Szóbeli tételek

1, Leszámlálások

Ismétlés nélküli:

permutáció: n elem sorbarendezése ismétlése nélkül

variáció: Def: Legyen $n \in \mathbb{N}$. Ekkor n elem egy permutációja az n db, egymástól megkülönböztethető elem egy sorbarendezését jelenti.

variáció: Legyen $k, n \in \mathbb{N}$, $0 \leq k \leq n$. Ekkor n elem k-adosztályú variációján n elemből kiválasztott egymástól megkülönböztethető k különböző elem egy sorrendjét értjük.

kombináció: $k, n \in \mathbb{N}$, $k \leq n$ esetén n elem k-adosztályú kombinációján egy n elemből álló halmaz k elemű részhalmazait értjük.

Ismétléses

permutáció: Legyen $k_1 \dots k_L \in \mathbb{N}$ rögzített számok, és $n = \sum_{i=1}^{L} k_i$. Ekkor n elem ismétléses permutációján az k féle elem egy n hosszú sorrendjét értjük, amiben az i-edik elem pontosan k_i-szer jelenik meg, ha $1 \leq i \leq L$.

variáció: n elem k-adosztályú ismétléses variációja alatt egy olyan k hosszú sorozatot értünk, amelynek tagjai n db egymástól megkülönböztethető elemek közül kerülnek ki, bármelyik elemet tetszőlegesen sokszor felhasználva.

Kiválasztás

	minden	$k-t$
	permutáció	variáció
Számít	$\frac{n!}{(\sum k_i)!}$	$\frac{n!}{(n-k)!}$
	$\Pi(k_i!)$	n^k
Számít nem számít	1	kombináció $\binom{n}{k} = \frac{n!}{k!(n-k!)}$
		$\binom{n+k-1}{k}$ =

~~$\frac{(n+k-1)!}{k!(n+k-1)!}$~~ + példák!

kombináció: n elem k-adosztályú ismétléses kombinációja n féle elemtípusból k db kiválasztást jelenti, ahol bármely típusból tetszőlegesen sokat választhatunk.

Binomiális tétel: (Newton)

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i$$

Bizonyítás: kiválasztás az $(a+b)(a+b)(a+b)\ldots$ szorzatból

2. Gráfelmélet alapfogalmai

Gráf: $G=(V;E)$ pár
pont: a gráfot véges alkotó nem üres halmaz elemei
él: a pontokból képezhető

Def: $G = (V(G), E(G))$ egy egyszerű gráf, ha $V \neq \emptyset$ és $E \subseteq \{\{u,v\} \mid u,v \in V, u \neq v\}$

$V(G)$ jelöli a G gráf csúcsainak/pontjainak a halmazát, $E(G)$ pedig a gráf éleinek halmazát. A gráf véges, ha $V(G)$ véges halmaz.

Fokszám: $d(v)$ ahol $v \in V(G)$: a v végpontú élek száma, (hurokél kétszer számít)

Tétel: $\sum d(v) = 2|E|$

G minimális fokszáma: $\delta(G)$

G maximális fokszáma: $\Delta(G)$

Ha $\delta(G) = \Delta(G) = k \Rightarrow G$ k-reguláris

Izomorfia: $G_1(V_1, E_1)$, $G_2(V_2, E_2)$ izomorfak, ha létezik $f: V_1 \to V_2$ bijekció, amelyre:

$$\{x,y\} \in E_1 \iff \{f(x), f(y)\} \in E_2$$

jelölés: $G_1 \cong G_2$

Megoldási idő: $2n!\binom{n}{2}$

Ellenőrzési idő: $2\binom{n}{2}$

Élsorozat: $(v_0, e_1, \dots e_n, v_n)$ sorozat, ahol $e_i = \{v_{i-1}, v_i\}$, $\forall v_i \in V(G)$, $\forall e_i \in E(G)$

Séta: élsorozat minden él különböző

Út: séta, minden pont különböző

Nyílt séta: $v_0 \neq v_n$, Zárt séta: $v_0 = v_n$.

Kör: zárt séta, minden más pont különböző

Összefüggő, körmentes gráf: $|E| = |V| - 1$

Erdő: fa komponenseiből álló gráf

Teljes gráf: K_n, körgráf: C_n, út: P_n

Páros gráf ("teljes"): $K_{a,b}$

Részgráf: G_1 részgráfja G_2-nek, ha

$V(G_1) \subseteq V(G_2)$, és $E(G_1) \subseteq E(G_2)$ és

$\forall \{u, v\} \in E(G_2)$: $u, v \in V(G_2)$.

