Bevezetés a számításelméletbe II. :

↳ gráfelmélet

↳ számelmélet

↳ absztrakt algebra

• def G gráf

- Euler-kör : zárt élsorozat, amely G minden élét pontosan egyszer tartalmazza.
- Euler-út : nyílt vagy zárt élsorozat, amely G minden élét pontosan egyszer tartalmazza.

• állítás . G-ben ∃ Euler-kör ⇒ minden pont foka páros

• tétel : G összefüggő (!) gráf

∃ Euler-kör ⇔ minden pont foka páros

bizonyítás : ⇒ ✓

⇐ : v tetszőleges csúcsból induljunk el élismétlés nélkül

ha elakadunk, akkor v-ben vagyunk, és minden élét elhasználtuk.

H : legyen G-ben a leghosszabb körséta, amelyben él nem ismétlődik.

• állítás : H Euler-kör

bizonyítás (indirekt) : tfh. H nem Euler-kör ⇒ ∃ w, aminek van H-beli és H-n kívüli éle is (összefüggő !)

G' : G-ből elhagyva H éleit ⇒ G'-ben is ∀ pont foka páros

H' : zárt élsorozat G'-ben élismétlés nélkül, ami w-ből w-ba megy

w-ből előbb H-n, majd H'-n végigmenve hosszabb utat kapunk ↯

• tétel G összefüggő gráf

∃ Euler-út ⇔ 0 vagy 2 darab páratlan fokú pont van

bizonyítás ⇒ ✓

⇐ : u és w páratlan fokúak

$G' = G + (u, w)$

G'-ben van Euler-kör ⇒ G-ben van Euler-út, az (u,w) elhagyásával Euler-utat kapunk.

• <u>def</u> G gráf

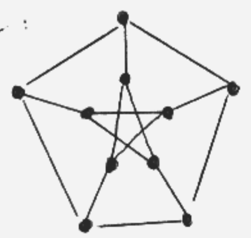
- Hamilton-kör: kör, ami G minden csúcsát tartalmazza.
- Hamilton-út: út, ami G minden csúcsát tartalmazza.

• <u>tétel</u>: G-ben $\exists$ Hamilton-kör $\Rightarrow$ G-ből $\forall$ k pontot kitörölve a gráf max. k komponensre bomlik.

<u>bizonyítás</u>: a Hamilton-kör $\leq k$ darabra esik, és a többi él ezt csak csökkentheti.

• <u>tétel</u>: G-ben $\exists$ Hamilton-út $\Rightarrow$ G-ből $\forall$ k pontot kitörölve a gráf max. k+1 komponensre bomlik.

A Hamilton-körös tétel fordítottjára ellenpélda a Petersen-gráf:



/ Feladat: 4×4-es sakktáblán lóval lépve létezik-e Hamilton kör/út? /

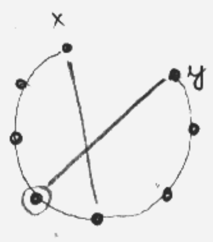
• <u>tétel</u> (Dirac, 1952)
Ha G n csúcsú egyszerű gráf, és $\forall$ pont foka $\geq \frac{n}{2}$, akkor $\exists$ Hamilton-kör.
(az Ore tételből triviálisan következik)

• <u>tétel</u> (Ore)
Ha G n csúcsú egyszerű gráf, és $\forall$ x, y nem szomszédos pontokra teljesül, hogy $d(x)+d(y) \geq n$, akkor a gráfban $\exists$ Hamilton-kör.
(A számítástudomány alapjai könyvben rosszul van kimondva)

<u>bizonyítás</u> Tfh. G n csúcsú ellenpélda, ezek közül az, amelynek a lehető legtöbb éle van.
x, y nem szomszédos csúcsok. A $G+(x,y)$ gráf nem ellenpélda, $\Rightarrow$ ebben van Ham.-kör. $\Rightarrow$ G-ben $\forall$ 2 nemszomszédos pont között vezet Hamilton-út.
Hamilton-út G-ben $x=x_1; x_2; \dots; x_n=y$

$P = \{x_i \mid \{x_1, x_{i+1}\} \in E(G)\}$ (piros)

$K = \{x_i \mid \{x_n, x_i\} \in E(G)\}$ (kék)



$\left.\begin{array}{l} |P| = d(x) \\ |K| = d(y) \end{array}\right\} d(x)+d(y) \geq n$ $\quad P \cap K \neq \emptyset$, és akkor

$y = x_n$ kívételen

Gráfok színezése

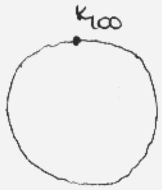
- a szomszédos csúcsok külön-b színűek
- nemcsak síkbarajzolhatóakra, hanem tetszőleges gráfokra is

• **def** a G gráf k színnel színezhető, ha a csúcsai megszínezhetők k színnel úgy, hogy a szomszédos csúcsok különbözőek legyenek
(G egyszerű gráf)

a G kromatikus száma k, ha k színnel színezhető, de $(k-1)$-gyel nem.
jelölése: $\chi(G) = k$

példa

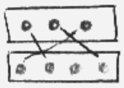
$\chi(G)=3$



100 csúcsú teljes gráf
$\chi(K_{100}) = 100$

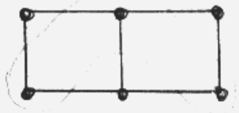
↳ Melyek azok a gráfok, melyeknek a kromatikus száma $\chi(G)$ ...

$\chi(G)=1 \Rightarrow$ nincsenek benne élek pl: 

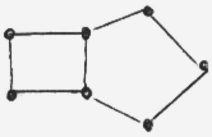
$\chi(G)=2 \Rightarrow$ két pontosztály van: kék & zöld 

• **def** G páros gráf, ha csúcsai két osztályba sorolhatók (A és B) úgy, hogy $\forall$ él A-beli és B-beli csúcsot köt össze.
jel: $G(A; B; E)$

példa:



páros gráf

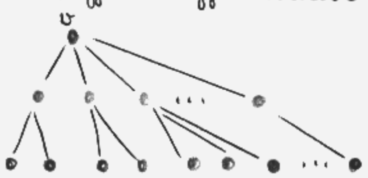


nem páros

• **tétel**: G páros $\Longleftrightarrow \nexists$ páratlan hosszú kör.

bizonyítás $\Rightarrow$ ✓

$\Leftarrow$: vegyünk egy v csúcsot – szomszédai zöldek, azoké ismét kékek, stb.

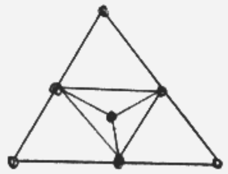


vegyünk két pontot, amelyek azonos színűek

keressük meg az első közös ősüket – ez páros sok; köztük ezért nem futhat él

- de ez csak összefüggő gráfokra igaz; arra a komponensre, amelyben benne van v.
- nem öf gráfra: minden komponensen elvégezzük.

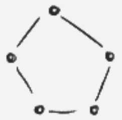
példa



4 színnel könnyen színezhető, 3-mal nem lehet
oka: a középső 4 pont teljes gráfot (részgráfot) alkot

- **def**: maximális klikkméret / jel: $\omega(G)$ /
  $\omega(G)=k$, ha $\exists$ G-ben k db csúcs, hogy bármelyik kettő szomszédos, de $(k+1)$ nem található.
- **állítás** $\omega(G) \leq \chi(G)$
  bizonyítás ha $\omega(G)=k$, akkor legalább k szín kell

példa

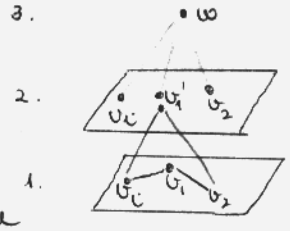


$\omega(C_5) = 2$
$\chi(C_5) = 3$

van-e olyan gráf, amelyre: $\omega(G)+2 = \chi(G)$
lehet-e tetszőlegesen nagy a különbség a max. klikkméret és a krom. szám között?
↓

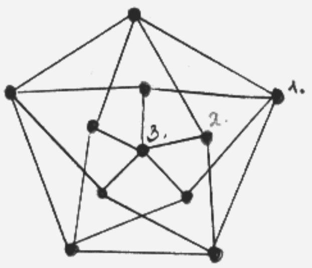
- **tétel** $\forall k \geq 3$ $\exists G_k$, amire $\omega(G_k)=2$ és $\chi(G_k)=k$ (Mycielski-konstrukció)
  bizonyítás: G_3:

G_{k+1}-et előállíthatjuk G_k-ból, ha G_k már ismert



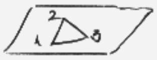
↳ 1. emelet: G_k csúcsai $\{v_1, v_2, \ldots, v_n\}$
↳ 2. emelet: $v_1', v_2', v_3', \ldots, v_n'$
v_i' csúcsot összekötjük v_i elsőemeleti szomszédaival
↳ 3. emelet: egyetlen csúcs van: w, amelyet összekötünk minden v_i'-vel

példa. $G_3 \to G_4$



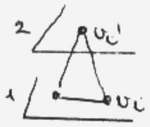
→ bizonyítás: nincs benne háromszög (indirekt biz.) → $\omega(G_k)=2$

a)



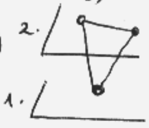
↯, nem így vettük fel!

b)



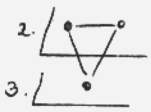
↯

c)



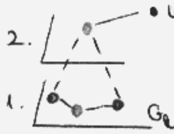
2. em-en nem kötünk össze pontokat! ↯

d)



↯ ↓ uaz

→ bizonyítás: G_k k színnel színezhető
G_{k-1}-re visszavezetve:



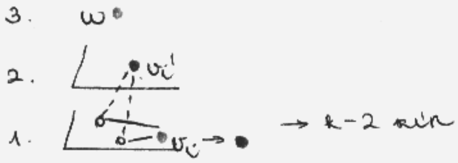
• w: külön színt kap
az 1-et átmásoljuk 2. em-re
G_{k-1} $\chi(G_{k-1})=k-1$

biz. folyt.: G_k nem színezhető $(k-1)$-gyel

indirekt bizonyítás (ha G_k színezhető lenne $(k-1)$-gyel, akkor G_{k-1} színezhető lenne $(k-2)$ színnel ↯)

tfh. $(k-1)$-gyel van kiszínezve

legyen w zöld színű: ha találunk az első emeleten zöld színűt, akkor azt átfestjük vmilyen másikra, pl. olyanra, amilyen v_i'. Mivel v_i' kék, ezért v_i is lehet kék, mert v_i' v_i szomszédaival van összekötve



$\omega(G) \le \chi(G) \le ?$

triviális: $\chi(G) \le n$

mohó színezés: vesszük a csúcsok vmilyen sorrendjét

v_i színe: a legkisebb sorszámú szín, amilyen szomszédja még nincs.

1 2 3 4 ...

