Számításelmélet 98/99 II. félév vizsgatételsor

Binzberger Viktor (bv121@hszk.bme.hu)

1999. június 7.

1 Euler-körök és -utak, Euler tétele.

Definíció G-ben **Euler-kör** egy olyan zárt séta, amely minden élen pontosan egyszer halad át. G-ben **Euler-út** egy olyan nem zárt séta, ami minden élen pontosan egyszer halad át.

Tétel (Euler) Egy G gráfban akkor és csak akkor van Euler-kör, ha G minden pontjának fokszáma páros.

Tétel Egy G gráfban akkor és csak akkor van Euler-út, ha két fokszám páratlan, a többi páros.

2 Hamilton-körök és -utak. Hamilton-kör létezésének szükséges teltétele. Nem elégségességre példa (Petersen-gráf). Elégséges feltételek: Dirac és Ore tétele.

Definíció Egy G gráfban **Hamilton-körnek** nevezünk egy kört, ha G minden pontját pontosan egyszer tartalmazza. Egy utat **Hamilton-útnak** nevezünk, ha G minden pontját pontosan egyszer tartalmazza.

2.1 Szükséges feltétel Hamilton-kör létezésére

Tétel Egy G gráfban csak akkor létezik Hamilton-kör, ha G-ből tetszőleges k db csúcsot elhagyva a megmaradó gráf komponenseinek a száma $\leq$ k.

2.2 Elégséges feltételek Hamilton-kör létezésére

Tétel (Dirac) Ha egy n csúcsú G gráfnak minden csúcsának a fokszáma $\geq$ n/2, akkor G-ben van Hamilton-kör.

Tétel (Ore) Ha G-ben minden olyan x,y $\in$ V(G) amire x,y $\notin$ E(G) igaz az, hogy d(x)+d(y) $\geq$ n akkor G-ben van Hamilton-kör.

3 További elégséges feltételek: Pósa és Chvátal tétele. A Chvátal-tétel optimalitása.

Tétel (Pósa) Ha G fokszámai $d_1 \leq d_2 \leq \ldots \leq d_n$, és $\forall k < n/2$-re teljesül $d_k \geq k+1$, akkor G-ben van Hamilton-kör.

Tétel (Chvátal) Ha G fokszámai $d_1 \leq d_2 \leq \ldots \leq d_n$, és minden k-ra - amelyre $d_k \leq k < n/2$ - teljesül, hogy $d_{n-k} \geq n-k$, akkor G-ben van Hamilton-kör.

4 Páros gráfok fogalma, karakterizációja. Párosítások, Hall és Frobenius tétele, Tutte tétele (utóbbi csak a könnyű irány bizonyításával).

Definíció G **páros gráf**, ha pontjainak V(G) halmaza felosztható A és B diszjunkt halmazokra úgy, hogy G minden élének egyik végpontja A-ban, másik végpontja B-ben van. Jele: G=(A,B)

Tétel Egy G gráf akkor és csak akkor páros gráf, ha nem tartalmaz páratlan hosszú kört.

Definíció (Részleges) **párosításnak** nevezünk egy M élhalmazt, ha semelyik élnek sincs közös pontja.

Egy párosítast **teljes párosításnak** nevezünk, ha a gráf minden pontját lefedi

Jelölés N(X)-szel jelöljük egy X $\subseteq$ V(G) ponthalmaz szomszédainak halmazát

Tétel (Hall-feltétel) Egy G=(A,B) páros gráfban akkor és csak akkor van A-t lefedő párositas, ha minden X $\subseteq$ A részhalmazra $\mid N(X) \mid \geq \mid X \mid$

Tétel (Frobenius) Egy G=(A,B) páros gráfban akkor és csak akkor van teljes párosítás, ha $\mid A \mid = \mid B \mid$ és $\mid N(X) \mid \geq \mid X \mid$.

Tétel (Tutte) Egy G tetszőleges gráfban akkor és csak akkor van teljes párosítás, ha bármely k pontot elhagyva a páratlan komponensek száma *leq* k.

