# Diszkrét matematika 2.C szakirány

## 11. előadás

Nagy Gábor
nagygabr@gmail.com
nagy@compalg.inf.elte.hu
compalg.inf.elte.hu/∼nagy

Komputeralgebra Tanszék

2017. tavasz

# Lineáris kódok

A kód távolsága leolvasható az ellenőrző mátrixból.

## Állítás

Legyen $\mathbf{H}$ egy $[n, k]$ kód ellenőrző mátrixa. A $\mathbf{H}$-nak pontosan akkor van $l$ darab lineárisan összefüggő oszlopa, ha van olyan kódszó, aminek a súlya legfeljebb $l$.

## Bizonyítás

Legyen $\mathbf{H} = \begin{pmatrix} \underline{h_1} & \underline{h_2} & \cdots & \underline{h_n} \end{pmatrix}$.

$\Longrightarrow$

Ekkor $\sum_{j=1}^{l} u_j \cdot \underline{h_{l_j}} = \underline{0}$. Tekintsük azt a vektort, aminek az $l_j$-edik koordinátája $u_j$, a többi pedig $0$. Ez egyrészt kódszó lesz (Miért?), másrészt a súlya legfeljebb $l$.

$\Longleftarrow$

Legyen $\underline{u} = (u_1, u_2, \ldots, u_n)^T$ az a kódszó, aminek a súlya $l$. Ekkor $\mathbf{H}$-nak az $\underline{u}$ nem-nulla koordinátáinak megfelelő oszlopai lineárisan összefüggőek.

# Lineáris kódok

## Következmény

A kód távolsága a legkisebb pozitív egész $l$, amire létezik az ellenőrző mátrixnak $l$ darab lineárisan összefüggő oszlopa.

## Példa

A (*) kód esetén:

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Egyik oszlopvektor sem a nullvektor, így nincs 1 darab lineárisan összefüggő oszlop.
Egyik oszlopvektor sem többszöröse egy másiknak, így nincs 2 darab lineárisan összefüggő oszlop.
Az 1., 3. és 5. oszlopok lineárisan összefüggőek, így a kód távolsága 3.

# Lineáris kódok

A $\mathbf{H}$ ellenőrző mátrix segítségével dekódolni is lehet.

## Definíció

Adott $\underline{v} \in \mathbb{F}_q^n$ esetén az $\underline{s} = \mathbf{H}\underline{v} \in \mathbb{F}_q^{n-k}$ vektort szindrómának nevezzük.

## Megjegyzés

A $\underline{v}$ pontosan akkor kódszó, ha $\underline{s} = \underline{0}$.

## Definíció

Legyen $\underline{c}$ a kódszó, $\underline{v}$ a vett szó. Az $\underline{e} = \underline{v} - \underline{c}$ a hibavektor.

## Állítás

$\mathbf{H}\underline{v} = \mathbf{H}\underline{e}$.

## Bizonyítás

$\mathbf{H}\underline{v} = \mathbf{H}(\underline{c} + \underline{e}) = \mathbf{H}\underline{c} + \mathbf{H}\underline{e} = \underline{0} + \mathbf{H}\underline{e} = \mathbf{H}\underline{e}$

# Lineáris kódok

A dekódolás elve: $\underline{v}$-ből kiszámítjuk a $\mathbf{H}\underline{v}$ szindrómát, ami alapján megbecsüljük az $\underline{e}$ hibavektort, majd meghatározzuk $\underline{c}$-t a $\underline{c} = \underline{v} - \underline{e}$ képlet segítségével.

## Definíció

Valamely $\underline{e}$ hibavektorhoz tartozó mellékosztály az $\{\underline{e} + \underline{c} : c \text{ kódszó}\}$ halmaz.

## Megjegyzés

Az $\underline{e} = \underline{0}$-hoz tartozó mellékosztály a kód.

## Állítás

Az azonos mellékosztályban lévő szavak pontosan az azonos szindrómájú szavak.

## Bizonyítás

Meggondolni...

# Lineáris kódok

## Definíció

Minden $\underline{s}$ szindróma esetén legyen $\underline{e_s}$ az a minimális súlyú szó, melynek $\underline{s}$ a szindrómája. Ez az $\underline{s}$ szindrómához tartozó mellékosztály-vezető, a mellékosztály elemei $\underline{e_s} + \underline{c}$ alakúak, ahol $\underline{c} \in K$ kódszó.

## Szindrómadekódolás

Adott $\underline{v}$ esetén tekintsük az $\underline{s} = \mathbf{H}\underline{v}$ szindrómát, és az $\underline{e_s}$ mellékosztály-vezetőt. Dekódoljuk $\underline{v}$-t $\underline{c} = \underline{v} - \underline{e_s}$-nek.