• állítás: mohó színezés $\le \Delta(G) + 1$ színt használ jel: $\Delta(G)$ max. fokszám

bizonyítás: $\Delta(G) + 2$-edik színre nem lehet szükség

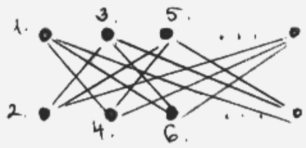
v_i-nek max. $\Delta(G)$ db szomszédja van, az max. $\Delta(G)$ db foglalt színt jelent, tehát a $+1$-edikkel mindig lehet színezni.

példa:

$\chi = 2$

$\Delta(G) = 6$ → rossz becslés

példa:



két pontosztály van, n–n db ponttal, majdnem minden ponttal összekötjük, kivéve azzal, amelyik szemben van v_i-vel

ha ebben a sorrendben halad a mohó algoritmus, akkor n színt használ, pedig $\chi(G) = 2$.

Lehet-e jobb a becslés? Nem, mert tudunk olyat mutatni, hogy $\Delta = n-1$ és $\chi = n$

példa 1.)

K_n $\Delta = n-1$
$\chi = n$

2.)

$\Delta = 2$
$\chi = 3$

• tétel (Brooks): ha G összefüggő, nem teljes gráf (K_n) és nem páratlan kör (C_{2k+1}) $\Rightarrow \chi(G) \le \Delta(G)$

• négyszíntétel: G síkbarajzolható $\Rightarrow \chi(G) \le 4$ (1977, Appel-Haken)
• ötszíntétel: G síkbarajzolható $\Rightarrow \chi(G) \le 5$ (Heawood) G egyszerű

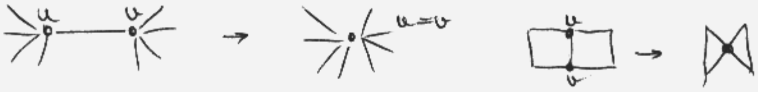
→ Lemma: G síkbarajzolható, egyszerű $\Rightarrow$ min. fokszám ≤ 5 ($\delta(G) \le 5$)

bizonyítás indirekt: ha minden pont foka ≥ 6

$6n \le \sum d_i = 2e$

$3n \le e \le 3n-6$ ↯

→ összehúzás

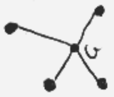


síkbarajzolható → síkbarajzolható marad

ötszíntétel bizonyítása: teljes indukcióval

tudom, hogy $\le k$ csúcsúra igaz $\Rightarrow$ $(k+1)$ csúcsúra is

I. eset: $\exists$ v csúcs, hogy $d(v) \le 4$ → kitöröljük a gráfból; így kapjuk G'-t, amit pedig tudjuk, hogy kiszínezhető 5 színnel, és 4 szomszédja van, v az 5. színű lesz

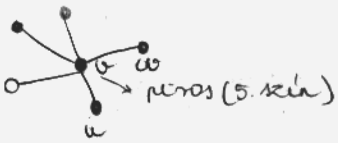


II. eset: $\exists$ v csúcs, hogy $d(v)=5$

szomszédai között $\exists 2$, amelyek nem szomszédosak (u, w)

/különben K_6 volna G-ben/

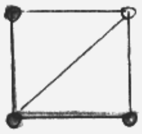
húzzuk össze $\left.\begin{matrix} u\text{-t és } v\text{-t} \\ w\text{-t és } v\text{-t} \end{matrix}\right\}$ → G' az 5 színű lehet, majd visszavisszük G'-t G-be. Legyen u, v, w is kék → v-t átfesthetjük az 5. színre (piros)



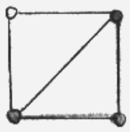
3. előadás febr. 25.

• Perfekt gráfok: $/\omega(G) \le \chi(G)/$

• def: G perfekt, ha $\omega(G) = \chi(G)$; továbbá G minden H feszített részgráfjára is $\chi(H) = \omega(H)$.

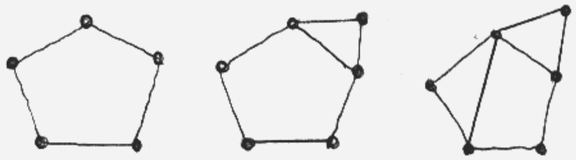


feszített



nem feszített

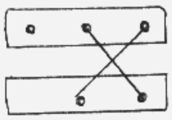
példák:



$\chi(G)=3$	$\chi=3$	
$\omega=2$	$\omega=3$	perfekt
nem perfekt	nem perfekt	

• **állítás**: minden páros gráf perfekt

bizonyítás:



kiválasztunk egy feszített részgráfot:

– ha üres: $\chi=1$, $\omega=1$ (nincsenek élek)

– nem üres: van él a kiv. csúcsok között → $\chi=2$, $\omega=2$

Nem perfekt gráfok: C_{2k+1} $(k\geq 2)$ ötszög, hétszög, kilencszög ... ; illetve ezek komplementerei sem perfekt gráfok $\overline{C}_{2k+1}$ $(k\geq 2)$

• **állítás**: $\chi(\overline{C}_{2k+1}) > \omega(\overline{C}_{2k+1})$

bizonyítás: a csúcsok a közvetlen szomszédokkal nincsenek csak összekötve

max. két csúcs lehet azonos színű: ha egy csúcs piros, akkor csak valamelyik szomszédját színezhetjük szintén pirosra → $\chi(\overline{C}_{2k+1}) \geq k+1$

$\omega(\overline{C}_{2k+1}) \leq k$, mivel ha $(k+1)$-et választanánk ki, már lenne két egymás melletti csúcs a "körben".

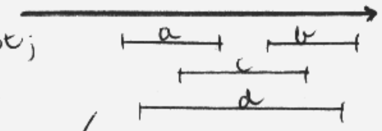
• **állítás**: G perfekt $\Rightarrow$ nem tartalmaz C_{2k+1}-et és $\overline{C}_{2k+1}$-et $(k\geq 2)$ feszített részgráfként

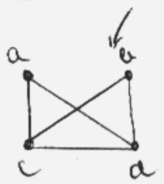
• **Berge sejtés, 1960**: $\Leftarrow$ (Erős perfekt gráf sejtés)
↳ **tétel** (2002 nyara)

• **Gyenge perfekt gráf sejtés**: G perfekt $\Rightarrow$ $\overline{G}$ perfekt
(bizonyította: 1972, Lovász) következik az előzőből

Intervallumgráfok

egy számegyenesen kiválasztunk néhány intervallumot; ezek lesznek a csúcsok; két csúcsot akkor kötünk össze, ha metszik egymást az intervallumok





• **def**: csúcsok: $I_1, I_2, \dots, I_n$ (zárt) intervallumok
él: I_i, I_j: $I_i \cap I_j \neq \emptyset \leftrightarrow v_i — v_j$

• tétel: $\forall$ intervallum-gráf perfekt

bizonyítás: mohó algoritmussal ① ② ③ ... ⓚ

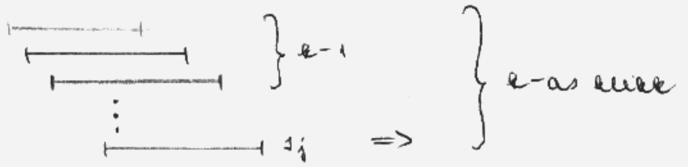
a csúcsok sorrendje: bal oldali végpont szerinti növekvő sorrend

→ mohó k színt használt

akarjuk bizonyítani: gráfban van k-as klikk } $\Rightarrow \chi = \omega = k$ következne

I_j: ezt olyan, amikor ⓚ színt használtunk

a többit nem használtuk, ezért van $(k-1)$ db intervallum, ami metszi, és balra van tőle:



tehát azt tudjuk, hogy: G intervallum gráf $\Rightarrow \chi(G) = \omega(G)$

illetve: intervallum gráf $\forall$ feszített részgráfja is intervallum-gráf (az intervallumok közül választunk ki intervallum~~gráf~~okat)

gyakorlati jelentősége az intervallumgráfoknak: pl. a kromatikus szám megmutatja, hogy legkevesebb hány processzor tudja elvégezni a feladatot.

Élszínezés

→ élkromatikus szám

jele: $\chi_e(K_4) = 3$

• def: $\chi_e(G) = k$, ha G élei k színnel kiszínezhetők úgy, hogy a szomszédos élek külö'b színűek legyenek; de $(k-1)$-gyel nem.

• állítás: $\chi_e(G) \geq \Delta(G)$

bizonyítás: az egy csúcsból kiinduló éleknek külö'beknek kell lenniük

• Vizing-tétel: G egyszerű gráf $\Rightarrow \chi_e(G) \leq \Delta(G) + 1$ $(\neg B)$

$\Downarrow$

egy egyszerű gráfot $\Delta(G)$ vagy $\Delta(G)+1$ színnel színezhetünk ki, de hogy a kettő közül melyik, azt nehéz eldönteni

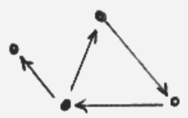
• példa:

$\Delta = 4$

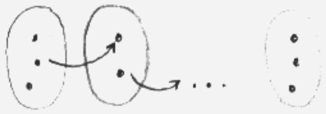
$\chi_e = 6$

→ nem egyszerű gráfoknál nagyobb is előfordulhat

Irányított gráfok



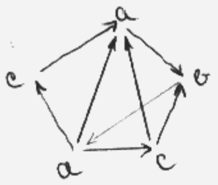
színezési feladat: részhalmazokra való bontás

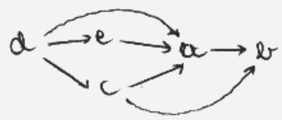


irányított gráfoknál: emeletekre bontás

minden nyíl balról jobbra mutat

példa:





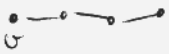
ha behúzzuk b-ből d-be menő élet, akkor nem adható meg; oka: irányított kör (b → d → c → b)

• tétel: ha $\vec{G}$ irányított gráf emeletekre bontható $\Longleftrightarrow$ nincs benne irányított kör

bizonyítás: ⇒ ✓

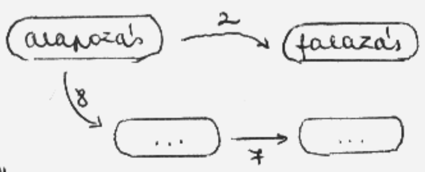
⇐ Lemma: ha aciklikus (nincs benne irányított kör) → ∃ nyelő

bizonyítása: v-ből indulunk ki, mivel nincs benne kör, ezért valahol elakadunk; ez a csúcs nyelő



↳ kiválasztjuk a nyelőket, ők alkotják az utolsó osztályt (emeletet); majd kitöröljük őket a gráfból, és folytatjuk az algoritmust: mindig kiválasztjuk a nyelőket az aktuális gráfból. Ezt mindig megtehetjük, hiszen eredetileg sem volt benne kör.