5 König-tétel, Gallai tételei.

Jelölés :
α(G) - független pontok maximális száma
τ(G) - lefogó pontok minimális száma
μ(G) - független élek maximális száma
ρ(G) - lefogó élek minimális száma

Tétel (Gallai) $\tau(G) + \alpha(G) = \mid V(G) \mid$ minden hurokmentes G gráfra.

Tétel (Gallai) $\mu(G) + \rho(G) =\mid V(G) \mid$ minden G gráfra, amelyben nincs izolált pont.

Tétel (König) Páros gráfban $\tau(G) = \mu(G)$, azaz a lefogó pontok minimális száma egyenlő a független élek maximális számával. Ha G-ben nincs izolált pont, akkor $\alpha(G) = \rho(G)$ is teljesül.

6 Gráfok színezése, kromatikus szám fogalma. $\chi(G)$ viszonya a maximális fokszámhoz és a klikkszámhoz, Brooks tétele (biz. nélkül), Mycielski konstrukciója.

Definíció Egy gráf kromatikus száma az a legkisebb szám, ahány színnel a gráf pontjai kiszínezhetők úgy, hogy minden két szomszédos pont színe különböző. Jele: $\chi(G)$

Definíció Egy gráf klikkszáma a benne lévő legnagyobb teljes részgráf csúcsainak a száma. Jele: $\omega(G)$

Tétel $\chi(G) \geq \omega(G)$

Tétel (Mycielsky konstrukciója) Minden $k \geq 2$-re létezik olyan G gráf, hogy $\omega(G) = 2$ és $\chi(G) \geq k$

Jelölés $\Delta(G)$ a G legnagyobb fokszáma

Tétel Minden gráfra $\chi(G) \leq \Delta(G) + 1$

Tétel (Brooks) Ha G összefüggő egyszerű gráf és nem K_n vagy páratlan hosszú kör, akkor $\chi(G) \leq \Delta(G)$

7 Speciális gráfok színezése: élgráfok, Vizing-tétel (biz. nélkül); síkgráfok, ötszíntétel.

Definíció Egy gráf kromatikus indexe az a legkisebb szám, ahány színnel a gráf élei kiszínezhetők úgy, hogy minden két csatlakozó él színe különböző. Jele: $\chi'(G)$

Tétel Minden gráfra $\chi'(G) \geq \Delta(G)$

Tétel (Vizing) Minden egyszerű gráfra $\chi'(G) \leq \Delta(G) + 1$

Tétel (Ötszíntétel) Minden síkgráfra $\chi(G) \leq 5$

Tétel (Négyszíntétel) Minden síkgráfra $\chi(G) \leq 4$

8 Perfekt gráfok, példák: páros gráfok, ezek komplementere, páros gráfok élgráfja, ezek komplementere.

Definíció G(V,E) gráfnak **feszített részgráfja** G'(V',E'), ha $V' \subseteq V$, és $E' \subseteq E$ az összes olyan élet tartalmazza, aminek mindkét végpontja V'-ben van.

Definíció G gráf perfekt, ha G-re és minden G' feszített részgráfjára $\chi(G) = \omega(G)$

Tétel Minden páros gráf komplementere perfekt.

9 Perfekt gráf tétel. Erős perfekt gráf sejtés.

Tétel (Lovász) Egy gráf akkor és csak akkor perfekt, ha a komplementere is az.

Tétel (Lovász) G akkor és csak akkor perfekt, ha minden G' feszített részgráfjára $\alpha(G')\omega(G') \geq \mid V(G) \mid$

Sejtés (Erős perfekt gráf sejtés (Berge)) Egy G gráf akkor és csak akkor perfekt, ha nem tartalmaz feszített részgráfként páratlan kört.

10 PERT módszer.

11 Gráfok és mátrixok.

12 Hálózati folyamok, Ford-Fulkerson tétel, Edmonds-Karp tétel (biz. nélkül)

Definíció **Hálózat:** $N = (G, s, t, c) \quad s, t \in V(G) \quad c : E(G) \to \mathbf{R}_+$
G - irányított gráf
s - forrás
t - nyelő
c - élekhez kapacitást rendelő függvény

Definíció **Megengedett folyam** egy olyan, élekhez folyamértékeket rendelő f függvény, amire a kapacitáskorlát és a csomóponti törvény teljesül, azaz
$f : E(G) \to \mathbf{R}_{0,+}$
$\forall e \in E(G) : f(e) \leq c(e)$
$\forall v \in V(G) \backslash \{s, t\} \sum f(e)_{e=(.,v)} = \sum f(e)_{e=(v,.)}$

Definíció Az f folyam értéke a forrásból kifutó (nyelőbe befutó) élek folyamértékeinek összege.