Feszített részgráf: $V(G_1) = V(G_2)$

Komponens: maximális él- és pontszámú összefüggő részgráf

Fák tulajdonságai:

két levél: minden fában $\exists$ legalább 2 db 1 fokszámú csúcs (ha $|V(G)| \geq 2$)

$\forall$ összefüggő gráfban létezik feszítőfa

3. Minimális költs. feszítőfa

Kruskal-algoritmus: lefutási idő: ~~O(e)~~ $C \cdot e$

0.: $F \leftarrow \emptyset$
1.: $X \leftarrow \{e \mid e \in E, e \notin F, F \cup \{e\}$ körmentes $\}$
$X == \emptyset \Rightarrow$ stop, eredmény F
2.:
3.: legyen $e_0 \in X : \forall e \in X : k(e_0) \leq k(e)$
$F \leftarrow F \cup \{e_0\} \rightarrow$ ugrás 1.

input: G gráf, $k : E(G) \rightarrow \mathbb{N}$ fgv.
output: ~~fa~~ min. költs. feszfa.

~~Tétel~~ Kruskal-tétel: tetszőleges öf. G gráfon a Kruskal algoritmus megtalálja a min. költs. fesz. fát.

Vágás: $Q \subseteq E(G)$ egy vágás, ha $G-Q$ nem összefüggő, de $\forall X \subset Q : G-X$ összefüggő

Normál fa: Áramkör, mint öf. gráf, csúcsok ekvipot. pontok, ~~öf. G gráf~~ minden éle fesz.forrás (1), áramforrás (5), ellenállás (3), kondi (2), tekercs (4) F feszítőfa normálfa, ha F tartalmaz minden fesz. forrást, nem tartalmaz áramforrást, minimális számú tekercset és maximális számú kondit tartalmaz.

- A feszültségforrások részgráfja körmentes kell legyen
- az áramforrások részgráfja vágásmentes kell legyen
↳ az áramforrásokat elhagyva G öf. marad. (Kruskal-alg.)

4. Euler-séta, H-kör

E-séta: minden élt pontosan egyszer tartalmazó séta (nyílt, zárt)

Tétel: G gráfban pontosan akkor van zárt E-séta, ha $\forall v \in V(G)$: $d(v)$ páros, és G ö.f.

Biz: Szükséges: triviális, ahova bemegyünk onnan ki is kell jönni.

Hamilton-kör (út): minden ponton pontosan egyszer áthaladó kör (út).

Ha $\exists$ H-kör (út) $\Rightarrow \forall X \subseteq V(G)$: $G-X$ komponenseinek száma $\leq |X|$ $(|X|+1)$

Biz: Ha G egy H-kör: triviális, egyébként csak kevesebb komp. lehet

Dirac-tétel: Ha G n pontú egyszerű gráf, és $\forall d(v) \geq \frac{n}{2} \Rightarrow \exists$ H-kör. (elégséges)

Ore-tétel: n pontú G egyszerű gráfban létezik H-kör, ha $\forall a, b \in V(G)$-re ha $d(a)+d(b) < n$ akkor $\{a, b\} \in E(G)$. (elégséges)

Biz: Dirac-tétel: Ore-tételből következik. (Ha teljesül a Dirac-tétel, akkor teljesül az Ore tétel is → az Ore tétel erősebb)

Szintes algoritmusok

- M.Ló algoritmus = Kruskal
- BFS: $l(e)=1$
- Ford: $l(e) \in \mathbb{R}$
- Floyd: dist(u,v) $\forall u,v$-re
- Dijkstra: $l(e) \in \mathbb{R}^+$

legegyszerűbb ötlet: módosított Kruskal-alg.

Mohó algoritmus = Kruskal alg. lépésszám: c·e

Inp: $G(V,E)$, $k(e) \in \mathbb{R}^+$ költség

out: Min. költs. feszítőfa

0.: $E = \{e_1, e_2, \dots e_m\}$, $\forall i < m-1 : k(e_i) \le k(e_{i+1})$

$F_m = \emptyset$, $i = 1$

1.: $F_m = \begin{cases} F_m \cup \{e_i\} & \text{ha } F_m \cup \{e_i\} \text{ körmentes} \\ F_m & \text{ha } F_m \cup \{e_i\} \text{ tartalmaz kört} \end{cases}$

$i++$

2.: ha $i > n$: STOP

BFS: lépésszám: $c \cdot (n+e)$

Inp: $\vec{G}(V;E)$, v_0

out: szélességi fa, elérési sorrend

Dijkstra: lépésszám: $c \cdot n^2$

Inp: $\vec{G}(V;E)$ $l(e) \to \mathbb{R}^+$, v_0

out: dist(v_0, v) $\forall v$-re, legrövidebb utak fája

0. $d(v_0) = 0$, $\forall x \in V \setminus \{v_0\} : d(x) = \infty$

$X \in \{v_0\}$, $Y \in V \setminus \{v_0\}$, $c \in v_0$

1. $\forall b \in Y$: $d(b) \leftarrow \min(d(b), dist(c) + l(c,b))$

2. $y_0 \in Y$: $\forall y \neq y_0 \in Y$: $d(y_0) \leq d(y)$

$X \leftarrow X \cup \{y_0\}$; $Y \leftarrow Y \setminus \{y_0\}$; $c \in y_0$ ~~$dist(x) = d(x)$~~ $dist(c) \leftarrow d(c)$