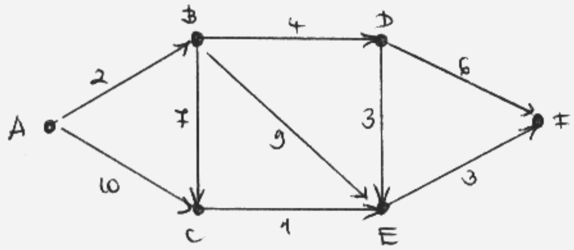
• gyakorlati példa: építkezés részfeladatai



feladat: a lehető legrövidebb legyen a munkafolyamat

⇓

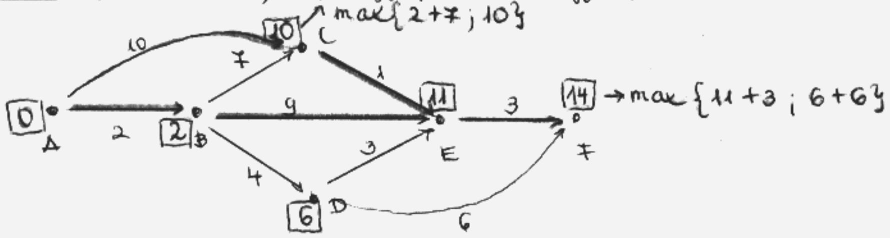
$\vec{G}$ aciklikus; emeletre bontható



egy nyelő van: F

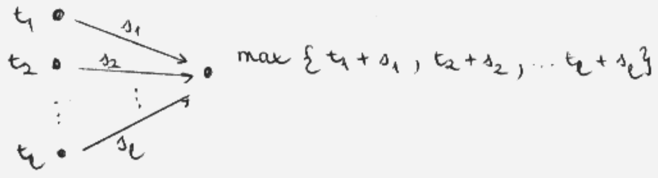
egy forrás van: A

PERT-módszer: feltételezi, hogy egy forrás és egy nyelő van



I.: emeletekre bontás (jobbról balra)

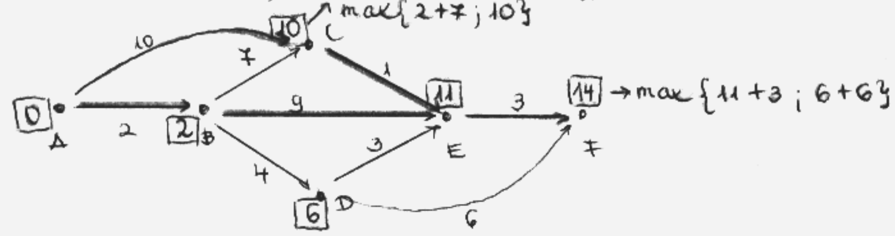
II: kezdési idők (balról jobbra)



III kritikus részfeladatok (jobbról balra)

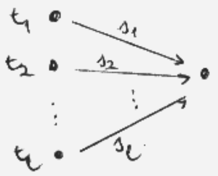
(olyan munkák, amelyek nem csúszhatnak) ⟶ -val jelölve

PERT-módszer: feltételezi, hogy egy forrás és egy nyelő van



I. emeletekre vonás (jobbról balra)

II. kezdési idők (balról jobbra)



$\max\{t_1+s_1, t_2+s_2, \dots, t_l+s_l\}$

III. kritikus részfeladatok (jobbról balra)

(olyan munkák, amelyek nem várhatnak) ⟶-val jelölve

4. előadás
márc. 4.

Párosítások

- **def:** $M \subset E(G)$ párosítás (vagy független élhalmaz), ha semelyik kettő M-beli élnek nincs közös végpontja.

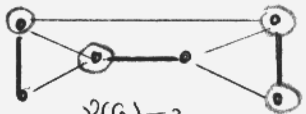
↳ Az M párosítás lefedi/lefogja a végpontjainak halmazát.

↳ M teljes párosítás, ha párosítás $\wedge$ minden csúcsot lefed.

↳ $\nu(G)$: a legnagyobb élszámú párosítás élszáma.
(„független élek maximális száma")

↳ $X \subseteq V(G)$ lefogó ponthalmaz, ha $\forall e \in E(G)$-re e legalább egyik végpontja X-beli.

↳ $\tau(G)$ lehető legkisebb lefogó ponthalmaz mérete
(„lefogó pontok min. száma")



$\nu(G)=3$
$\tau(G)=4$

- **állítás:**

$$\left.\begin{array}{l} M \text{ párosítás} \\ X \text{ lefogó ponthalmaz} \end{array}\right\} \Rightarrow |M| \le |X| \iff \nu(G) \le \tau(G)$$

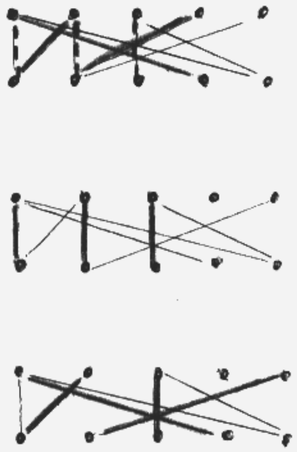
bizonyítás:
- a párosítás minden egyes élét különböző pont fogja le
- esetleg még vannak további pontjai is a lefogó ponthalmaznak

$\nu = 1$
$\tau = 2$

Párosítás páros gráfokban:

– algoritmus (magyar módszer)

- független éleket veszünk fel, amíg lehet
- javítóút keresése és növelés, amíg lehet



javítóút egy adott párosításra (valóban út)

- az egyik halmazból nem lefogott pontból indul
- minden második éle ~~lefogott~~ párosításbeli él
- a másik halmazba nem lefogott pontba ér.

alternáló út egy adott párosításra

- nincs több javítóút => stop!

- tétel: ha az algoritmus leáll => max. méretű párosítás jött létre

bizonyítás: a k élű eredményhez keresünk k pontú lefogó ponthalmazt.

~ L, F: a páros gráf két ponthalmaza

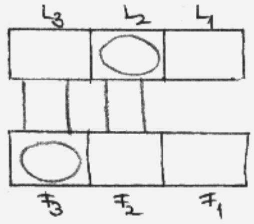
~ L_1, F_1: a párosítatlan pontok

~ L_2: F_1-ből alternáló úttal elérhető

(az algoritmus leállása miatt $L_1 \cap L_2 = \emptyset$)

~ F_2: L_2 csúcsainak párosításbeli párjai

~ L_3, F_3: a többi pont



állítás: G-ben nincs $(F_1 \cup F_2)$-ből $(L_1 \cup L_3)$-ba él

=> $L_2 \cup F_3$ lefogó és akkora, mint M.

↳ bizonyítás: $L_1 - F_1$: javítóút volna ↯

$L_3 - F_1$: a pont elérhető lenne alternáló úton F_1-ből ↯

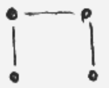
$L_1 - F_2$: létezne $F_1 - L_2 - F_2 - L_1$ út, ami javítóút ↯

$L_3 - F_2$: létezne $F_1 - L_2 - F_2 - L_3$ alternáló út ↯

- tétel (Kőnig): G páros $\Longrightarrow$ $\nu(G) = \tau(G)$

bizonyítás: ld. fent

példa:



$\nu = 2$

$\tau = 2$

$\nu = 2$

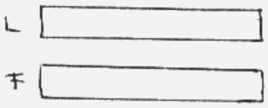
$\tau = 2$

=> nem páros gráfban is igaz lehet, hogy $\nu(G) = \tau(G)$

• **tétel** (Hall-tétel)

G(F;L;E) /páros gráf/ :

∃ F-et lefedő párosítás $\iff \underbrace{\forall X\subseteq F : |N(X)|\ge |X|}_{\text{Hall-feltétel}}$



$X\subseteq F$: $N(X)$: X-beliek szomszédai a gráfban

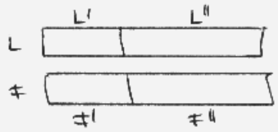
bizonyítás:

$\Rightarrow$ ✓ (triviális)

$\Leftarrow$: ∃ F-et lefedő párosítás $\iff \nu(G)\ge |F| \overset{\text{König}}{\iff} \tau(G)\ge |F|$

indirekt: tfh. $F'\cup L'$ lefogó ponthalmaz $\land$ $|F'\cup L'|<|F|$

$$\left.\begin{array}{l}|F'|+|L'|<|F|\\ |F'|+|F''|=|F|\end{array}\right\}\Rightarrow |L'|<|F''|$$



$N(F'')\subseteq L' \Rightarrow |N(F'')|<|L'|$ ↯ (Hall-feltétel)

$|L'|<|F''|$

• **tétel** (Frobenius)

G(F;L;E) páros gráf :

∃ teljes párosítás $\iff \begin{cases}|F|=|L|\\ \forall X\subseteq F : \ |N(X)|\ge |X|\end{cases}$

bizonyítás: $\Rightarrow$ ✓ (triviális)

$\Leftarrow$: ∃ F-et fedő párosítás, ez teljes, mert $|F|=|L|$

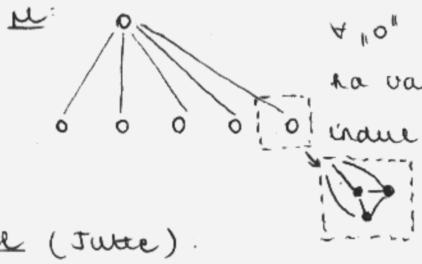
Tetszőleges gráfok

jelölések: H: gráf

Cp(H) db páratlan csúcsú komponense van H-nak

G − X : G gráfból az X csúcsokat a belőlük induló élekkel elhagyjuk.

pl:

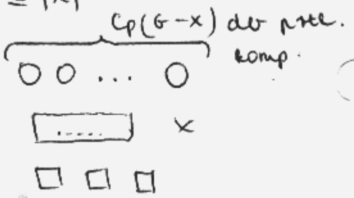


∀ „o" egy △-et jelöl, az élek minden △-beli csúccsal össze vannak kötve. Ha van benne teljes párosítás, akkor az alsó △-ekből indul 1-1 él. De fenn csak 3 csúcs van.

• **tétel** (Tutte).

G-ben ∃ teljes párosítás $\iff \forall X\subseteq V(G) : Cp(G-X)\le |X|$

bizonyítás:



$\Leftarrow$ (nehéz biz.)

$\Rightarrow$: ha van teljes párosítás, akkor

a páratlanokból van ~~lefedő~~ él X-be (párosításbeli) : $Cp(G-X)\le |X|$

• **def** ↳ egy ponthalmaz független, ha semelyik két pontja között nincs él.
↳ egy élhalmaz lefogó, ha minden csúcsból indul ki közülük valamelyik él a gráfban.

	független (max)	lefogó (min)
élek	ν	ρ
pontok	α	τ

• **állítás**: $\alpha \leq \rho$

• **tétel**: (Gallai)

I. minden hurokmentes G gráfra: $\alpha(G) + \tau(G) = n$

bizonyítás: X független ponthalmaz $\iff$ $V(G) - X$ lefogó ponthalmaz

$$\left.\begin{array}{l} \hookrightarrow \alpha(G) = k \Rightarrow \tau(G) \leq n-k \Rightarrow \alpha(G) + \tau(G) \leq n \\ \hookrightarrow \tau(G) = k \Rightarrow \alpha(G) \geq n-k \Rightarrow \alpha(G) + \tau(G) \geq n \end{array}\right\} \Rightarrow \alpha(G) + \tau(G) = n$$

II. $\nu(G) + \rho(G) = n$, ha G-ben nincs izolált pont.

5. előadás
márc. 11.