Definíció Egy (G,s,t,c) hálózat (s,t) vágása egy olyan tartalmazásra nézve minimális élhalmaz (ennél kisebb már nem rendelkezik a tulajdonsággal), amelyhez tartozó éleket elhagyva G-ből G két komponensre esik, továbbá s és t a két különböző komponensbe kerül.

Tétel (Ford-Fulkerson) Egy hálózatban a maximális folyamérték egyenlő a minimális (s,t) vágáséval

Tétel (Maximális folyam keresése) :
1. Keressünk javító utat
A G gráfon adott f folyamhoz definiáljunk egy G_f irányított gráfot. $V(G_f) = V(G)$ és fusson irányított él x-ből y-ba, ha

- $(x, y) \in E(G)$ és $f(x, y) < c(x, y)$, vagy pedig
- $(y, x) \in E(G)$ és $f(y, x) > 0$

Ha a G_f gráfban BFS kereséssel találunk s-ből t-be vezető utat, akkor ennek G-ben egy javító út felel meg, ellenkező esetben nincs javító út.
2. A javító út mentén növeljük meg a folyamot
Legyen a javító út előre (s-ből t-be) mutató e_i élei esetén $d_i = c(e_i) - f(e_i)$, visszafelé mutató élei esetén pedig $d_i = f(e_i) - 0$ Legyen d a d_i-k minimuma. Az előremutató éleket növeljük, a visszafelé mutatókat csökkentsük d-vel.
3. Folytassuk ezt addig, amíg van javító út.

Tétel (Edmonds-Karp) Ha a fenti algoritmusban mindig a legrövidebb javító utat vesszük, akkor a szükséges lépésszám felülről becsülhető a pontok számának polinomjával.

13 Menger-tételek, magasabb összefüggőség, Dirac-tétel (biz. nélkül).

Tétel (Menger I.) Legyen G egy irányított gráf, $s, t \in V(G)$. Ekkor az s-ből t-be vezető élidegen irányított utak maximális száma egyenlő az irányított s-t utakat lefogó élek minimális számával.

Tétel (Menger II.) Legyen G egy irányított gráf, $s, t \in V(G)$ két nem szomszédos pont. Ekkor az s-ből t-be vezető (s,t kivételével) pontidegen irányított utak maximális száma egyenlő az irányított s-t utakat (s,t kivételével) lefogó pontok minimális számával.

Tétel (Menger III.) Legyen G egy irányított gráf, $s, t \in V(G)$. Ekkor az s-ből t-be vezető élidegen irányítatlan utak maximális száma egyenlő az irányítatlan s-t utakat lefogó élek minimális számával.

Tétel (Menger IV.) Legyen G egy irányított gráf, $s, t \in V(G)$ két nem szomszédos pont. Ekkor az s-ből t-be vezető (s,t kivételével) pontidegen irányítatlan utak maximális száma egyenlő az irányítatlan s-t utakat (s,t kivételével) lefogó pontok minimális számával.

Definíció Egy gráf **k-szorosan összefüggő**, ha legalább $k+1$ pontja van, és k-nál kevesebb pontot elhagyva a gráf összefüggő marad.

Definíció Egy gráf **k-szorosan élösszefüggő**, ha k-nál kevesebb élet elhagyva a gráf összefüggő marad.

Tétel Egy gráf akkor és csak akkor k-szorosan összefüggő, ha legalább $k+1$ pontja van, és bármely két pontja között létezik k pontidegen út.

Tétel Egy gráf akkor és csak akkor k-szorosan élösszefüggő, ha bármely két pontja között létezik k élidegen út.

Tétel Egy gráf akkor és csak akkor 2-szeresen összefüggő, ha bármely 2 pontján át vezet kör.

