Bevezetés az algebrába 2 – Lineáris algebra alkalmazásai

Wettl Ferenc
Algebra Tanszék

BUDAPESTI MŰSZAKI
MATEMATIKA
ÉS GAZDASÁGTUDOMÁNYI
INTÉZET
EGYETEM

2016. május 27.

Fisher-egyenlőtlenség

P Tekintsük a v-elemű P halmaz részhalmazainak egy halmazát. E részhalmazokat blokkoknak is szokás hívni, 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 Bármely 2-struktúra blokkjainak száma legalább annyi, mint pontjaié, azaz $b \geqslant v$.

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

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

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

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

- A $\mathbf{J}$ pozitív szemidefinit, ugyanis szimmetrikus és ha $\mathbf{0} \neq \mathbf{x} \in \mathbb{R}^v$ tetszőleges, akkor $\mathbf{x}^{\mathsf{T}}\mathbf{J}_v\mathbf{x} = \sum_{i,j} x_i x_j = \left(\sum_i x_i\right)^2 \geqslant 0$.
- $\operatorname{diag}(r_1 - \lambda, r_2 - \lambda, \ldots, r_v - \lambda)$ minden főátlóbeli eleme pozitív, ugyanis $r_i > \lambda$, tehát e mátrix pozitív definit.
  (Ha $r_i = \lambda$ volna, akkor minden $j \neq i$ pontra az i-t tartalmazó blokkok tartalmaznák 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 $\rightsquigarrow$ $b \geqslant v$.

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** Ismétlő 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 $\mathbf{v} = (v_1, v_2, \ldots, v_n)$ vektorából álló kód, melyekre $v_1 + v_2 + \cdots + v_n = 0$, azaz melyekre $\mathbf{1} \cdot \mathbf{v} = 0$.

Hamming-kód

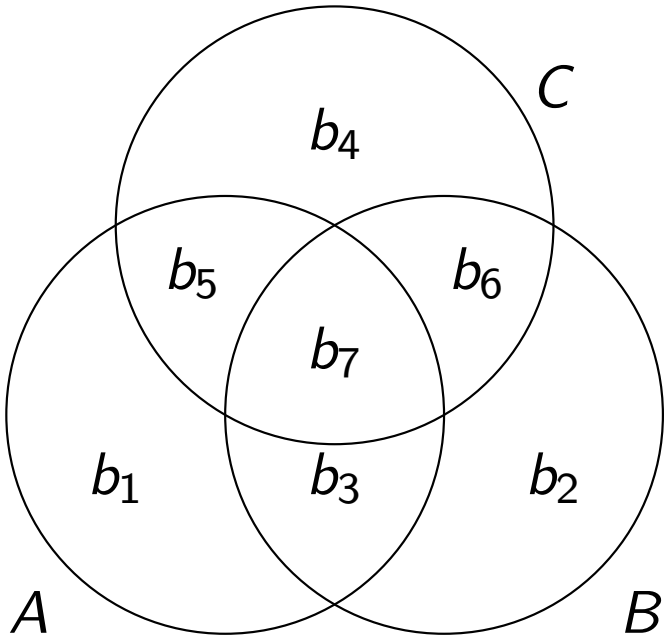
P bináris, 7-hosszú, mely egy 4-hosszú üzenethez három paritásbitet ad. A kódolandó üzenet $b_3 b_5 b_6 b_7$, a kód $\mathbf{b} = b_1 b_2 b_3 b_4 b_5 b_6 b_7$, a b_1, b_2, b_4 paritásbitek a következő egyenlőségekből számolandók:

$$b_1 + b_3 + b_5 + b_7 = 0$$
$$b_2 + b_3 + b_6 + b_7 = 0$$
$$b_4 + b_5 + b_6 + b_7 = 0$$

Á A fent definiált Hamming-kód $\mathbb{F}_2^7$ 16 vektorából áll, 2-hibajelző, és 1-hibajavító. $\mathbb{F}_2^7$ minden vektora vagy fenti egyenletek által definiált bináris 7-hosszú Hamming-kódhoz tartozó 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 senki se látja a sajátját. 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. Tudunk-e számukra olyan eljárást javasolni, ami 1/2-nél nagyobb valószínűséggel megmenekíti őket. Mi a legnagyobb valószínűség, amit el tudunk érni?