Hálózati folyamok

• **def**:

$$\left.\begin{array}{l} \vec{G}(V, \vec{E}) \\ s, t \in V: s \text{ termelő}, t: \text{fogyasztó} \\ c: E \to \mathbb{R}^{+,0}: \text{kapacitásfgv.} \end{array}\right\} (G; s; t; c): \text{hálózat}$$

a kapacitásokat ált-ban ()-ben írjuk az élekre, elé pedig az $f(e)$-t írjuk.

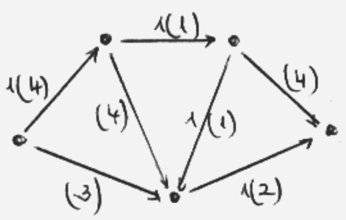
• **def**: folyam: $f: E \to \mathbb{R}^{+,0}$

(1): $\forall e \in E$: $f(e) \leq c(e)$

(2): $\forall v \in V \setminus \{s, t\}$: $\sum \{f(e) \mid \xrightarrow{e} \bullet\, v\} = \sum \{f(e) \mid v \bullet \xrightarrow{e}\}$

• **def** folyamérték $m_f = \sum \{f(e) \mid s \xrightarrow{e}\} - \sum \{f(e) \mid s \xleftarrow{e}\} =$

$$= \sum \{f(e) \mid \xrightarrow{e} \bullet\, t\} - \sum \{f(e) \mid \xleftarrow{e} \bullet\, t\}$$



Maximális értékű folyam

- adott: $(\vec{G}; s; t; c)$
- def: (s,t)-vágás: $X \subseteq V$
  $s \in X$, $t \notin X$

  Azon élek halmaza, amelyek X és $V-X$ között futnak. jele: C

- def: vágás értéke
  $c(C) = \sum \{ c(e) \mid X \xrightarrow{e} V-X \}$ jele: $c(C)$

- állítás: $m_f \le c(C)$
  $\Updownarrow$
  maximális folyam értéke $\le$ minimális vágás értéke

- algoritmus max. folyam keresésére:
  (1): tetszőleges folyam (pl. $\equiv 0$ folyam)
  (2): javítás, amíg lehet
  (3): STOP, ha nem lehet már javítani

↳ javítás: H_f segédgráf: $V(H_f) = V(G)$

(1.) $\vec{xy} \in E(H_f)$, ha $f(\vec{xy}) < c(\vec{xy})$

(2.) $\vec{yx} \in E(H_f)$, ha $f(\vec{xy}) > 0$

↳ javítóút: H_f-ben $s \rightsquigarrow t$ irányított út
legyen p egy javítóút:

$$d = \min \left\{ c(e_i) - f(e_i) \mid e_i \in p \wedge e_i \text{ (1)-es} \right\} \cup \left\{ f(e) \mid e_i \in p \wedge e_i \text{ (2)-es} \right\}$$

$$\underset{s}{\bullet} \xrightarrow{e_1} \dots \xrightarrow{e_n} \underset{t}{\bullet}$$

ha e_i (1)-es típusú: $f(e_i) + d$

ha e_i (2)-es típusú: $f(e_i) - d$

↳ a javítás jó

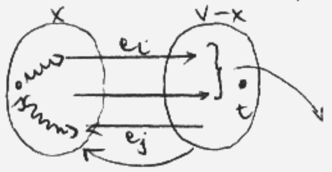
$$\xrightarrow[+d]{(1)} \underset{v}{\bullet} \xrightarrow[+d]{(1)} \qquad \xrightarrow[+d]{(1)} \underset{v}{\bullet} \xleftarrow[-d]{(2)} \quad ✓ \quad \dots \text{stb.}$$

• **állítás:** ha H_f-ben nincs javítóút, akkor a folyam maximális.

bizonyítás: mutassunk ugyanolyan értékű vágást!

$X = \{ v \in V \mid s\text{-ből } v\text{-be van irányított út a segédgráfban} \}$

$t \notin X$; $s \in X$



e_i : $f(e_i) = c(e_i)$

e_j : $f(e_j) = 0$

$c(C) = m_f$

• **tétel:** max folyamérték = min. vágás értéke

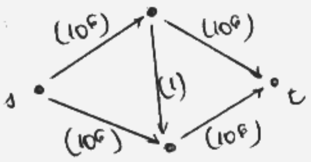
(Ford, Fulkerson tétele)

bizonyítás: algoritmus

• **tétel** (Edmonds, Karp)

Ha H_f-ben mindig a legrövidebb javítóutat veszem s-ből t-be, akkor véges sok lépésben leáll az algoritmus, sőt, polinomiális az algoritmus. ($O(n^5)$)

példa:



az algoritmussal: ↗↓↗ ↘↑↘ ... ha egy fajtája, akkor kétmillió lépés lenne a kettő helyett (nem a legrövidebbet választja)

feladat: program → van-e egy gráfban Hamilton-kör?

ha megfogalmazzuk a csúcsokat, vesszük az összes lehetséges sorrendjüket, ($n!$); véges sok lépés után megkaphatjuk a megoldást – de milyen gyors? → osztályozás: (input mérete: n)

$$\left.\begin{array}{l} n \to c \cdot n \\ n \to c \cdot n^2 \\ \vdots \end{array}\right\} \text{polinomiális algoritmus}$$

nem polinomiális: $n \to n!$

$n \to 2^n$

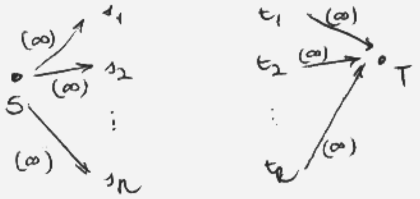
• **egészértékűségi lemma:** ha $\forall$ élen a kapacitás egész $\Rightarrow$ $\exists$ olyan maximális folyam, ami minden élen egész értékű.

bizonyítás: csupa 0-ból indul, és mindig egész számmal változtat

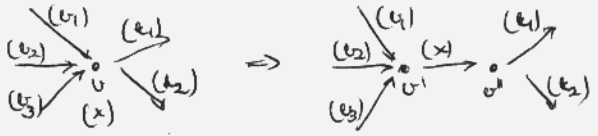
A folyamprobléma általánosításai

(1) több termelő és több fogyasztó

algoritmus: két fiktív pontot veszünk fel, (S, T); az S-ből s-ekbe ill. t-kből T-be ∞-nek választjuk a kapacitásokat



(2) csúcsoknak is van kapacitásuk



(3) irányítatlan gráf

két irányított éllel helyettesítjük:

(4) alsó korlát is van az éleken – szintén megoldható

(5) többtermékes folyamprobléma (pl. több termék szállítása)

nem vezethető vissza az algoritmusra – sejtés: nincs algoritmus

6. előadás
márc. 18.

$\vec{G}$ hálózat

- **def:** $X \subseteq E(\vec{G})$ lefogja az $s \to t$ irányított utakat, ha $\forall$ $s \to t$ irányított út legalább egy X-beli élet tartalmaz.

- **tétel** (Menger)

  $s \to t$ éldiszjunkt irányított utak maximális száma $=$ $s \to t$ irányított utakat lefogó élek min. száma

  bizonyítás:

  $$\left.\begin{array}{l} x \text{ db irányított } s \to t \text{ út} \\ y \text{ db él lefogja az összeset} \end{array}\right\} \Rightarrow x \le y$$

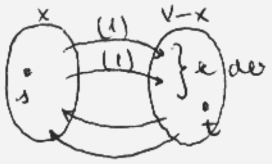
  hátra van: példa „$=$"-re

  A hálózathoz a $c \equiv 1$ kapacitásfgv. tartozik

  $\max m_f = k = \min c(C)$

  ↳ k értékű folyam $\xRightarrow[\text{lemma}]{\text{egészértékűségi}}$ 1-es értékű élekből éppen kijön k db, páronként éldiszjunkt $s \to t$ út

  ↳ k értékű vágás $(s \to t)$:



ez lefogja az $s \to t$ utakat

Minimax-tételek

$\omega(G) \le \chi(G)$ intervallumgráfokra =

$\nu(G) \le \tau(G)$ páros gráfokra =

$m_f \le c(C)$

$x \le y$

G irányítatlan gráf

• tétel (Menger) I.

$s-t$ éldiszjunkt irányítatlan utak maximális száma = $s-t$ irányítatlan utakat lefogó élek min. száma

bizonyítás max $\le$ min egyértelmű

nadítev → példát mutatunk „="-re

az irányítatlan éleket egy oda-vissza mutató irányított élre cseréljük le → $\vec{G}$

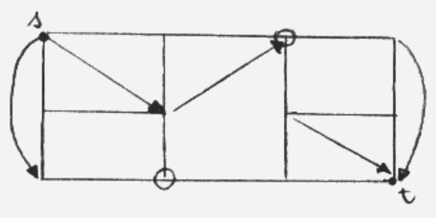
↳ $\vec{G}$-ben van k db irányított él, ami lefogja az $s \to t$ utakat ⇒ G-beli megfelelő élek lefogják az összes $s-t$ utat.

↳ $\vec{G}$-ben van k db, páronként éldiszjunkt út

probléma: megoldás:

minden probléma feloldható így

pontdiszjunkt $s-t$ utat keresünk.



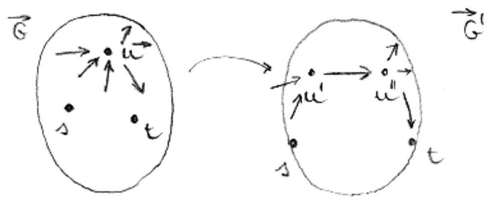
minden út átmegy a kijelölt csúcsok valamelyikén

• def: $Y \subseteq V(\vec{G})$ lefogja az $s \to t$ utakat, ha minden $s \to t$ út átmegy valamelyik ponton és $\{s;t\} \cap Y = \emptyset$

• tétel (Menger III.) (s és t nem szomszédosak, nincs közvetlen él)

$s \to t$ páronként p.diszjunkt irányított utak max száma = $s \to t$ utakat lefogó pontok min. száma bizonyítás: max{} ≤ min{} egyértelműen igaz

nehezebb: példa „="-re



minden $u \notin \{s,t\}$-re

majd alkalmazzuk erre a Menger I-et: $\vec{G}'$-ben k db éldiszjunkt $s \to t$ út ⇒ megfelelő utak $\vec{G}$-ben; a pontok diszjunktak

probléma: k db $u' \to u''$ jellegű él kell $\vec{G}'$-ben

megoldás: 

⇒ $\vec{G}$-ben k db pont, ami lefogja az $s \to t$ utakat

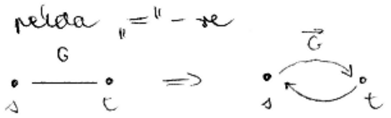
• tétel (Menger IV.)

G irányítatlan, s és t nem szomszédosak

s–t pontdiszjunkt irányítatlan utak max száma = s–t irányítatlan utat lefogó pontok min. száma

bizonyítás: max{} ≤ min{} nyilvánvaló

példa „="-re



$\vec{G}$-ben k db $s \to t$ pontdiszjunkt irányított út → G-ben k db irányítatlan pontdiszjunkt út

k db pont, ami lefogó csúcs $\vec{G}$-ben → G-ben k db csúcs, ami lefog

---

• def: G k-élösszefüggő, ha bármely legfeljebb $(k-1)$ élet kitörölve G összefüggő marad.