Tétel Egy gráf akkor és csak akkor 2-szeresen összefüggő, ha bármely 2 élén át vezet kör.

Tétel (Dirac) Ha egy gráf k-szorosan összefüggő, akkor bármely k db pontján át vezet kör.

14 Ramsey-tétel, Erdős-Szekeres féle becslés.

Tétel (Ramsey) Minden k, l egészhez létezik olyan n_0 szám, hogy $n \geq n_0$ esetén K_n-t pirossal és kékkel színezve biztosan lesz piros K_k vagy kék K_l. A legkisebb ilyen n_0 jele $R(k, l)$.

Tétel

$$R(k, l) \leq R(k-1, l) + R(k, l-1)$$

Bizonyítás Vegyünk egy K_n gráfot ($n = R(k-1, l)+R(k, l-1)$), éleit színezzük pirosra (k) és kékre(l). Válasszunk ki egy x pontot. Ebből

1. $\geq R(k-1, l)$ piros, vagy
2. $\geq R(k, l-1)$ kék él fut ki. (Mert minden pont fokszáma n-1)

1. A kifutó piros élek másik végpontjai között (R(k-1,l) definíciója miatt) vagy van
   (a) K_{k-1} ami piros -¿ ezek x-szel együtt egy piros K_k; avagy
   (b) K_l ami kék
2. Az előbbihez hasonlóan

Tétel (Erdős-Szekeres)

$$R(k, l) \leq \binom{k+l-2}{k-1}$$

15 Turán-tétel. Erdős-Stone tétel (biz. nélkül), Erdős-Simonovits tétel.

DEFINÍCIÓ $ex(n, F)$ az n pontú, F-et nem tartalmazó gráf maximális élszáma.

TÉTEL (TURÁN) G n-csúcsú gráfnak, amire $K_r \not\subseteq G$ legfeljebb annyi éle lehet, amennyi az $r-1$ osztályú T_n^{r-1} Turán-gráfnak, azaz $ex(n, K_r) = |T_n^{r-1}|$. Egyenlőség esetén $G \cong T_n^{r-1}$.

BIZONYÍTÁS $K_r \not\subseteq T_n^{(r-1)}$
Teljes indukció: tegyük fel, hogy $T^{r-1}_{n-(r-1)}$ -re igaz a tétel.
Legyen G egy $n > r$ csúcsú K_r-re telített gráf. $\omega(G) = r-1$, hiszen egyetlen további él K_r -et hoz létre. Tekintsünk egy r-1 méretű klikket. Hívjuk a továbbiakban K-nak.

- $|E(G\backslash K)| \leq |E(T^{r-1}_{n-(r-1)})|$
- $|E(K)| = \binom{r-1}{2}$ (teljes gráf élszáma)
- Mivel $G\backslash K$ minden csúcsa K-nak legfeljebb $r-2$ csúcsával van összekötve (mert ha $r-1$ -el lenne, akkor egy K_r-et kapnánk), ezért
  K és $G\backslash K$ közti élek száma $\leq |V(G\backslash K)|(r-2) = (n-(r-1))(r-2)$

Ebből tehát

$$|E(G)| \leq |E(T^{r-1}_{n-(r-1)})| + \binom{r-1}{2} + (n-(r-1))(r-2) = |T_n^{r-1}|$$

Egyszerű megfontolással adódik, hogy egyenlőség csak $G \cong T_n^{r-1}$ esetén van.

16 Oszthatóság, legnagyobb közös osztó, legkisebb közös többszörös, prímek, a számelmélet alaptétele, osztók száma, osztók összege.

Tétel Lnko, Lkkt kiszámítása
Legyen p_i m és n összes prímosztójának a sorozata. Ekkor

$$m = \prod_{i=1}^{t} p_i^{\alpha_i} \quad n = \prod_{i=1}^{t} p_i^{\beta_i}$$

$$lnko(m,n) = (m,n) = \prod_{i=1}^{t} p_i^{\min(\alpha_i,\beta_i)} \quad lkkt(m,n) = [m,n] = \prod_{i=1}^{t} p_i^{\max(\alpha_i,\beta_i)}$$

Tétel (A számelmélet alaptétele) Minden szám egyértelműen felbontható prímtényezők szorzatára.