3. Ha $|Y| = 0$: STOP, és

különben jump 1.

bejárások: $c \cdot n \cdot e$

Ford:

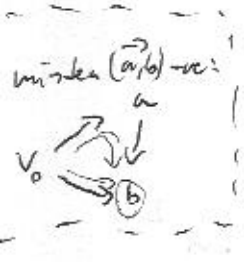
Inp: $\vec{G}(V, E)$, $l(e) \to \mathbb{R}^+$, v_0 ($\vec{G}$-ben nincs negatív hosszú kör)

Out: $dist(x) = \min_{v_0 \to x} \sum_{e \in (v,x) \in v,x\text{-út}} l(e)$: $\forall x$-re

0. $d(v_0) \leftarrow 0$, $\forall x \neq v_0$: $d(x) \leftarrow \infty$, $i \leftarrow 0$

1. $\forall e$: legyen $e \in (a,b)$ $d(b) \leftarrow \min(d(b), d(a) + l(e))$

Ha $i < n$: $i{+}{+}$ jump 1 (csinos n-szer)



2. $dist(x) \leftarrow d(x)$ $\forall x$-re, STOP

bejárások: $c \cdot n^3$

Floyd:

Inp: $G(V, E)$, $l(e) \to \mathbb{R}$

Out: $dist(u, v)$ $\forall u, v \in V$-re $d_0(v_i, v_j) = \infty$ ha $v_i v_j \notin E$

$d_0(v_i, v_j) = l(v_i, v_j)$ ha $v_i v_j \in E$

$d_{k+1}(v_i, v_j) = \min\left[d_k(v_i, v_j), d_k(v_i, v_k) + d_k(v_k, v_j)\right]$

~~Ha $k = n$: STOP~~ $\forall v_i, v_j$: $dist(v_i, v_j) \leftarrow d_n(v_i, v_j)$

A számítástudomány alapjai 2015. I. félév

3. gyakorlat. Összeállította: Katona Gyula (kiskat@cs.bme.hu)

Tudnivalók

Def: Ha $G = (V, E)$ egy gráf és $k : E \to \mathbb{R}_+$ az éleken értelmezett költségfüggvény, akkor G tetszőleges G' részgráfjának *költsége* a $E(G')$ élhalmazbeli élek költségeinek összege.

Kruskal algoritmus: Input: $G = (V, E)$ összefüggő gráf és $k : E \to \mathbb{R}_+$ költségfüggvény. Output: $F = F_m$ a G egy minimális költségű feszítőfája.

Működés: Legyen $E = \{e_1, e_2, \ldots, e_m\}$, és $k(e_1) \leq k(e_2) \leq \ldots \leq k(e_m)$. Legyen $F_0 = \emptyset$, és

$$F_{i+1} := \begin{cases} F_i \cup \{e_i\} & \text{ha } F_i \cup \{e_i\} \text{ körmentes} \\ F_i & \text{ha } F_i \cup \{e_i\} \text{ tartalmaz kört.} \end{cases}$$

Tétel: A Kruskal algoritmus által kiszámított $F = F_m$ élhalmaz a G egy min ktgű feszítőfája.

Def: A $G = (V, E)$ (irányított vagy irányítatlan) gráf egy *bejárásán* a V-beli csúcsok végiglátogatását értjük, ahol a alábbiak szerint. A csúcsok állapota kezdetben *eléretlen*, idővel *elértté* válik, a bejárás végére pedig *befejezett* lesz (mégpedig akkor, amikor észrevesszük, hogy onnan már nem tudunk újabb csúcsot elérni). A fő szabály, hogy az újonnan elért csúcsot –ha lehetséges– mindig már korábban elért csúcsból induló él mentén elérni. Ha ez nem lehetséges, de még van eléretlen csúcs, akkor tetszőleges eléretlen csúcs lehet a következőnek elért csúcs. (Irányítatlan gráf esetén minden élt oda-vissza irányított élnek tekintünk.) A bejárás során kialakul a csúcsok egy elérési ill. egy befejezési sorrendje, továbbá minden csúcshoz feljegyezzük azt is, hogy melyik él mentén értük el. Ez utóbbi élek az ún. *faélek*, és a bejárás *fáját* alkotják (ami egyrészt lehet irányított, másrészt pedig erdő).

Def: A *szélességi bejárás* (BFS) inputja a $G = (V, E)$ gráf és egy r gyökércsúcs. Az ouptut egy r-ből induló bejáráshoz tartozó ún. *szélességi fa* (a bejárás fája) és egy elérési sorrend. A bejárás az fenti szabály azon kiegészítésével történik, hogy a következőnek elért csúcsot mindig a lehető legkorábban elért csúcsból kell elérnünk. (Ezért a BFS bejáráshoz tartozó elérési sorrend megegyezik a befejezési sorrenddel.)