• def: G k-szorosan pontösszefüggő, ha bármely legfeljebb $(k-1)$ pontot kitörölve összefüggő marad, és legalább $(k+1)$ csúcsú.

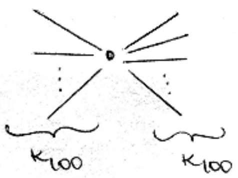
⇓

hálózat megbízhatósága

általában

- k élösszefüggő $\Rightarrow$ $(k-1)$ élösszefüggő
- k öf $\Rightarrow$ $(k-1)$ öf is
- k öf $\Rightarrow$ k élösszefüggő $\Rightarrow$ biz: $(k-1)$ csúcs kitörlésével együtt legalább $(k-1)$ élet is törlünk, a feltétel miatt ez összefüggő. Tehát $1, 2, \dots, (k-1)$ él kitörlésével öf marad $\Rightarrow$ k élösszefüggő.

Fordítva nem igaz, erre példa:



nem 2 öf.
100 élöf.

- tétel (Menger V.)

G k élösszefüggő $\Longleftrightarrow$ $\forall$ 2 pontja között $\exists$ k db éldiszjunkt út

bizonyítás:

$\Leftarrow$: ha van k db éldiszjunkt út; akkor a max $(k-1)$ él kitörlésével max $(k-1)$ utat "ronthatunk" el, így még mindig marad út $\forall$ két pontja között

$\Rightarrow$: $s-t$ éldiszjunkt utak max száma $\geq k$

$\Updownarrow$ Menger

$s-t$ utakat lefogó élek min. száma $\geq k$

$\Uparrow$

G k élösszefüggő

- tétel (Menger VI.)

G k összefüggő $\Longleftrightarrow$ $\forall$ 2 pontja között $\exists$ k db pontdiszjunkt, és legalább $(k+1)$ csúcsa van.

bizonyítás

$\Leftarrow$ a legfeljebb $(k-1)$ pont kitörlése legfeljebb $(k-1)$ pontdiszjunkt utat "rongál meg".

$\Rightarrow$: $s-t$ pontdiszjunkt irányítatlan utak max száma $\geq k$

$\Updownarrow$ Menger

$s-t$ utat lefogó pontok min. száma $\geq k$

$\Uparrow$

G k összefüggő

ez csak akkor igaz, ha s és t nem szomszédosak

ha szomszédosak: elhagyjuk a köztük lévő élet (G') s — t $\Rightarrow$ s t

G' $(k-1)$ öf $\Rightarrow$ G'-ben van $(k-1)$ db $s-t$ út $\Rightarrow$ G-ben van k db $s-t$ út

7. előadás • <u>tétel</u>

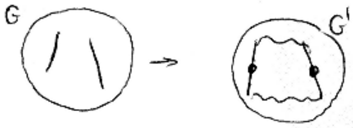
márc. 25.

G gráf 2-öf $\iff$ $\forall$ 2 pontja között $\exists$ 2 db pontdiszjunkt út $\iff$ $\forall$ 2 ponton át vezet kör $\iff$ $\forall$ 2 élen át vezet kör

<u>az utolsó következtetés bizonyítása</u>:

$\Leftarrow$ triviális

$\Rightarrow$: az éleket felosztjuk egy-egy ponttal:

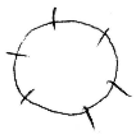


ekkor már alkalmazhatjuk azt, hogy $\forall$ 2 ponton át vezet kör.

• <u>tétel (Dirac)</u>:

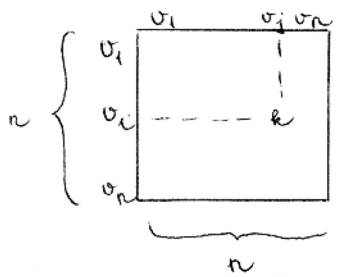
G gráf k-öf $\Rightarrow$ bármely k ponton át vezet kör

(a tétel visszafelé nem igaz $k \geq 3$-ra!) $\rightarrow$ <u>ell</u>:



Gráfok és mátrixok kapcsolata

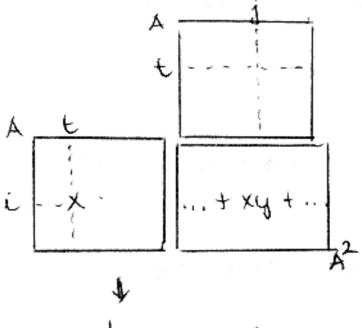
gráf leírása mátrixszal:



• <u>def</u>: szomszédossági mátrix

$V(G)=\{v_1, v_2, \dots, v_n\} \rightarrow A(G)$ $n \times n$-es

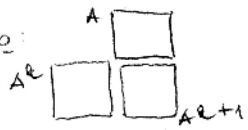
$$a_{ij}=\begin{cases} k, & \text{ha } v_i, v_j \text{ között } k \text{ él fut } (i \neq j) \\ 0, & \text{ha } v_i, v_j \text{ nem szomszédosak } (i \neq j) \\ l, & \text{ha } i=j \text{ és } v_i\text{-nél } l \text{ db hurokél van.} \end{cases}$$



• <u>állítás</u>: $C=A^k$

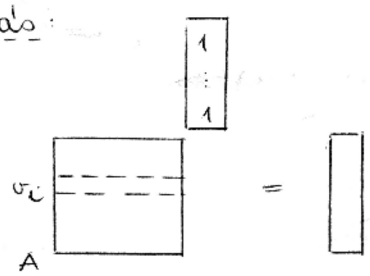
c_{ij} = G-ben v_i-ből v_j-be hány k élű élsorozat található.

<u>bizonyítás</u>:



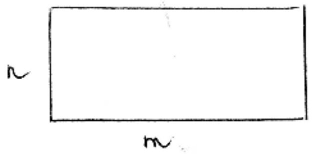
k-indukció

• <u>állítás</u>: G k-reguláris (minden pont foka k) $\Rightarrow$ A(G) k sajátértéke bizonyítás:



← A oszlopainak összegét kapjuk, azonban az összeg éppen az adott v_i sorának, v_i-nek fokszáma.

• def: illeszkedési mátrix



$$\left.\begin{array}{l} \vec{G}:\ V(\vec{G}) = \{v_1, v_2, \dots, v_n\} \\ \phantom{\vec{G}:\ } E(\vec{G}) = \{e_1, e_2, \dots, e_m\} \end{array}\right\} \Rightarrow B(\vec{G})$$

$$b_{ij} = \begin{cases} 1, & \text{ha } v_i \xrightarrow{e_j} \\ -1, & \text{ha } \xrightarrow{e_j} v_i \\ 0, & \text{ha } e_j \text{ nem illeszkedik } v_i\text{-hez} \end{cases}$$

• tétel: G irányítatlan, hurokmentes, n csúcsú, c komponensű gráf. $\vec{G}$ legyen egy tetszőleges irányítása G-nek.
$r(B(\vec{G})) = n - c$

bizonyítás:

↳ lemma:

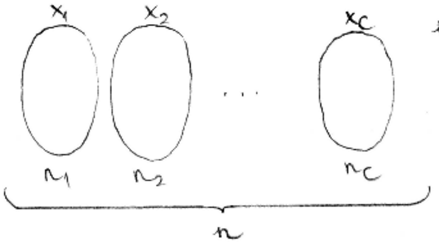
$$M = \begin{pmatrix} M_1 & & & 0 \\ & M_2 & & \\ & & \ddots & \\ 0 & & & M_k \end{pmatrix}$$

$r(M) = r(M_1) + r(M_2) + \dots + r(M_k)$

biz: együtt is lineárisan függetlenek

I. eset: ha G összefüggő $(c=1)$ $\Rightarrow$ $r = n-1$

II. eset: $c>1$ db komponense van:



komponensek

$$B(\vec{G}) = \begin{array}{c|cccc} & x_1 \text{ élei} & x_2 \text{ élei} & & \\ \hline x_1 \text{ csúcsai} & B(x_1) & 0 & & \\ x_2 \text{ csúcsai} & 0 & B(x_2) & & \\ & & & \ddots & \\ & & & & B(x_c) \end{array}$$

$r(B(\vec{G})) = (n_1 - 1) + (n_2 - 1) + \dots + (n_c - 1) = n - c$

I. eset bizonyítása: $r \le n-1$ $\Leftarrow$ összes sor lineárisan öf. $\Leftarrow$ a sorok összege 0.

↳ további bizonyítandó: $r \ge n-1$ $\Leftrightarrow$ $(n-1)\times(n-1)$-es $\neq 0$ determináns.

van benne feszítőfa:

F feszítőfa

v_1: elsőfokú F-ben $\to$ e_1 él kapcs. hozzá

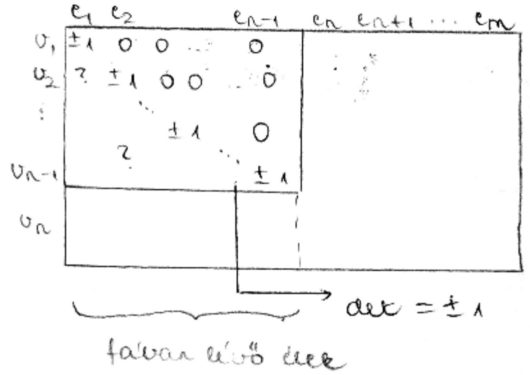
v_2: elsőfokú $(F-v_1)$-ben $\to$ e_2 él

$\vdots$

ilyen sorrendben képezzük el az illeszkedési mátrixot: $\Leftarrow$ v_k: elsőfokú $(F-\{v_1, v_2, \dots, v_{k-1}\})$-ben $\to$ e_k él

$\vdots$

v_n



észrevétel: bármelyik csúcs lehet a v_n (mert bármelyik fában $\exists$ két elsőfokú csúcs) $\Rightarrow$ bármelyik sor kihagyása után $r = n-1$, azaz $\forall$ $(n-1)$ sor lineárisan független.

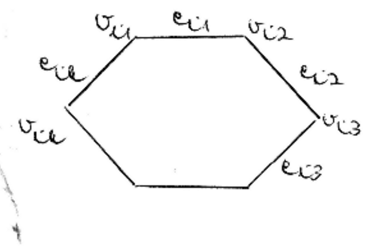
• tétel: G irányítatlan, összefüggő, n csúcsú
$\vec{G}$ tetszőleges irányítással nyerhető G-ből.

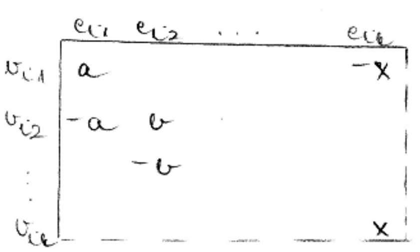
$(n-1)$ oszlopa $B(\vec{G})$-nek lin. független $\Leftrightarrow$ megfelelő élek G-ben feszítőfát alkotnak

bizonyítás

$\Leftarrow$: előző biz-ból következik.

