$, de tetszőleges $c \in \mathbb{F}_q$ konstansra $\mathbf{s} = \mathbf{V} \mathbf{a} = \mathbf{V}(\mathbf{a} + c \mathbf{w})$ is teljesül. Így bármely c_0 -hoz található olyan $\mathbf{c} = (c_0, c_1, \dots, c_t)$ vektor, hogy $\mathbf{s} = \mathbf{V} \mathbf{c}$. Így a T -beli résztvevők semmit nem tudhatnak a_0 -ról.