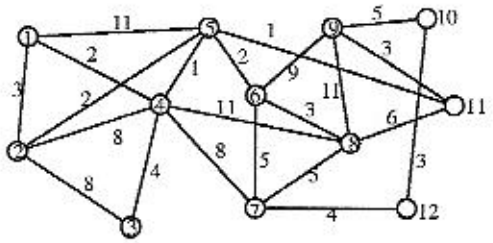
Tétel: A BFS bejárás fája az r csúcsból minden más csúcsba a G gráf egylegrövidebb (legkevesebb élből álló) legrövidebb útját tartalmazza, azaz tetszőleges v csúcs G-beli távolsága r-től megegyezik az r gyökerű szélességi fán mért távolsággal.

Tétel: A szélességi bejárás lépésszáma legfeljebb $konst \cdot (n+m)$, ahol n a G csúcsainak, m pedig G éleinek száma.

Def: Adott $G = (V, E)$ (ir) gráf és egy $l : E \to \mathbb{R}$ élhosszfv. Egy G-beli (ir) út hossza az út éleinek összhossza. $dist(u, v)$ jelöli az (ir) uv utak közül a legrövidebb hosszát.

Def: Adott $G = (V, E)$ (ir) gráf, $u \in V$ és egy $l : E \to \mathbb{R}$ élhosszfv. Tegyük fel, hogy $d(v) \geq dist(u, v)$ teljesül G minden v csúcsára. Az $e = vw$ *él menti javítás* azt jelenti, hogy a $d(w)$ értéket a $\min\{d(w), d(v) + l(vw)\}$ értékkel helyettesítjük. (Ha minden élhossz nemnegatív, akkor $d(w) \geq dist(u, w)$ az él menti javítás után is teljesülni fog.)

Gyakorlatok



1. Keressünk az alábbi gráfban minimális költségű feszítőfát! Hány minimális költségű feszítőfája van a gráfnak?
2. Adott a $G = (V, E)$ gráf és az élein egy $k : E \to \mathbb{R}_+$ költségfüggvény. Tegyük fel, hogy ismerünk a $G - e$ gráfon egy minimális költségű F feszítőfát. Határozzuk meg a G gráfnak egy olyan minimális költségű feszítőfáját, amelynek F-fel a lehető legtöbb közös éle van.
3. Abszurdisztán kormánya tendert ír ki n településnek a helyi vízműre történő rácsatlakoztatására. Minden ajánlat két település (vagy egy település és a vízmű) között kiépítendő vezeték

költségét tartalmazza. Tudjuk, hogy a kormány úgy választja ki a megépítendő vezetékeket és az azokat építő egyes vállalkozásokat, hogy a lehető legolcsóbban csatlakozzon az n település a vízműhöz. Cégünk különféle homályos üzletek nyélbeütésével igen olcsón meg tudná építeni a Rátótot és Piripócsot összekötő vezetéket, ráadásul minisztériumi kapcsolatunk, Mutyi bácsi elárulta nekünk az összes beérkezett ajánlatot. Hogyan árazzuk a saját Rátót-Piripócs ajánlatunkat, hogy a lehető legnagyobbat szakítsuk?

4. Legyenek a gráf $e_1, e_2, \ldots$ élei egymástól függetlenül rendre $p_1, p_2, \ldots$ valószínűséggel meghibásodó telefonvonalak. A feszítőfák közül keressük meg azt, melynek a legnagyobb a megbízhatósága (tehát melyre maximális annak a valószínűsége, hogy egyik él sem hibásodik meg).
5. Törpfalván kitört a járvány: csúf kórság fertőzött meg néhány törpöt. Szerencsére a betegségből minden törp egy nap alatt meggyógyul, és ezután egy napig immunissá válik, ám sajnos ezt követően újra fertőződhet. Kellemetlen, hogy a törpök még betegen sem adják fel azt a megrögzött szokásukat, hogy minden egyes nap minden barátjukat meglátogatják. Márpedig ha beteg és nem immunis törp találkozik, az utóbbi bizonyosan megfertőződik. Mutassuk meg, hogy ha Törpfalván 100 törp él, akkor a járványnak a kitörését követő 101-dik napon már bizonyosan vége van. Legfeljebb hány napig tarthat a járvány akkor, ha a törpök időközben újabb ismeretséget is köthetnek?
6. Egy városban 1000 ember lakik. Mindenki minden nap elmondja az ismerőseinek az összes előző nap megtudott hírt. Előbb-utóbb mindenki megtud mindent. Bizonyítsuk be, hogy van 90 olyan ember, hogy ha ők egyszerre megtudnak valamit, akkor legkésőbb 10 nap múlva mindenki megtudja!
7. Adjunk hatékony algoritmust, aminek a bemenete egy n csúcsú összefüggő irányítatlan gráf, a kimenet pedig egy olyan gráfcsúcs, amiből minden más csúcs lefeljebb $n/2$ élű úton elérhető.