$\Rightarrow$: indirekt biz: tfh. nem feszítőfa, tehát van benne kör





a k sor összege 0, tehát az oszlopa lin. összefüggőek ↯

• def. körmátrix

$\vec{G}$ $E(G) = \{e_1, e_2, \dots, e_m\}$

$C = \{C_1, C_2, \dots, C_k\} \rightarrow$ minden körhöz hozzárendelve egy körbejárás $\Big\}$ $C(\vec{G}) = k \times m$-es

$$c_{ij} = \begin{cases} +1, \text{ ha } e_i \in C_j & \text{megfelelő irányú} \\ -1, \text{ ha } e_i \in C_j & \text{az ellentétes irányú} \\ 0, \text{ ha } e_i \notin C_j & \end{cases}$$

huroktörvények $C \cdot \underline{u} = \underline{0}$

• tétel: G n csúcsú, e élű, összefüggő

• $r(C(\vec{G})) = e - n + 1$

• $e-n+1$ oszlop lin. független $\Leftrightarrow$ feszítőfa komplementerének megfelelő oszlopok

$\downarrow$

$e-(n-1)$

• def: vágásmátrix

$\vec{G}$: $E(\vec{G}) = \{e_1, e_2, \dots, e_m\}$

$Q = \{Q_1, Q_2, \dots Q_L\} \rightarrow \forall$ vágáshoz hozzárendelve egy irányítás (a két csúcshalmaz közötti "átlépés" iránya) $\Big\}$ $Q(\vec{G}) = L \times m$

$$q_{ij} = \begin{cases} +1, \text{ ha } e_i \in Q_j & e_i + \text{ irányítású} \\ -1, \text{ ha } e_i \in Q_j & e_i - \text{ —"—} \\ 0, \text{ ha } e_i \notin Q_j & \end{cases}$$

• tétel G n csúcsú, e élű, öf.

• $r(Q(\vec{G})) = n-1$

• $n-1$ oszlop lin. független $\Leftrightarrow$ feszítőfának megfelelő oszlopok

8. előadás
ápr. 1.

SZÁMELMÉLET

- a számelmélet egész számokkal foglalkozik

• <u>def</u>:

b osztója a-nak ; a többszöröse b-nek, ha $\exists q$: $a=bq$

<u>jelölés</u>: $b|a$

tulajdonságok: $b|a$ és $a|c \Rightarrow b|c$

$b|a_1$ és $b|a_2 \Rightarrow b|a_1 \pm a_2$

$\forall k$-ra: $k|0$

x egység, ha $\forall k$: $x|k$ $\quad x \in \{-1,1\}$

• <u>def</u>: a,b legnagyobb közös osztója d_1, ha

↳ $d_1|a$

↳ $d_1|b$

↳ $\forall c$: $c|a \wedge c|b \Rightarrow |c| \leq |d_1|$

• <u>def</u>: a,b kitüntetett közös osztója d_2, ha

↳ $d_2|a$

↳ $d_2|b$

↳ $\forall c$: $c|a \wedge c|b \Rightarrow c|d_2$

• <u>állítás</u>: kitüntetett közös osztó $\Leftrightarrow$ legn. közös osztó

<u>biz</u> $\Rightarrow$: $c|d_2 \Rightarrow |c| \leq d_2$

• <u>def</u>: a,b relatív prím, ha $(a,b)=1$

$a_1,a_2,\dots,a_k$ relatív prímek, ha $(a_1,a_2,\dots,a_k)=1$ - azaz nemcsak 2 számra lehet definiálni. de nem jelenti azt, hogy páronként is relatív prímek lennének. pl: $(6,10,15)=1$

• <u>def</u>: p szám felbonthatatlan, ha $p=ab \Rightarrow a=\pm 1$ vagy $b=\pm 1$

$p \neq 0$ és $p \neq$ egység

• <u>def</u>: p szám ($p \neq 0$ és $p \neq$ egység) prím tulajdonságú, ha $p|ab \Rightarrow p|a$ vagy $p|b$
(vagy mindkettő)

• <u>állítás</u>: prím $\Leftrightarrow$ felbonthatatlan

<u>biz</u>: $\Rightarrow$: indirekt: tfh p prímtulajdonságú, de $p=a\cdot b$ úgy, hogy

$|a|>1 \wedge |b|>1$

$p|ab \Rightarrow$ pl. $p|a$ ↯ mert $|b|>1$-ből: $|a|<|p|$

• A számelmélet alaptétele: ∀ egész szám egyértelműen előáll prímek (felbonthatatlan számok) szorzataként sorrendtől és egységekkel való szorzástól eltekintve.

Bizonyítás → felbontható: ∀ egész szám előáll felbonthatatlanok szorzataként
↳ ha felbonthatatlan ✓
↳ ha nem, akkor felbontjuk, ezt értékben mindig kisebb számot kapunk, mivel véges számokról van szó, ezért egyszer felbonthatatlanokhoz jutunk

→ egyértelműen

• def: szám kanonikus alakja: $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \dots = \prod_{i=1}^{\infty} p_i^{\alpha_i}$

→ azonban ∀ konkrét számra ez véges szorzat

→ végtelen sok prímszám van

$$n = \prod p_i^{\alpha_i}, \quad k = \prod p_i^{\beta_i} \quad \Rightarrow \quad (n,k) = \prod p_i^{\min(\alpha_i,\beta_i)}$$

• n pozitív osztóinak a száma: $d(n) = \prod_{i=1}^{\infty} (\alpha_i + 1)$

• n pozitív osztóinak az összege: $\sigma(n) = \prod_{i=1}^{\infty} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}$

biz: $(1 + p_1 + p_1^2 + p_1^3 + \dots + p_1^{\alpha_1})(1 + p_2 + p_2^2 + p_2^3)(\dots)$

minden kombináció egyszer fordul elő → ez az összes osztó

$$\sum_{\beta_i \le \alpha_i} p_1^{\beta_1} \cdot p_2^{\beta_2} \dots$$

• Euklideszi algoritmus: $a, b : a \ge b$

$$\begin{aligned}
a &= b \cdot k_1 + m_1 & 0 &\le m_1 < b \\
b &= m_1 \cdot k_2 + m_2 & 0 &\le m_2 < m_1 \\
m_1 &= m_2 \cdot k_3 + m_3 & 0 &\le m_3 < m_2 \\
m_2 &= m_3 \cdot k_4 + m_4 & 0 &\le m_4 < m_3 \\
&\vdots \\
m_{n-1} &= m_n k_{n+1} + m_{n+1} \\
m_n &= m_{n+1} k_{n+2} + \underline{\underline{0}} & &\to \text{akkor } m_{n+1} = (a,b)
\end{aligned}$$

pl: $(51, 24) = ?$

$51 = 2 \cdot 24 + 3$

$24 = 8 \cdot \underline{\underline{3}} + 0$

bizonyítás: azt bizonyítjuk, hogy r_{n+1} kitüntetett osztó $\Rightarrow r_{n+1} | a$

$r_{n+1} | b$

utolsó sor: $r_{n+1} | r_n$

utolsó előtti sor: $r_{n-1} = \underbrace{r_n k_{n+1}}_{r_{n+1}|} + r_{n+1} \Rightarrow r_{n+1} | r_{n-1}$

illetve $\forall x | a \wedge x | b$ -re $\Rightarrow x | r_{n+1}$

$x | r_1$, $x | r_2$, ...

a Fibonacci-számoknál a leglassabb az algoritmus, azaz ha két egymás melletti Fibonacci-szám legn. közös osztóját keressük (mivel a hányados mindig 1)

- állítás 1) ha $c > 0$: $(ca, cb) = c(a, b)$

  az euklideszi algoritmusból követk.

  2) ha $c | ab$ és $(c, a) = 1 \Rightarrow c | b$

  biz: $c | ab \wedge c | cb \Rightarrow c | (ab, cb)$

  $c | b(a, c) = b$

  relatív prímek

  3) p felbonthatatlan $p | ab$ és $p \nmid a \overset{?}{\Rightarrow} p | b$

  $(p, a) = 1$: mert $(p, a) | p$ $\left.\begin{matrix} \\ p \text{ felbonthatatlan} \end{matrix}\right\} (p, a) = 1$ ugyanígy b osztója

  4) egyértelmű felbontás bizonyítása:

  $n = p_1 \cdot p_2 \cdot p_3 \cdot \ldots = q_1 \cdot q_2 \cdot q_3 \cdot \ldots$

  $p_1 | q_1 \cdot q_2 \cdot q_3 \cdot \ldots \Rightarrow \exists i$, hogy $p_1 | q_i$

  ⋮ stb.

a páros számok körében nem igaz a felbonthatatlanság és az egyértelműség

pl: $2 | 6 \cdot 10 \not\Rightarrow 2 | 6$ vagy $2 | 10$, sem az egyiko $\Rightarrow$ kitüntetett o. pl. a polinomoknál.

Prímszámok tulajdonságai

- tétel: ∞ sok prímszám van $2, 3, 5, 7, \ldots$

  biz: indirekt: tfh. $p_1, p_2, \ldots, p_N$ az összes prím

  $X = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_N + 1$ ... összetett lenne, de egyik p_i-vel sem osztható ↯

- egyetlen páros prímszám van

ha x prím $\Rightarrow$ $\left.\begin{array}{l} x=4k+1 \\ x=4k-1 \end{array}\right\}$ alakú

- tétel: ∞ sok $4k-1$ alakú prím van

biz: indirekt tfh. $p_1, p_2, \dots p_n$ az összes $4k-1$ alakú prím

$Y = p_1 \cdot p_2 \cdot p_3 \cdots p_n - 1$ összetett lenne

de nem lehet, hogy minden prímosztója $4k+1$ alakú legyen,

mert azok szorzata $4k+1$ alakú $\lightning$

- tétel (Dirichlet): ha $(a,b)=1 \Rightarrow \infty$ sok $ak+b$ alakú prím is van

- tétel (Csebisev): $\forall x$-re x és $2x$ között van prím

- sejtés: $\forall x$-re: x és $x+\sqrt{x}$ között van prím

de: x és $x+x^{0,5351}$ között van prím $\Rightarrow$ igaz (bizonyított)

- sejtés: végtelen sok ikerprím van
- sejtés: $\forall$ páros szám (≥ 4) előáll két prímszám összegeként

9. előadás
ápr. 8.

- def: $\pi(x)$ = a $[2,x]$ intervallumban található prímek száma.

$\pi(x) \sim \frac{x}{\ln x}$ - azaz: $\lim\limits_{x\to\infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1$. (Gauss bizonyította)

- tétel: $\sum\limits_{i=1}^{\infty} \frac{1}{p_i}$ divergens ($\sum \frac{1}{n^2}$ konv., tehát a prímszámok "sűrűbben vannak", mint a négyzetszámok)

- tétel:

$\forall k$-ra létezik intervallum, hogy k db konszekutív szám egyike se prím.

bizonyítás: legyen $N>k$;

akkor: $N!+2$ osztható 2-vel

$N!+3$ –"– 3-mal

$\vdots$ $\vdots$

$\Downarrow$ $N!+N$ –"– N-nel

ez legalább k db szám; mind összetett, hiszen osztható 2-vel vagy 3-mal vagy ... N-nel ha $m>1$ rögzített egész szám: m elem-ű "csoport"-ot különíthetünk el oszthatóság szerint.