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.

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

$$\mathbf{c} = \mathbf{x}\mathbf{G},$$

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

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

P Paritásellenőrző kód, nullösszegű kód. $(a_1, \ldots, a_{n-1}) \in \mathbb{F}_q^{n-1} \mapsto (a_1, \ldots, a_{n-1}, -\sum_{i=1}^{n-1} a_i) \in \mathbb{F}_q^n$ leképezés mátrixa

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

P $[7,4,3]_2$ Hamming-kód. Az $\mathbb{F}_2^4 \to \mathbb{F}_2^7 : (b_3, b_5, b_6, b_7) \mapsto (b_1, \ldots, b_7)$, 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

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

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

P Ternér $[4, 2, 3]_3$ Hamming-kód. A $\mathbb{F}_3^2 \to \mathbb{F}_3^4 : (a, b) \mapsto (a, b, a + b, a + 2b)$ leképezés mátrixa

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

Ellenőrző mátrix

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. $\mathcal{C}^\perp = \{\, \mathbf{v} \in \mathbb{F}_q^n : \mathbf{v}\mathbf{G}^\mathsf{T} = \mathbf{0} \,\}$,
2. $\mathcal{C}^\perp$ egy $[n, n-k]$-kód,
3. $\mathcal{C}^{\perp\perp} := (\mathcal{C}^\perp)^\perp = \mathcal{C}$,
4. $\mathcal{C} = \{\, \mathbf{c} \in \mathbb{F}_q^n : \mathbf{c}\mathbf{H}^\mathsf{T} = \mathbf{0} \,\}$,
5. $\mathbf{G}\mathbf{H}^\mathsf{T} = \mathbf{O}_{k\times(n-k)}$, $\mathbf{H}\mathbf{G}^\mathsf{T} = \mathbf{O}_{(n-k)\times k}$,
6. ha $\mathbf{G} = [\mathbf{I}_k|\mathbf{A}]$ a $\mathcal{C}$ kód standard alakú generátormátrixa, akkor ellenőrző mátrixa $\mathbf{H} = [-\mathbf{A}^\mathsf{T}|\mathbf{I}_{n-k}]$.

B 1. ✓ ($\mathcal{C}^\perp$ megegyezik $\mathbf{G}^\mathsf{T}$ 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 kapjuk, hogy $\mathcal{C}^{\perp\perp}$ 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. Mivel minden $\mathbf{x} \in \mathbb{F}_q^k$ vektorra $\mathbf{x}\mathbf{G} \in \mathcal{C}$, azaz $\mathbf{x}\mathbf{G}\mathbf{H}^\mathsf{T} = \mathbf{0}$, ezért $\mathbf{G}\mathbf{H}^\mathsf{T}$ csak a zérusleképezés lehet.

6. $\mathbf{G}\mathbf{H}^\mathsf{T} = \mathbf{O}$, így bármely $\mathbf{c} = \mathbf{x}\mathbf{G}$ kódszóra $\mathbf{c}\mathbf{H}^\mathsf{T} = \mathbf{x}\mathbf{G}\mathbf{H}^\mathsf{T} = \mathbf{x}\mathbf{O} = \mathbf{0}$, tehát szerint $\mathbf{H}$ valóban ellenőrző mátrix, mivel sorai lineárisan függetlenek

A Hamming kód konstrukciója

D Vegyünk egy olyan **H** mátrixot, melynek oszlopai között $\mathbb{F}_q^r$ minden nemnulla vektorának pontosan egy nem nulla konstansszorosa szerepel. (Például ilyen az a mátrix, mely az összes olyan nemnulla oszlopvektorból áll, melynek első nemnulla koordinátája 1.) Azt a kódot, melynek a **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 **H**-ban bármely két oszlop független, de van három összefüggő. A kód perfektsége egyszer számolással adódik.