5. Legrövidebb utak

Szélességi bejárás (BFS) algoritmus:

G gráfban $v \in V(G)$-ből minden ponthoz megadja a távolságát: egy pont először elérhetetlen, majd elért, végül befejezett lesz

Lefutási idő: $c \cdot (e + n)$

Minimális távolság: dist(u, v)

Konzervatív hosszfüggvény: nincs negatív kör

Dijkstra: lépésszám: $c \cdot n^2$ ir. gráf súly $k \in \mathbb{R}^+$

Ford: $c \cdot n \cdot e$ irányított gráfban, $k \in \mathbb{R}$

Floyd: $c \cdot n^3$ minden pontpárra

Szélesség függvény: $w: E \to \mathbb{R}^+$

Az út szélességét a legkeskenyebb él szélessége határozza meg.

Algoritmus: Kruskal algoritmus módosítása irányítatlan gráfnál, Dijkstra módosítása irányított gráfnál.

„jóslás" fgv. definiálása: monoton konzisztens rendezés G gráf útjain

Bejárási fa: Egy gráf pontjait egy csúcsból indulva, egymás után a gráf éleinek mentén látogatjuk végig és feljegyezzük a sorrendet, valamint azt tároljuk el, hogy melyik élen jutottunk el az egyes csúcsokba. Ezek az élei a fa élei. Ezek határozzák meg a bejárás fáját.

Előrefelé: ősből leszármazottba vezető él.
Visszafelé: előrefelé futó él
A többi él keresztél.

6. Mélységi keresés (DFS) Lépésszám: $C(n+e)$

Input: $\vec{G}(V, \vec{E})$ irányított gráf, és $v_0 \in V$
output:
- mélységi fa
- előrési sorrend mélységi száma ($m(x)$)
- csúcspont ősei
- befejezési szám

élek osztályozása: előrefelé $m(x) < m(y)$ (eredeti éllistában)
$x \to y$ él: visszafelé $m(y) \leq m(x)$ (leszármazottba)
keresztél: $m(x) > m(y)$ (nem leszármazott)

Def: A $\vec{G}$ gráf aciklikus, ha nincs benne irányított kör (=DAG)

Topologikus sorrend: $v_1, v_2 \dots v_n$ top. sorrend, ha csak kisebb indexű pontból nagyobb indexűbe fut él.

Tétel: Ha G DAG, akkor a DFS utáni befejezési sorrendek fordítottja topologikus sorrend.

Ha G DAG, ~~akkor~~ $\Leftarrow\!\!\!\Rightarrow$ G mélységi bejárásakor nem keletkezik visszaél. $\Leftarrow\!\!\!\Rightarrow$ ~~tétt~~ $\exists$ G topologikus sorrendje (befejezés fordítottja)

PERT-módszer:

F feladat ütemezése

P(F) irányított gráf, aciklikus kell legyen

$c: E(P(F)) \to \mathbb{R}^+$

Az u kritikus tevékenység, ha a feladatban ~~befejezési~~ szükséges idő ~~ideje~~ függ az u kezdési idejétől.

Feladat kezdési ideje: $k(v)$

Első ~~feladat~~ tevékenység ~~tervezett~~: $k(s) = 0$

Minden $\vec{uv}$ élre: $k(v) \geq k(u) + c(\vec{uv})$

Elvégzéshez szükséges idő: $k(t) = \max_{v \in V(F)} k(v) = h(F)$ (t: utolsó tevékenység)

Az F feladat hossza megegyezik az irányított $\vec{st}$ utak súlyának maximumával.

u tev. kritikus $\Leftarrow\!\!\!\Rightarrow$ $\exists\, h(F)$ súlyú $\vec{st}$ ir. út, hogy $u \in \vec{st}$

A P(F) h(F) súlyú irányított $\vec{st}$ útjait kritikus útnak nevezzük.

Alapkörrendszer: $\{F \cup \{u,v\}, \mid u,v \in V(F), u \neq v, \{u,v\} \notin E(F)\}$ (fa; annak köre)

~~(Egy fához minden lehetséges~~

Ha egy fához minden lehetséges módon hozzávesszük még egy élt, akkor a keletkező körök unióját a gráf adott fájához tartozó alapkörrendszerének hívjuk.