## Állítás

Legyen $\underline{c}$ a kódszó, $\underline{v} = \underline{c} + \underline{e}$ a vett szó, ahol $\underline{e}$ a hiba, és $w(\underline{e}) < d/2$, ahol $d$ a kód távolsága. Ekkor a szindrómadekódolás a minimális távolságú dekódolásnak felel meg.

# Lineáris kódok

## Bizonyítás

Egyrészt a korábbi állítás alapján $\underline{s} = \mathbf{H}\underline{v} = \mathbf{H}\underline{e}$, másrészt $\underline{e_s}$ definíciója miatt $\underline{s} = \mathbf{H}\underline{e_s}$. Ezért $\underline{e}$ és $\underline{e_s}$ ugyanabban a mellékosztályban van, továbbá $w(\underline{e_s}) \leq w(\underline{e})$.
$w(\underline{e} - \underline{e_s}) = d(\underline{e}, \underline{e_s}) \leq d(\underline{e}, \underline{0}) + d(\underline{0}, \underline{e_s}) = w(\underline{e}) + w(\underline{e_s}) < d$.
De $\mathbf{H}(\underline{e} - \underline{e_s}) = \underline{0}$ miatt $\underline{e} - \underline{e_s}$ kódszó (Miért?), így $\underline{e} = \underline{e_s}$.

## Példa

Tekintsük a (*) kódot.
$\underline{v} = (1, 1, 0, 1, 1)^T$ esetén $\mathbf{H}\underline{v} = \underline{0}$, így $\underline{v}$ kódszó.
$\underline{v} = (1, 1, 0, 0, 1)^T$ esetén $\mathbf{H}\underline{v} = (0, 1, 0)^T = \underline{s}$.
Mi az $\underline{s}$-hez tartozó mellékosztály-vezető?
A $(0, 0, 0, 1, 0)^T$ súlya 1, és a szindrómája a keresett $(0, 1, 0)^T$, így ez lesz a mellékosztály-vezető.
$\underline{c} = \underline{v} - \underline{e_s} = (1, 1, 0, 0, 1)^T - (0, 0, 0, 1, 0)^T = (1, 1, 0, 1, 1)^T$

# Lineáris kódok

## Emlékeztető (Hamming-korlát)

Ha $K \subset A^n$, $|A| = q$ és $K$ $t$-hibajavító, akkor

$$|K| \sum_{j=0}^{t} \binom{n}{j} (q-1)^j \leq q^n.$$

Egyenlőség esetén perfekt kódról beszélünk.

## Definíció

Az 1-hibajavító perfekt lineáris kódot Hamming-kódnak nevezzük.

## Emlékeztető

A kód távolsága a legkisebb pozitív egész $l$, amire létezik az ellenőrző mátrixnak $l$ darab lineárisan összefüggő oszlopa.

# Lineáris kódok

Ha egy olyan bináris kódot készítünk, amelyre a **H** ellenőrző mátrix oszlopainak a különböző nemnulla, $r$ hosszú vektorokat választjuk, akkor egy 1-hibajavító kódot kapunk (Miért?).
Ekkor a Hamming-korlát alakja:
$2^k(1+n) \leq 2^n$.
Egyenlőség esetén $n = 2^{n-k} - 1$, és pont ennyi $n-k$ hosszú, nemnulla vektor van.

$n = 2^r - 1$ esetén $k = n - \log(n+1)$, így a megfelelő $(n,k)$ párok:

| $n$ | 3 | 7 | 15 | 31 | 63 | 127 | $\cdots$ |
|---|---|---|---|---|---|---|---|
| $k$ | 1 | 4 | 11 | 26 | 57 | 120 | $\cdots$ |

Dekódolás Hamming-kód esetén:
Ha csak 1 hiba van, akkor a hibavektornak csak egy koordinátája 1, a többi 0, így a szindróma az ellenőrző mátrix valamely oszlopa lesz. Ennek az oszlopnak megfelelő koordinátája hibás az üzenetben.

# Lineáris kódok

## Példa

$n = 7$, $k = 4$

$$\mathbf{H} = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

és

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

$v = (1, 1, 0, 0, 1, 1, 1)^T$ esetén $\mathbf{H}v = (0, 1, 1)^T = s$, ami a $\mathbf{H}$ 2. oszlopa, így a 2. koordináta romlott el, vagyis a küldött kódszó $c = (1, 0, 0, 0, 1, 1, 1)^T$.