Tétel $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ osztóinak száma $d(n) = \prod_{i=1}^{k}(\alpha_i - 1)$.

Tétel $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ osztóinak összege

$$\sigma(n) = (1 + p_1 + p_1^2 + \ldots + p_1^{\alpha_1})(1 + \ldots + p_2^{\alpha_2}) \dots (1 + \ldots + p_k^{\alpha_k}) = \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}$$

17 Euklideszi algoritmus, nevezetes tételek prímszámokról.

Tétel (Euklidészi algoritmus) :
Be: m, n
$a := n \quad b := m$
CIKLUS: $a = kb + r \quad r =?$ maradékos osztás
Ha $r = 0$, akkor $(m,n) = b \quad$ STOP
Egyébként $a := b \quad b := r$
ugrás: CIKLUS

Tétel (Euklidesz) A prímek száma végtelen

Tétel (Dirchlet) Ha $(a,b) = 1$ (relatív prímek), akkor végtelen sok prím van az $ak + b$ sorozat elemei között.

Tétel (Prímszámtétel)

$$\lim_{n\to\infty} \frac{\pi(n)}{\frac{n}{\ln n}} = 1$$

ahol $\pi(n)$ az n-nél nem nagyobb prímek számát jelenti.

Tétel (Csebisev) n és $2n$ között mindig van prímszám.

Sejtés (Goldbach) Minden 2-nél nagyobb páros szám felírható két prím összegeként

Tétel (Rényi) A páros számok felírhatók $u + v_\ell$ alakban, ahol u prím, v_ℓ pedig ℓ db prímszám szorzata. ℓ egy globális állandó.

18 Kongruencia fogalma, teljes és redukált maradékrendszer, ϕ-függvény, Euler-Fermat tétel, Wilson-tétel.

Definíció $a \equiv b \; mod\, c$ azt jelenti, hogy a és b egészek c-vel való osztásakor ugyanaz a maradék.

Definíció $n \in \mathbf{N}$ teljes maradékrendszere $\{0, 1, \ldots, n-1\}$.

Definíció $n \in \mathbf{N}$ redukált maradékrendszere n RMR-ének n-hez relatív prím elemei.

Definíció Az Euler féle $\varphi(n)$ függvény az n-nél kisebb, n-hez relatív prímek számát jelenti, azaz $\varphi(n) = |RMR|$.

Tétel

$$\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

Állítás Ha n RMR-e: $\{a_1, \ldots, a_{\varphi(n)}\}$ és a egy $(a, n) = 1$-et teljesítő elem, akkor az $aa_1, \ldots, aa_{\varphi(n)} \; mod\, n$ elemek megint n RMR-ét adják.

Tétel (Euler-Fermat) Tetszőleges $n \in \mathbf{N}$-re $(a, n) = 1$ esetén fennáll

$$a^{\varphi(n)} \equiv 1 \; mod\, n$$

Tétel (Wilson)

$$(n-1)! \equiv \begin{cases} -1 & \text{ha } n \text{ prím} \\ 0 & \text{ha } n \text{ összetett} \\ 2 & \text{ha } n = 4 \end{cases} \quad mod\, n$$

19 Lineáris kongruenciák megoldása.

Tétel (Műveletek) Általános alak: $ax \equiv b \; mod\, c$

- a, b szorozható és osztható c-hez relatív prímekkel
- a, b, c szorozható és osztható ugyanazzal a számmal
- A kongruencia átalakítható $ax = b + kc$ alakú egyenletté és viszont.

Tétel A megoldhatóság szükséges és elégséges feltétele $(a, c)|_b$.

20 Aritmetikai algoritmusok bonyolultsága, prímtesztelés, nyilvános kulcsú titkosírások.

21 Művelet, félcsoport, csoport, példák.

Definíció $(G, \cdot)$ **csoport**, ha

1. a művelet nem vezet ki a halmazból
2. a művelet asszociatív: $\forall a, b, c \in G \quad (ab)c = a(bc)$
3. létezik egységelem: $\exists e \in G \quad \forall g \in G \quad eg = ge = g$
4. minden elemnek létezik inverze: $\forall g \in G \quad \exists g' \in G \quad gg' = g'g = e$

Definíció Csoport **rendje** a csoport elemszáma

Definíció $(G, \cdot)$ félcsoport, ha a csoportaxiómákat az inverz létének kivételével teljesíti.