7. Gráfok színezése

$f: V(G) \to \text{szín}$ (nincs kavarás)

ha $u, v \in V(G), \{u,v\} \in E(G) \Rightarrow f(u) \neq f(v)$

Kromatikus szám: legkisebb színkészlet színszáma

$$\chi(G) = \min\left|\{f(v) \mid \forall v \in V(G)\}\right|$$

Klikkszám: a gráfban lévő maximális teljes részgráf pontjainak a száma: $\omega(G)$

$\forall G$-re: $\omega(G) \leq \chi(G) \leq \Delta(G) + 1$

$\chi(G) \cdot \alpha(G) \geq n$

$(\chi(K_n) = n)$

$\forall$ síkbarajzolható gráfra: $\chi(G) \leq 4 \leq 5 \leq 6$

$\chi(G) \leq 2 \iff G$-ben nincs páratlan hosszú kör

$\equiv G$ páros gráf

8. Hálózati folyamok

Hálózat: $(\vec{G}, s, t, c)$

s: kezdő/forrás, $s \in V(G)$ (source)

t: végső/nyelő, $t \in V(G)$ (target)

c: kapacitás függvény $c: E(G) \to \mathbb{R}^+$

f: folyam $f: E(G) \to \mathbb{R}^+$

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

Kirchhoff-törvény:

$$\sum_{\forall e\text{ v-be}} f(e) - \sum_{\forall e\text{ v-ből}} f(e) = \begin{cases} 0 & \text{ha } v \neq s,t \\ m(f) & \text{ha } v = s \\ -m(f) & \text{ha } v = t \end{cases}$$

Folyamnagyság: $m(f)$

st-vágás/vágat: legyen X a G csúcsainak s-t tartalmazó, de t-t nem tartalmazó részhalmaza. Ekkor az X és $G-X$ közötti éleket st-vágásnak nevezzük. A vágás kapacitása az élek kapacitásösszege.

Ford-Fulkerson tétel: Ha G egy véges hálózat, akkor $\exists f$ folyam és $s \in X \subseteq V(G) - \{t\}$ részhalmaz, hogy $m(f)$ folyamnagyság azonos az X által definiált st-vágás kapacitásával. ($\Rightarrow \exists m_f$ maximális folyam)

Biz: javító utas algoritmus

(másnéven: Kantorovics / maxflow-minflow tétel)

Javító utas algoritmus: segédgráf: $\overrightarrow{H_f}$ $V(H_f) = V(G)$

Ha $\overrightarrow{(u;v)} \in E(G)$ és $f(\overrightarrow{uv}) < c(\overrightarrow{uv})$:

$E(H_f) \leftarrow \overrightarrow{uv}$, $c_f(\overrightarrow{uv}) \leftarrow c(\overrightarrow{uv}) - f(\overrightarrow{uv})$

Ha $\overrightarrow{(u;v)} \in E(G)$ és $f(\overrightarrow{uv}) > 0$:

$E(H_f) \leftarrow \overrightarrow{vu}$; $c_f(\overrightarrow{vu}) \leftarrow f(\overrightarrow{uv})$

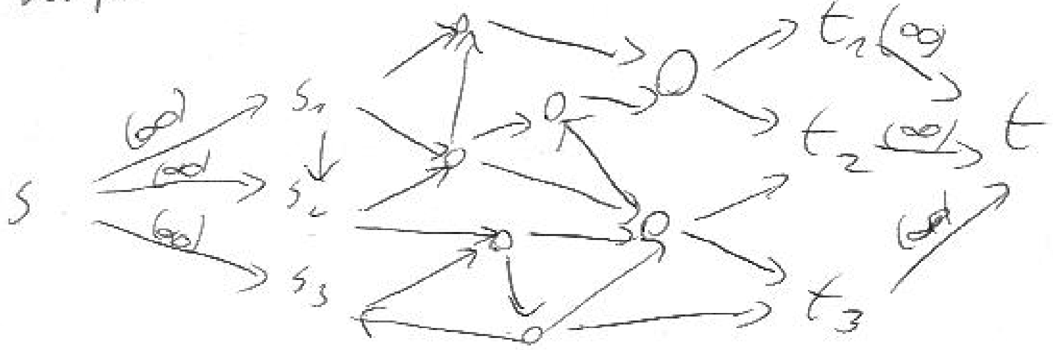
Ha $\exists$ $\overrightarrow{st}$ ir. út H_f-ben akkor lehet javítani.

Edmonds–Karp tétel: Ha mindig a legkevesebb élből álló javítóutat választjuk, akkor az algoritmus $c \cdot n^3$ lépésben véget ér, és legfeljebb ~~[illegible]~~ $n \cdot e$ javítást kell végezni.

Egészértékűségi lemma: Ha ~~$\forall v \in V(G)$: c(~~
Ha $\forall e \in E(G): c(e) \in \mathbb{Z} \Rightarrow \exists f: \forall e \in E(G): f(e) \in \mathbb{Z}$ és f maximális.

Biz: Kezdetben $\forall e \in E(G): f(e) = 0$, minden javítással ~~[illegible]~~ egész értékekkel változik

2a Szuperforrás, szupernyelő:



Csúcskapacitás:

9. Páros gráfok

Párosítás: gráf csúcsainak párba állítása élek mentén

$M \subseteq E(G)$ egy párosítás, ha semelyik két M-beli élnek nincs közös végpontja

Egy párosítás maximális, ha nincs olyan másik párosítás, amiben ennél több pontja van.