# Lineáris kódok

## Megjegyzés

A $[7, 4]$-es Hamming-kódot egy paritásbittel kiegészítve kapjuk a teletextnél használt kódolást.
A $[15, 11]$-es Hamming-kódot egy paritásbittel kiegészítve a műholdas műsorszórásnál (DBS) használják.

## Definíció

A $K \subset \mathbb{F}_q^n$ kód ciklikus, ha minden $(u_1, u_2, \ldots, u_{n-1}, u_n) \in K$ esetén $(u_2, u_3, \ldots, u_n, u_1) \in K$.

## Példa

$K = \{000, 101, 110, 011, 111\}$ bináris kód ciklikus.

## Megjegyzés

Ez nem lineáris kód: $101 + 111 = 010 \notin K$.

# Címkézett gráfok

## Algoritmus(Kruskal)

Egy élsúlyozott gráf esetén az összes csúcsot tartalmazó üres részgráfból kiindulva minden lépésben vegyük hozzá a minimális súlyú olyan élt, amivel nem keletkezik kör.

## Tétel

A Kruskal-algoritmus egy minimális súlyú feszítőerdőt határoz meg. Összefüggő gráf esetén minimális súlyú feszítőfát kapunk.

## Bizonyítás

Elég összefüggő gráfra bizonyítani (Miért?).
Összefüggő gráf esetén az algoritmus nyilván feszítőfát eredményez (Miért?).
Indirekt tfh. van az algoritmus által meghatározott $F$ feszítőfánál kisebb súlyú feszítőfája a gráfnak. Ha több ilyen van, akkor $F'$ legyen az a minimális súlyú, amelyiknek a legtöbb közös éle van $F$-fel. Legyen $e'$ olyan éle $F'$-nek, ami nem éle $F$-nek. (Miért van ilyen?)

# Címkézett gráfok

## Biz.folyt.

Az $F$-hez $e'$ hozzávételével kapott gráfban van egy $K$ kör (Miért?). Ezen kör tetszőleges $e$ élére $w(e) \leq w(e')$ (Miért?). Az $F'$-ből az $e'$ törlésével kapott gráf nem összefüggő (Miért?), és pontosan 2 komponense van (Miért?). A $K$-nak van olyan éle ($e''$), aminek a végpontjai az $F'$-ből az $e'$ törlésével kapott gráf különböző komponenseiben vannak (Miért?). Tekintsük azt a gráfot, amit $F'$-ből az $e'$ törlésével és az $e''$ hozzávételével kapunk. Az így kapott gráf is feszítőfa (Miért?), és $w(e'') < w(e')$ esetén kisebb súlyú, mint $F'$, míg $w(e'') = w(e')$ esetén ugyanakkora súlyú, de több közös éle van $F$-fel. Mindkét esetben ellentmondásra jutottunk.

# A maradékos osztás tétele és következményei

## Tétel (polinomok maradékos osztása)

Legyen $R$ egységelemes integritási tartomány, $f, g \in R[x]$, és tegyük fel, hogy $g$ főegyütthatója egység $R$-ben. Ekkor egyértelműen léteznek olyan $q, r \in R[x]$ polinomok, melyekre $f = qg + r$, ahol $deg(r) < deg(g)$.

## Bizonyítás

Egyértelműség: Tekintsük $f$ két megfelelő előállítását:
$f = qg + r = q^*g + r^*$, amiből:

$$g(q - q^*) = r^* - r.$$

Ha a bal oldal nem $0$, akkor a foka legalább $k$ (Miért?), de a jobb oldal foka legfeljebb $k - 1$ (Miért?), tehát
$0 = g(q - q^*) = r^* - r$, és így
$q = q^*$ és $r = r^*$.

# A maradékos osztás tétele és következményei

## Bizonyítás folyt.

Létezés: $f = 0$ esetén $q = 0$ és $r = 0$ jó választás. $f \neq 0$ esetén $f$ foka szerinti TI: $0 = deg(f) = deg(g)$ esetén $f = f_0 = f_0 \cdot g_0^{-1} g_0 + 0$,
$0 = deg(f) < deg(g)$ esetén $f = 0 \cdot g + f$.
Ha $deg(f) < deg(g)$, akkor $q = 0$ és $r = f$ esetén megfelelő előállítást kapunk.
Legyen $f$ főegyütthatója $f_n$, $g$ főegyütthatója $g_k$. $n \geq k$ esetén legyen $f^*(x) = f(x) - f_n g_k^{-1} g(x) x^{n-k}$.
$deg(f^*) < deg(f)$ (Miért?) miatt $f^*$-ra használhatjuk az indukciós feltevést, vagyis léteznek $q^*, r^* \in R[x]$ polinomok, amikre $f^* = q^* g + r^*$.
$f(x) = f^*(x) + f_n g_k^{-1} g(x) x^{n-k} = q^*(x) g(x) + r^*(x) + f_n g_k^{-1} g(x) x^{n-k} =$
$= (q^*(x) + f_n g_k^{-1} x^{n-k}) g(x) + r^*(x)$,
így $q(x) = q^*(x) + f_n g_k^{-1} x^{n-k}$ és $r(x) = r^*(x)$ jó választás.