Küszöbséma interpolációs polinommal (Shamir)

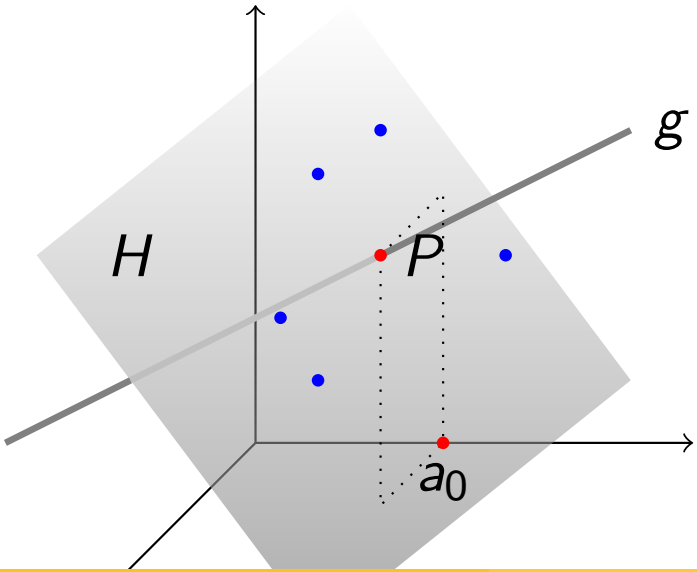
n ember közül bármely k föl tudja fedni a titkot: (n, k) küszöbséma.

Interpolációs polinommal: már volt

Geometriai konstrukció (Blakley)

K a t-dimenziós $\mathcal{V} = \mathbb{F}_q^t$ tér egy véletlen $P = (a_0, \ldots, a_{t-1}$ pontjának első koordinátája a titok. Publikálva van egy ezen a ponton átmenő g egyenes, mely nem merőleges az $\mathbf{e}_1 = (1, 0, \ldots, 0)$ 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 általános helyzetű pontjait.
- Ez azt jelenti, hogy bármely t résztvevő egyértelműen föl tudja írni H egyenletét, így a g-vel való metszéspontját is.



Tetszőleges részhalmazokra (Brickel)

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

A p_i résztvevőhö 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 $\mathbf{e}_1 = (1, 0, \ldots, 0)$ 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.

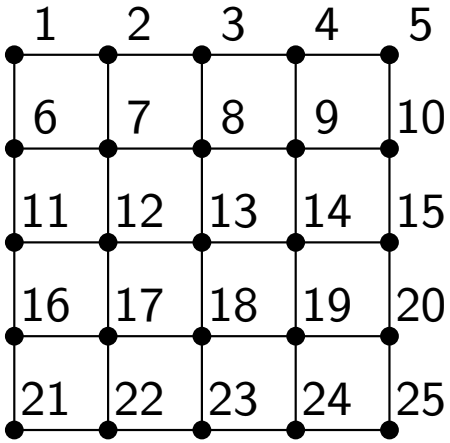
TFH $\mathbf{e}_1 \in \mathcal{S}(\mathbf{V}) \rightsquigarrow$ létezik olyan $\mathbf{w}$ vektor, hogy $\mathbf{w}^\mathsf{T}\mathbf{V} = \mathbf{e}_1^\mathsf{T}$, így $\mathbf{w}^\mathsf{T}\mathbf{V}\mathbf{a} = a_0$. Mivel a konstrukció szerint $\mathbf{V}\mathbf{a} = \mathbf{s}$, ezért $\mathbf{w}^\mathsf{T}\mathbf{s}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