Teljes párosítás: minden pontnak van párja.

A-t fedő párosítás: minden A-beli pontnak van párja.

páros gráf: G csúcsai két diszjunkt halmazra bonthatók úgy, hogy minden él a két halmaz közötti fut $\equiv$ G kiszínezhető két színnel ($\chi(G) \leq 2$) $\equiv$ G nem tartalmaz páratlan hosszú kört ($\Rightarrow$ ha páros)

X beli elemek lehetséges szomszédainak halmaza $N(X)$.

Hall-tétel: Egy G gráfban $\exists A$-t fedő párosítás,

$$\iff \forall X \subseteq A : |N(X)| \geq |X|$$

(Bizi alkalmas utas algoritmus)

Frobenius-tétel: G páros gráfban $\exists$ teljes párosítás $\iff |A| = |B|$ és $\forall X \subseteq A : |N(X)| \geq |X|$

Alternáló utas algoritmus:
kiindulunk az üres párosításból, és javítóutakat keresünk. Segédgráf: egy meglévő M párosításhoz M éleit irányítjuk A-ból B-be, G−M élei irányítsuk B-ből A-ba.

<u>Alternálóút:</u> fedetlen A-ból fedetlen B-be futó irányított út a segédgráfban.

Az alternálóút M-beli éleit vegyük ki M-ből, és az azon kívüli éleit pedig vegyük bele, így M-nél eggyel nagyobb párosítást kapunk.

Ha nincs alternáló út, akkor M maximális párosítás.

	max. független	min. lefogó	Gallai-t.
pont	α	τ	$\nexists$ hurok: $\alpha + \tau = n$
él	ν	ρ	$\nexists$ izopont: $\nu + \rho = n$

Páros gráfra: $\alpha = \rho$, $\nu = \tau$ } Kőnig-tétel

Véges G gráfra:
$\nu \leq \tau \leq 2\nu$, $\alpha \leq \rho$, Ha G egyszerű: $\alpha(G) = \omega(\bar{G})$

$\nu \leq \frac{1}{2}|V|$

maximális párosítás: $|M| = \nu$

Független ponthalmaz: nem feszít élt

Lefogó ponthalmaz: G minden élének van végpontja benne

Független élhalmaz: végpontjaik különbözők

Lefogó élhalmaz F: $V(F) = V(G)$

10. Síkbarajzolhatóság

A G gráf síkbarajzolható, ha létezik olyan síkbeli diagramja, amiben az élek csak a végpontokban metszik egymást.

G síkbarajzolható $\Leftrightarrow$ G gömbbarajzolható

Sztereografikus projekció: A D a gömb és a sík érintési pontja, $\bar{E}$ a gömbön ezzel átellenes pont. $\forall P_{\neq \bar{E}}$ gömbfelület: $\exists !$ egyenes, ami P' síkon és $\bar{E}, P, P' \in e$, és ha $P = \tilde{P}$ akkor $P' = \tilde{P}'$.

$\Rightarrow$ $\exists !$ bijekció a gömbfelület $\bar{E}$-t kivéve.

Lehet a gömböt úgy forgatni, hogy $\bar{E}$ ne legyen pontja.

G-nek vagy G éleinek. (szögtartó transzformáció)

Ha G síkbarajzolható, és egy síkbarajzolásnál T belső tartomány, akkor $\exists$ síkbarajzolás ahol T külső tartomány. Biz: gömbfelületen minden külső tartomány

Euler-féle poliédertétel: Ha G síkbarajzolt gráf $\Rightarrow$ $n + t = e + k + 1$

Ha G összef.: $n + t = e + 2$ (Euler)

n: pontok száma
t: tartományok száma
e: élek száma
k: komponensek száma

Következmények:

- Ha G sr, bármely gráfelvágásnál egyszerű részgráfja van
- Ha G egyszerű, legalább 3 pontú sr. gráf, akkor $e \leq 3n - 6$

  $\Rightarrow K_5$ és $K_{3,3}$ nem sr.
- Ha G-nek nincs $\triangle$ lapja, akkor $e \leq 2n - 4$

(Bizonyítás)

- Ha G egyszerű sr. gráf, akkor $\delta(G) \leq 5$.

11. Kuratowski-tétel

Kuratowski-gráfok: K_5 és $K_{3,3}$ (nem sr.)