$\Downarrow$

$\boxed{\text{Maradékosztályok (mod } m)}$

$a \equiv b \pmod m$ – a kongruens b-vel

ha ugyanabban a mod m maradékosztályban vannak

$\Updownarrow$

$m \mid a-b$

tulajdonságok:

- $\forall a$-ra: $a \equiv a \pmod m$ /reflexivitás/
- $\forall a,b$-re: ha $a \equiv b \pmod m \Rightarrow b \equiv a \pmod m$ /szimmetria/
- $\forall a,b,c$-re: ha $\left.\begin{array}{l} a \equiv b \pmod m \\ \text{és } b \equiv c \pmod m \end{array}\right\} \Rightarrow a \equiv c \pmod m$ /tranzitivitás/

- tfh $a \equiv b \pmod m$ és $c \equiv d \pmod m$

  ekkor: (1) $a+c \equiv b+d \pmod m$

  (2) $a-c \equiv b-d \pmod m$

  (3) $ac \equiv bd \pmod m$

  (3) bizonyítása: $ac-bd = ac-bc+bc-bd = c(a-b)+b(c-d)$

  osztható m-mel

megj: viszont nem mindig igaz, hogy $\frac{a}{c} \equiv \frac{b}{d} \pmod m$

- tfh. $ac \equiv bc \pmod m$ és $(c,m)=1 \Rightarrow a \equiv b \pmod m$
- $ac \equiv bc \pmod m \Rightarrow a \equiv b \left(\text{mod } \frac{m}{(c,m)}\right)$

  a tétel bizonyítása:

  legyen $(c,m)=d$ $\quad \left(\frac{m}{d}, c\right)=1$

  $m \mid ac-bc = c(a-b)$ $\quad m = d \cdot \frac{m}{d}$

  $\left.\begin{array}{ll} d \cdot \frac{m}{d} \mid c(a-b) \Rightarrow \frac{m}{d} \mid \frac{c}{d}(a-b) & \\ d \mid c & \left(\frac{m}{d}; \frac{c}{d}\right)=1 \end{array}\right\} \Rightarrow \frac{m}{d} \mid a-b$

Lineáris kongruenciák

$ax \equiv b \pmod m$ keressük azokat a maradékosztályokat (mod m), melyekre ez teljesül

pl

$2x \equiv 0 \pmod 2$	$3x \equiv 5 \pmod 2$	$2x \equiv 3 \pmod 2$
$x \equiv 0 \pmod 2$	$x \equiv 1 \pmod 2$	nincs mo.
$x \equiv 1 \pmod 2$		

• tétel

$ax \equiv b \pmod m$ megoldható $\iff$ $(a,m) \mid b$

1) $\Rightarrow$ bizonyítás: $(a,m) = d$

$\left.\begin{array}{l} a = da_1 \\ m = dm_1 \end{array}\right\}$ és $(a_1, m_1) = 1$

$ax \equiv b \pmod m \rightarrow m \mid ax - b$

$dm_1 \mid a_1 d x - b$

$d \mid a_1 d x - b \Rightarrow d \mid b$

2) $\Leftarrow$ bizonyítás: $a = da_1$; $m = dm_1$; $b = db_1$

$ax \equiv b \pmod m$

$d_1 a_1 x = db_1 \pmod{dm_1}$

$a_1 x = b_1 \pmod{m_1}$ megoldható; ahol $(a_1, m_1) = 1$.

Teljes maradékrendszer (mod m)

egy olyan $\{r_1, r_2, r_3, \dots, r_k\}$ számhalmaz, melyből $\forall$ mod m maradékosztályra épp egy elem esik

• tétel: egy $\{r_1, r_2, \dots, r_k\}$ számhalmaz teljes maradékrsz. (mod m)

$\iff \begin{cases} (1): k = m \\ (2)\ r_i \not\equiv r_j \pmod m \text{ ha } i \neq j \end{cases}$

• tétel: legyen $\{r_1, r_2, \dots, r_k\}$ teljes maradékrsz. (mod m) és legyen q olyan, hogy $(q, m) = 1$ $\Rightarrow$ $\{r_1 q, r_2 q, \dots, r_k q\}$ is teljes maradékrsz. (mod m)

bizonyítás: $\Rightarrow$ triv. (1.)

(2): tfh. $r_i q \equiv r_j q \pmod m \Rightarrow m \mid q(r_i - r_j) \underset{(m,q)=1}{\Rightarrow} m \mid r_i - r_j$

ezért $i = j$ lenne $\lightning$

$\{0; 1; 2; \dots; m_1 - 1\}$ teljes maradékrsz. (mod m_1); szorozzuk a_1-gyel:
$\{0; a_1; 2a_1; \dots (m_1-1)a_1\}$ is teljes — " — ; hiszen $(a_1, m_1) = 1$.
↳ ezért $\exists x$: $a_1 x \equiv b_1 \pmod{m_1}$

(pl) $12x \equiv 39 \pmod 9$

$(12, 9) = 3 \mid 39$ ✓ megoldható $\rightarrow$ $4x \equiv 13 \pmod 3$

$x \equiv 1 \pmod 3$

$x \equiv 1$ vagy 4 vagy 7 (mod 9) – eredetire mo.

(12) $8x \equiv 17 \pmod{13}$

$8x \equiv 4 \pmod{13}$

$2x \equiv 1 \pmod{13}$

$2x \equiv 14 \pmod{13}$

$x \equiv 7 \pmod{13}$

$\boxed{\text{Lineáris diofantikus egyenletek}}$

$17x + 31y = 291$

$31y \equiv 291 \pmod{17}$

$14y \equiv 2 \pmod{17}$

$7y \equiv 1 \pmod{17}$

$4y \equiv 3 \pmod{17}$

$-y \equiv -5 \pmod{17}$

$y \equiv 5 \pmod{17}$ $\quad \underline{y = 17k + 5}$

$17x + 31 \cdot 17k + 31 \cdot 5 = 291$

$17(x + 31k) = 291 - 155 = 136 = 17 \cdot 8$

$x + 31k = 8$

$x = \underline{8 - 31k}$ $\quad \Rightarrow$ megoldás: $x = 8$; $y = 5$

• tétel: ha $(a, b) = 1 \Rightarrow \exists\, k, l$ egészek, hogy $ak + bl = 1$

$\forall\, a, b\ \exists\, k, l$ hogy $ak + bl = (a, b)$

Szimultán kongruenciarendszerek:

$2x \equiv 5 \pmod 7$ és $3x \equiv 4 \pmod 8$

$x \equiv 6 \pmod 7$

$x = 7k + 6$

$21k + 18 \equiv 4 \pmod 8$

$5k + 2 \equiv 4 \pmod 8$

$5k \equiv 2 \pmod 8$

$k \equiv 2 \pmod 8 \Rightarrow k = 8l + 2$

$x = 56l + 14 + 6 = 56l + 20$ //

• Wilson-tétel: ha p prímszám, akkor

$(p-1)! \equiv -1 \pmod p$

Biz: $1 \cdot \underbrace{2 \cdot 3 \cdot \ldots \cdot (p-3)(p-2)}(p-1)$

ha $x \in \{2, 3, \ldots, p-2\} \Rightarrow \exists\, y$, hogy $xy \equiv 1\ (p)$ és $y \in \{2, 3, \ldots, p-2\}$.

$xy \equiv 1 \pmod p$ megoldható, mert:

$(x, p) = 1$

továbbá bizonyítandó, hogy $\nexists\ x^2 \equiv 1 \pmod p \rightarrow x^2 - 1 \equiv 0$

$p \mid (x-1)(x+1)$ $\nearrow p \mid x-1$ $\searrow p \mid x+1$ $\quad$ G

• <u>def</u>: redukált maradékrendszer mod m (RMR): $\{a_1, a_2, \dots, a_k\}$

(1) $k = \varphi(m)$

(2) $i \neq j \Rightarrow a_i \not\equiv a_j \ (m)$

(3) $(a_i, m) = 1$

• <u>def</u>: $\varphi(m) = 1$ és m között m-hez relatív prímek száma

pl. $\varphi(8) = 4 \quad (1, 3, 5, 7)$

$\varphi(10) = 4$

pl: mod 10: $\{1, 3, 7, 9\}$; $\{81; 2003; 27; 49\}$

$\rightarrow \varphi(p) = p - 1$ ha p prím

$\rightarrow \varphi(p^\alpha) = p^\alpha - \frac{p^\alpha}{p} = p^\alpha - p^{\alpha-1}$

$\rightarrow \varphi(pq) = pq - p - q + 1 = (p-1)(q-1)$

• <u>tétel</u> $(a, b) = 1 \Rightarrow \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ (¬B)

tetszőleges számra: $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$

$$\varphi(n) = \varphi(p_1^{\alpha_1}) \cdot \varphi(p_2^{\alpha_2}) \cdot \ldots \cdot \varphi(p_k^{\alpha_k}) =$$

$$= \boxed{(p_1^{\alpha_1} - p_1^{\alpha_1 - 1})(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \ldots (p_k^{\alpha_k} - p_k^{\alpha_k - 1})} =$$

$$= p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) p_2^{\alpha_2}\left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot p_k^{\alpha_k}\left(1 - \frac{1}{p_k}\right) =$$

$$= \boxed{n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right)}$$

pl. $\varphi(100) = \varphi(2^2 \cdot 5^2) = (2^2 - 2)(5^2 - 5) = 40$

• <u>tétel</u>: $\left.\begin{array}{l} c_1, c_2, \dots, c_{\varphi(m)} \\ \text{RMR mod } m \\ (a, m) = 1 \end{array}\right\} \Rightarrow ac_1, ac_2, \dots, ac_{\varphi(m)}$ RMR mod m

<u>bizonyítás</u>: (1) $\varphi(m)$ db ✓

(2) indirekt tfh $ac_i \equiv ac_j \pmod m$ $/ :a \leftarrow (a, m) = 1$

$c_i \equiv c_j \pmod m$

$i = j$ ↯

(3) $\left.\begin{array}{l} (c_i, m) = 1 \\ (a, m) = 1 \end{array}\right\} \overset{?}{\Rightarrow} (ac_i, m) = 1$

a-nak és c_i-nek nem volt közös prímosztója m-mel, így ac_i-nek sem lesz

• tétel (Euler – Fermat)

$(a,m)=1 \Rightarrow a^{\varphi(m)} \equiv 1 \pmod m$

példa: $m=100$; $a=2003$

$2003^{40} \equiv 1 \pmod{100}$

bizonyítás: $c_1, c_2, \dots, c_{\varphi(m)}$ RMR mod m $\Rightarrow$ $ac_1, ac_2, \dots ac_{\varphi(m)}$ RMR mod m

összeszorozva:

$$(ac_1)(ac_2)\cdots(ac_{\varphi(m)}) \equiv c_1 \cdot c_2 \cdots c_{\varphi(m)} \pmod m$$

$$a^{\varphi(m)} \cdot c_1 \cdot c_2 \cdots c_{\varphi(m)} \equiv c_1 \cdot c_2 \cdots c_{\varphi(m)} \pmod m \quad /: c_1 c_2 \cdots c_{\varphi(m)}$$

mert $(c_i, m)=1$

$$a^{\varphi(m)} \equiv 1 \pmod m$$

ha $m=p$ prím ; $p \nmid a$ $\Rightarrow$ $a^{p-1} \equiv 1 \ (p)$ $/ \cdot a$

$a^p \equiv a \ (p)$ → Fermat csak ezt bizonyította

• tétel (kis Fermat tétel)

p prím $\Rightarrow a^p \equiv a \pmod p$

bizonyítás: $p \nmid a \Rightarrow$ láttuk

$p \mid a \Rightarrow 0^p \equiv 0 \pmod p$

$0 \equiv 0$ ✓

CSOPORTELMÉLET

• def: $H \neq \emptyset$ tetszőleges alaphalmaz

H^2: { H-ból képezhető rendezett párok }

$f: H^2 \to H$ függvény → művelet H-n

példa 1) H = { skalárok }

műv: skalár szorzás → NEM MŰV.