Állítás Az egységelem és az inverz egyértelmű

Állítás Egyszerűsítési szabály: $ab = ac \quad \Leftrightarrow \quad b = c$

22 Elem rendje, ciklikus csoport, részcsoport, mellékosztály, Lagrange-tétel.

Definíció $(G, \cdot)$ csoportnak részcsoportja $(H, \cdot)$, ha $H \subseteq G$ és H is csoportot alkot ugyanazzal a művelettel. Jele: $H \leq G$.

Állítás Részcsoportok metszete is részcsoport.

Definíció Legyen $K \subseteq G$. A K **által generált részcsoport** a K-t tartalmazó legszűkebb részcsoport, azaz a K-t tartalmazó csoportok metszete. Jele: $\langle K \rangle$.

Definíció a elem **rendje** az a legkisebb kitevő, amelyre a-t emelve az egységelemet kapjuk. Ha nincs ilyen kitevő, akkor a rendje végtelen.

Definíció Az egy elem által generált csoport **ciklikus csoport**.

Definíció $H \leq G \quad a \in G$. Ekkor
H **baloldali,** a **szerinti mellékosztálya** $aH := \{ah : h \in H\}$
H **jobboldali,** a **szerinti mellékosztálya** $Ha := \{ha : h \in H\}$
a a mellékosztály **reprezentánsa**.

Állítás Legyen $H \leq G$. Ekkor

1. $a \in Ha$
2. a Ha mellékosztály minden eleme reprezentálja a Ha mellékosztályt

3. két különböző jobboldali mellékosztály vagy egybeesik, vagy diszjunktak.

4. ha H véges, akkor H bármely mellékosztályának rendje megegyezik H rendjével

Tétel (Lagrange) Legyen G véges, $H \leq G$. Ekkor H rendje osztja G rendjét.

Definíció A $|G|/|H|$ számot H G-beli indexének nevezzük. Jele: $|G : H|$

23 Normálosztó, faktorcsoport, homomorfizmus-tétel.

Definíció Legyen $N \leq G$. N **normálosztó** G-ben, ha N jobb- és baloldali mellékosztályai megegyeznek. Jele: $N \triangleleft G$.

Tétel Egy normálosztó mellékosztályai csoportot alkotnak a halmazszorzás műveletére nézve.

Definíció G csoport N normálosztójának mellékosztályait és a halmazszorzás műveletét együtt G N-szerinti **faktorcsoport**jának nevezzük. Jele: G/N. Elemszáma egyenlő N G-beli indexével.

Definíció A $\phi : G_1 \to G_2$ csoportok közti leképezést **homomorfizmus**nak nevezzük, ha G_1 minden elemén értelmezve van és művelettartó, azaz $\phi(ab) = \phi(a)\phi(b)$.

Definíció

$$\begin{aligned} Ker(\phi) &= \{g \in G_1 : \quad \phi(g) = 1_{G_2}\} \\ Im(\phi) &= \{g \in G_2 : \quad \exists h \in G_1 \quad \phi(h) = g \end{aligned}$$

Állítás Homomorfizmusnál egységelem képe egységelem, inverz képe a kép inverze, a kép részcsoport, a mag normálosztó.

Tétel (Homomorfizmus tétel) Legyen $\phi : G_1 \to G_2$ homomorfizmus. Ekkor

$$G_1/Ker(\phi) \simeq Im(\phi)$$

azaz a mag, mint normálosztó szerinti faktorcsoport izomorf a képpel.

24 Permutációcsoportok, Cayley-tétel.

25 Gyűrűk, testek.

Credits Ezt a dokumentumot a szerző feltüntetésével bárki szabadon terjesztheti. Felhasznált irodalom: Dr Simonyi Gábor óráinak jegyzete, Katona-Recski-Szabó: Gráfelmélet, algoritmuselmélet, algebra.