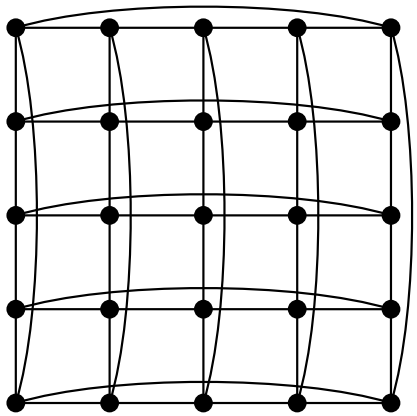
TFH $\mathbf{e}_1 \notin \mathcal{S}(\mathbf{V})$. $\mathbf{V} = [\mathbf{u}_0|\mathbf{u}_1|\ldots|\mathbf{u}_t]$. Ha $\mathbf{u}_0 \notin \operatorname{span}(\mathbf{u}_1, \ldots, \mathbf{u}_t)$, akkor van olyan $\mathbf{d}$ vektor, hogy $\mathbf{d} \cdot \mathbf{u}_i = 0$, ha $i = 1, 2, \ldots, t$, és $\mathbf{d} \cdot \mathbf{u}_0 = 1$.

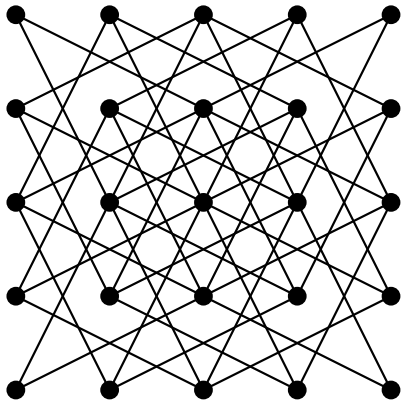
$\rightsquigarrow \mathbf{d}^\mathsf{T}\mathbf{V} = \mathbf{e}_1$, ellentmondás $\rightsquigarrow \mathbf{u}_0 \in \operatorname{span}(\mathbf{u}_1, \ldots, \mathbf{u}_t)$, így van olyan $\mathbf{w}$ vektor, hogy $\mathbf{V}\mathbf{w} = \mathbf{0}$, de $w_0 \neq 0$. Az ugyan igaz, hogy $\mathbf{s} = \mathbf{V}\mathbf{a}$, 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 $\mathbf{c} = (c_0, c_1 \ldots, c_t)$ vektor, hogy $\mathbf{s} = \mathbf{V}\mathbf{c}$. Így a T-beli résztvevők semmit nem tudhatnak a_0-ról.

m lámpák egyúttal kapcsolók is, megnyomásukra megváltozik a saját és bizonyos „szomszédaik” állapota is.

- „XL25” 1983 (nem került forgalomba)
- „Button Madness”, ahol a szomszédság a határon átnyúlik és a szemközti oldalon folytatódik (tórusz),
- „Gamze”, ahol a lámpák rombuszalakban vannak elhelyezve,
- „Lights Out 2000”, ahol a lámpáknak nem két, hanem három állapotuk van (kikapcsolt, piros, zöld),
- „Lights Out Cube”, ahol a lámpák egy $3 \times 3 \times 3$-as kocka oldalain vannak,
- „Orbix”, ahol a lámpák egy dodekaéder csúcsaira vannak helyezve,
- „Merlin”, ami a hetvenes években jelent meg, 3×3-as táblán kellett játszani, és valószínűleg a legelső megjelent lámpás játék lehetett.







Illeszkedési mátrix

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

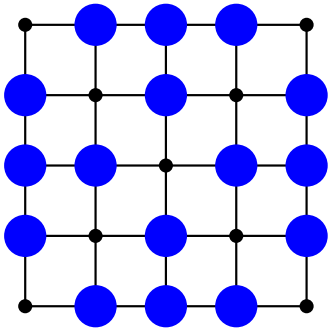
- Egy gomb páros sokszori megnyomása olyan, mintha egyszer sem nyomtuk volna meg, míg páratlan sokszori megnyomása egy nyomással ekvivalens. Eszerint a nyomások számát modulo 2 számolhatjuk, vagyis $\mathbb{F}_2$ elemeivel.
- Másrészt a fenti mátrix is tekinthető $\mathbb{F}_2$ fölöttinek, melynek i-edik 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 e lámpák pontosan akkor kapcsolhatók le, ha van olyan $\mathbf{x}$ vektor, melyre $\mathbf{Ax} = \mathbf{b}$.