## Definíció

$c \in R$ esetén $(x - c) \in R[x]$ a $c$-hez tartozó gyöktényező.

# A maradékos osztás tétele és következményei

## Következmény (gyöktényező leválasztása)

Ha $0 \neq f \in R[x]$, és $c \in R$ gyöke $f$-nek, akkor létezik olyan $q \in R[x]$, amire $f(x) = (x - c)q(x)$.

## Bizonyítás

Osszuk el maradékosan $f$-et $(x - c)$-vel (Miért lehet?):

$$f(x) = q(x)(x - c) + r(x).$$

Mivel $deg(r(x)) < deg(x - c) = 1$, ezért $r$ konstans polinom.
Helyettesítsünk be $c$-t, így azt kapjuk, hogy
$0 = f(c) = q(c)(c - c) + r(c) = r(c)$,
amiből $r = 0$.

# A maradékos osztás tétele és következményei

## Következmény

Az $f \neq 0$ polinomnak legfeljebb $deg(f)$ gyöke van.

## Bizonyítás

$f$ foka szerinti TI:
$deg(f) = 0$-ra igaz az állítás (Miért?).
Ha $deg(f) > 0$, és $f(c) = 0$, akkor $f(x) = (x - c)g(x)$ (Miért?), ahol $deg(g) + 1 = deg(f)$ (Miért?). Ha $d$ gyöke $f$-nek, akkor $d - c = 0$, amiből $d = c$, vagy $d$ gyöke $g$-nek (Miért?). Innen következik az állítás.

# A maradékos osztás tétele és következményei

## Következmény

Ha két, legfeljebb $n$-ed fokú polinomnak $n+1$ különböző helyen ugyanaz a helyettesítési értéke, akkor egyenlőek.

## Bizonyítás

A két polinom különbsége legfeljebb $n$-ed fokú, és $n+1$ gyöke van (Miért?), ezért nullpolinom (Miért?), vagyis a polinomok egyenlőek.

## Következmény

Ha $R$ végtelen, akkor két különböző $R[x]$-beli polinomhoz nem tartozik ugyanaz a polinomfüggvény.

## Bizonyítás

Ellenkező esetben a polinomok különbségének végtelen sok gyöke lenne (Miért?).

# Polinomok felbonthatósága

## Tétel (Schönemann-Eisenstein)

Legyen $f(x) = f_n x^n + f_{n-1}x^{n-1} + \ldots + f_1 x + f_0 \in \mathbb{Z}[x]$, $f_n \neq 0$ legalább elsőfokú primitív polinom. Ha található olyan $p \in \mathbb{Z}$ prím, melyre

- $p \nmid f_n$,
- $p | f_j$, ha $0 \leq j < n$,
- $p^2 \nmid f_0$,

akkor $f$ felbonthatatlan $\mathbb{Z}$ fölött.

## Bizonyítás

Tfh. $f = gh$. Mivel $p$ nem osztja $f$ főegyütthatóját, ezért sem a $g$, sem a $h$ főegyütthatóját nem osztja (Miért?). Legyen $m$ a legkisebb olyan index, amelyre $p \nmid g_m$, és $o$ a legkisebb olyan index, amelyre $p \nmid h_o$. Ha $k = m + o$, akkor

$$p \nmid f_k = \sum_{i+j=k} g_i h_j,$$

mivel $p$ osztja az összeg minden tagját, kivéve azt, amelyben $i = m$ és $j = o$.

# Polinomok felbonthatósága

## Bizonyítás folyt.

Így $m + o = deg(f)$, ahonnan $m = deg(g)$ és $o = deg(h)$. Viszont $m$ és $o$ nem lehet egyszerre pozitív, mert akkor $p^2 | f_0 = g_0 h_0$ teljesülne. Így az egyik polinom konstans, és ha nem lenne egység, akkor $f$ nem lenne primitív.

## Megjegyzés

A feltételben $f_n$ és $f_0$ szerepe felcserélhető.

## Megjegyzés

A tétel nem használható test fölötti polinom irreducibilitásának bizonyítására, mert testben nem léteznek prímek, hiszen minden nem-nulla elem egység.