2.) H = { 5-tel nem osztható egészek } műv: + → NEM MŰV.

pl. 7+3

jelölés: $+(7,3)=10$

↓

$7+3=10$

$(\mathbb{Z},+)$	H = {n×n-es mátrixok}, ·	H = {zsiráfok} $z_1 \times z_2 \to$ magasabb	H = {banánok} $b_1 ⌂ b_2 = b_2$
kommut. ✓	$\notin$ nem	✓	nem
asszociatív	✓	✓	✓
egységelem: 0	E	legkisebb zsiráf	nincs
inverz: ← $-a$ ∀ elemre	← A^{-1}, ha det ≠ 0	← nincs, csak legkisebb	

• def: $*$ kommutatív, ha $\forall a,b \in H$-ra: $a*b = b*a$
• def: $*$ asszociatív, ha $\forall a,b,c \in H$-ra: $(a*b)*c = a*(b*c)$
• def: $(S,*)$ $*$ asszociatív $\Rightarrow$ $(S,*)$ félcsoport
• def: $e \in H$ egységelem, ha $\forall a \in H$: $a*e = a = e*a$
• def: $a \in H$, van egységelem
a-nak a^{-1} inverze, ha $a*a^{-1} = e = a^{-1}*a$

• állítás: az egységelem egyértelmű (ha van egységelem)
biz: indirekt: e és f egységelem
$f = e*f = e \Rightarrow f = e$

• állítás: inverz egyértelmű (ha van inverz)
biz: $a \to b$, $a \to c$ } inverz

$$c = e*c = \underbrace{b*a}_{e}*c = b*\underbrace{(a*c)}_{e} = b \Rightarrow b = c$$

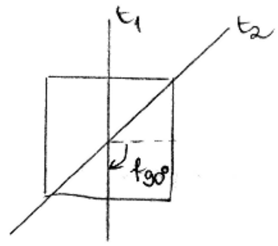
• def: $(G,*)$ csoport, ha:
(1): $*$ asszociatív
(2) van egységelem
(3): $\forall$ elemnek van inverze — példa: $(\mathbb{Z},+)$; $(\mathbb{Q},+)$; $(\mathbb{R},+)$; $(\mathbb{C},+)$

• def: Abel-csoport: olyan csoport, amelyben a műv. kommutatív
példa: $\Rightarrow (\mathbb{R},\cdot)$ $e = 1$
0-nak nincs inverze $\Rightarrow$ nem csoport
$\Rightarrow (\mathbb{R}\setminus\{0\},\cdot)$ csoport $\underset{\neq 0}{a}\cdot\underset{\neq 0}{b} \neq 0$

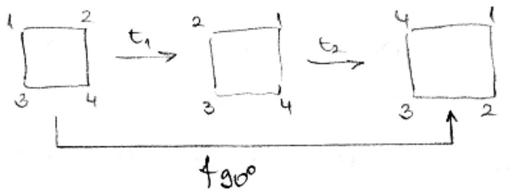
$\Rightarrow \{1;-1;i;-i\}$ asszociatív; egységelem: 1; inverzek:
$1^{-1}=1$; $-1^{-1}=-1$; $i^{-1}=-i$; $(-i)^{-1}=i$

$\Rightarrow$ $n\times n$-es mátrixok, $\cdot$, $\det \neq 0$ } csoport, de nem Abel-csoport

Csoportelméleti alkalmazás:
$R \to$ síkbeli rajz
$H = \{R$-et önmagába vivő egybevágósági transzformációk$\}$
művelet: egymás utáni alkalmazás (kompozíció)
$\to$ R szimmetriacsoportja



$t_1 \circ t_2 = t_{90°}$



$t_1^{-1} = t_1$

asszociatív : ✓

egységelem : identitás

11. előadás
ápr. 22

• def: hatványozás $(G,*)$; $g \in G$ csoport

$$g^n = \underbrace{g * g * g * \dots * g}_{n \text{ db}} \qquad g^1 = g \ ; \ g^0 = e$$

* asszociatív, így nincs zárj-i probléma

példa: $(\mathbb{Z},+)$: $3^5 = 15$

G véges, $g \in G$

$g^1, g^2, g^3, \dots g^l, g^k$

$\exists\ 1 \le l < k \qquad g^k = g^l \qquad / \cdot g^{-1}$

$$\underbrace{g \cdot g \cdots g}_{k-1} = \underbrace{g \cdot g \cdot g \cdots g}_{l-1}$$

$$g^{k-1} = g^{l-1} \qquad / \cdot g^{-1}$$

$$\vdots$$

$$e = g^{k-l}$$

• def: $(G,\cdot)$ $g \in G$

g rendje a legkisebb $n \ge 1$, amelyre $g^n = e$; jele: $o(g)$ /order/

ha ilyen nincs, akkor $o(g)$ végtelen

• tétel: G véges $\Rightarrow$ $\forall$ elemnek véges a rendje

biz: ld. előbb

• def: csoport rendje az elemszáma ; jele: $|G|$

példa: $\{\pm 1 ; \pm i\}$

$i^1, i^2 = -1 ; i^3 = -i, i^4 = 1 \qquad o(i) = 4$

• def: ha $\exists\, g \in G$, hogy g hatványai és ezek inverzei a teljes csoportot kiadják, akkor G ciklikus csoport.

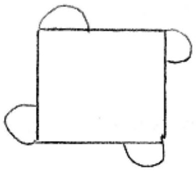
Ez az g elem a csoport generátoreleme.

példa: ciklikus csoportra

$\Rightarrow (\mathbb{Z}; +)$: 1

$\Rightarrow (\{\pm 1; \pm i\}, \cdot)$

$\Rightarrow$



$I;\ f_{90°},\ f_{180°},\ f_{270°}$

↳ generátorelem

• állítás: $|G|$ véges

G ciklikus $\iff \exists\, g \in G \quad o(g) = |G|$

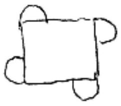
bizonyítás: $\Leftarrow$ g hatványai kimerítik a csoportot

$\Rightarrow o(g) = n$: $(g^k)^{-1} = g^{n-k}$, mert $g^k \cdot g^{n-k} = g^n = e$

• def: $(G_1, \circ), (G_2, \circ)$ izomorfak, ha $\exists\, f$ függvény: $G_1 \to G_2$ kölcsönösen egyértelmű; és $\forall\, a, b \in G_1$-re: $f(a \circ b) = f(a) \circ f(b)$

jele: $G_1 \cong G_2$

példa 1) $(\{\pm 1; \pm i\}, \cdot)$



$i, -1, -i, 1$

$\updownarrow$

$f_{90°}, f_{180°}, f_{270°}, I$

2) $(\mathbb{R}^+, \cdot) \xrightarrow{\log} (\mathbb{R}, +)$

$\log(ab) = \log a + \log b$

• def: diédercsoport: szabályos n-szög szimmetriacsoportja; jele: D_n

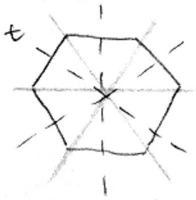
→ elemei: $I, f_\alpha, f_{2\alpha}, \dots, f_{(n-1)\alpha}$; ahol $\alpha = \frac{360°}{n}$

n db tükrözés

$\Downarrow$

$|D_n| = 2n$

t



$o(t) = 2$

$o(f_\alpha) = n$

$o(f_{2\alpha}) =$ ↗ $\frac{n}{2}$, ha n ps. ↘ n, ha n ptl.

• tétel: (Lagrange)

$\left.\begin{array}{l} G \text{ véges} \\ g \in G \end{array}\right\} \Rightarrow o(g) \mid |G|$

elemszám: 1 C_1

2 C_2

3 C_3

4 C_4 ; D_2 - nem izomorf : Klein

5 C_5

6 C_6 ; D_3 az első, amelyik nem Abel-csoport

7 C_7

8 C_8 ; D_4 + még egy nem-Abel van

• Szimmetrikus csoport

• def permutáció

$f: \{1,2,3,\dots,n\} \to \{1,2,3,\dots,n\}$ f kölcsönösen egyértelmű

jelölése pl. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}$

• def: $H = \{ \{1,2,\dots,n\}$ permutációi $\}$; művelet: $\circ$ $\Rightarrow S_n$

$|S_n| = n!$

$$\underset{a}{\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}} \circ \underset{b}{\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix}} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 5 & 2 \end{pmatrix}$$

$$b \circ a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 5 & 2 \end{pmatrix} \neq$$ nem kommutatív

• állítás: S_n csoport

- asszociatív ✓
- egységelem: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$
- inverz pl. $a^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$ $a \circ a^{-1} = e$

$S_3 \cong D_3$; $C_2 \cong S_2$

• def: részcsoport ; jele: $H \leq G$

$(G, \cdot)$ csoport, $H \subseteq G$

H részcsoport, ha $(H, \cdot)$ csoport

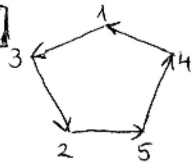
példa: $(\mathbb{Q}, +) \leq (\mathbb{R}, +)$; $(\mathbb{Z}, +) \leq (\mathbb{Q}, +)$

$D_3 \geq H = \{1, t\}$ 

$D_3 \geq H' = \{1, f_{120°}, f_{240°}\}$

• <u>tétel</u> (Cayley)

Minden véges csoport izomorf (alkalmas n-re) S_n egy részcsoportjával. (TB)

Ciklus: 

jelölés: $(1\,3\,2\,5\,4) = (2\,5\,4\,1\,3)$

$a = (1\,5\,3)(2\,4) \Rightarrow$ ciklusfelbontás: diszjunkt ciklusok kompozíciójaként való felírás

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 4 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$$

$$(1\,5\,3)(2\,4) \circ (1\,3\,2\,5\,4) = (1\,4\,5\,2)\underbrace{(3)}_{1} = (1\,4\,5\,2)$$