- Ha minden lámpa ég, akkor az $\mathbf{Ax} = \mathbf{1}$ egyenletet kell megoldani:

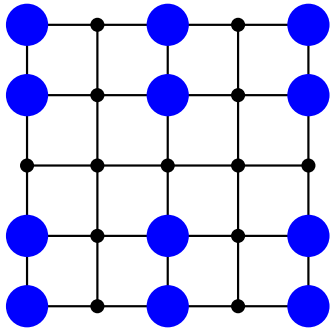
$$\mathbf{R} = \mathbf{rref}(\mathbf{A}) = \begin{bmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&1&1\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0
\end{bmatrix}$$

- $\mathbf{A}$ nem invertálható $\rightsquigarrow$ $\mathbf{Ax} = \mathbf{b}$ nem oldható meg minden $\mathbf{b}$ vektorra!
- Az $\mathbf{A}$ rangja 23, tehát $\mathbf{A}$ magterének dimenziója $25 - 23 = 2$, négy vektora: $\mathbf{0}$, $\mathbf{u} = (01110101011101110101011 10)$,
  $\mathbf{v} = (10101101010000010101101 01)$,
  $\mathbf{u} + \mathbf{v} = (11011000001101100000110 11)$.

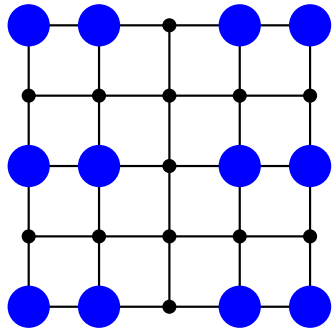
- Ezek tehát azok a minták, melyek gombjainak megnyomása nem változtatja meg a a lámpák állapotát:



az $\mathbf{u}$ vektor

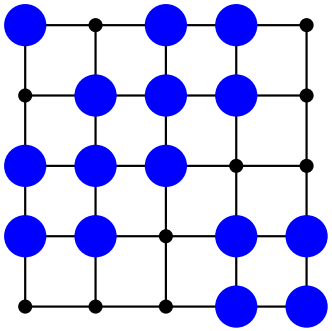


a $\mathbf{v}$ vektor

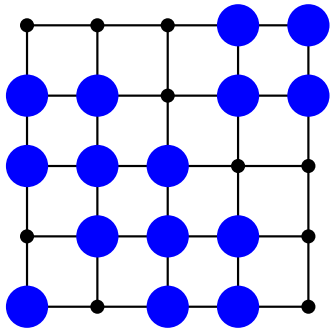


az $\mathbf{u}+\mathbf{v}$ vektor

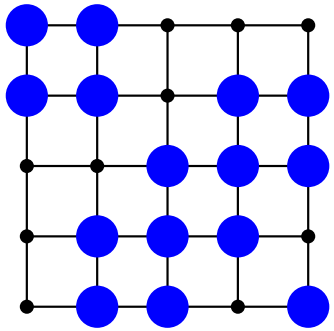
- A megoldások egyikéhez a nulltér fenti elemeit hozzáadva megkapjuk az összes megoldást:



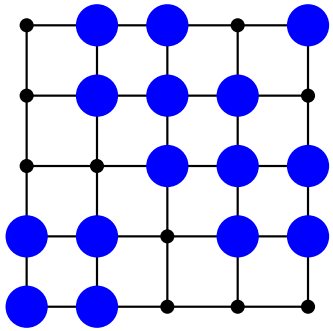
$\mathbf{x}$



$\mathbf{x}+\mathbf{u}$



$\mathbf{x}+\mathbf{v}$



$\mathbf{x}+\mathbf{u}+\mathbf{v}$