Soros bővítés: Egy él helyettesítése egy ponttal. pl:

(egy egyesítése)

(topologikus izomorfia)

- Egy e-él 2 hosszú úttal való helyettesítése
- Egy 2 hosszú út éllel való helyettesítése (kiszipsó pont fokszáma 2)

Kuratowski-tétel: Egy G gráf sr. $\Leftrightarrow$ ha G nem tartalmaz Kuratowski-gráf soros bővítését

Síkbarajzolt gráf duálisa:

G sr. gráf	$\Leftrightarrow$	G^* duális gráf
tartomány		pont
pont		tartomány
él		él
kör		vágás
vágás		kör
fa		fakomplementer
(egyszerű) párhuzamos él		soros él
soros él		párhuzamos él

~~$G^{**} = G$~~

~~Soros~~ Elvágó él: e él elvágó, ha $\{e\}$ vágás

Soros él: ha $\{e, e'\}$ vágás, akkor e és e' soros élek

párhuzamos él: két végpontjuk megegyezik (többszörös él)

Def: Legyen $G = (V, E)$ sr. gráf,

V^* a G lapjainak halmaza. Ekkor $G^* = (V^*, E^*)$

a G duálisa, ahol $E^* = \{e^* : e \in E\}$ és e^* az

e-t határoló tartományokat összekötő él.

$e = e^*$

$(v = t^*)$

$t = v^*$

~~A duális gráf~~

Tétel: Ha G^* a G duálisa,

akkor G^* sr. és öf.

12. Algoritmusok bonyolultsága

Egy algoritmus gyors, ha a lépések száma
$\leq p(\langle \text{input hossza} \rangle)$ (polinomidejű algoritmus)

Egy probléma könnyű, ha létezik rá gyors
algoritmus $\equiv$ P-beli probléma
Egy probléma nehéz, ha biztosan nem létezhet
rá gyors algoritmus $\equiv$ nem P-beli probléma

Az algoritmus x inputjának mérete egy
nemnegatív egész szám, az x méretének. Jele: $|x|$

Eldöntési probléma: $\forall$ inputra a válasz $\in \{\text{igen}, \text{nem}\}$
Keresési probléma: nem eldöntési probléma

Egy probléma NP-beli (co-NP beli) ha $\forall$ olyan
I inputra akkor a válasz igen (nem) létezik
olyan T tanú + plusz információ - amely
segítségével polinomidőben bizonyítható, hogy
a válasz tényleg igen (nem).
Futási idő: $\leq p(|I|+|T|)$, $|T| \leq p'(|I|)$

Karp redukció: (polinomiális visszavezetés)

Az X Karp-redukciója az Y problémára egy olyan polinom időben számolható f fgv. amely az X minden lehetséges bemenetéhez hozzárendeli az Y egy bemenetét úgy, hogy

$x \in X \Leftrightarrow f(x) \in Y$. Jelölés $X \prec Y$.

~~Ha Y polinomos ~~ Ha p-beli, akkor X is p-beli.

~~X NP-beli $\Rightarrow$ Y NP-beli~~

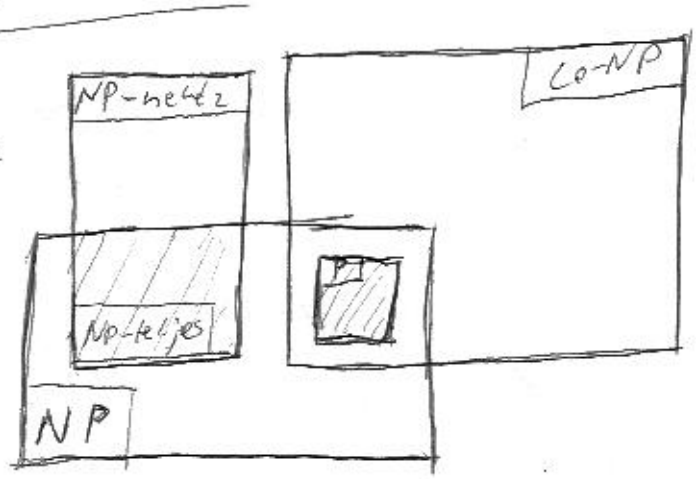
Ha $X \in P$ és $X \prec Y$ akkor $X \in P$.

Egy probléma NP-nehéz, ha minden NP-beli probléma polinomiális visszavezethető rá.

Egy probléma NP-teljes, ha NP-nehéz és NP-beli is.

Cook-Levin: Létezenek NP-teljes problémák. (SAT)

Döntési problémák:



$P \in NP \cap co\text{-}NP$

Sejtés: $P \neq NP$

Ha Π $\in$ NP-nehéz $\Rightarrow \forall \Pi' \in NP : \Pi' \prec \Pi$.

Példák:

P-beli: Euler-kör keresése (c.s.)

NP-beli: ~~Hamilton-kör keresése~~ G sr.? (tanú: G optimális színezésének költsége)
~~(tanú: Hamilton-kör maga)~~

Co-NP-beli: prímszám-e ~~n~~? (tanú: egy valódi osztó)

NP-teljes problémák:

SAT: input: f boole fgv. KNF (konjunktív alg. alakban)
kérdés: létezik-e $x_1 \dots x_n \in \{0,1\}$ hogy $f(x_1, \dots x_n) = 1$?

HAM: input: ~~G~~ gráf
kérdés: létezik-e Hamilton-kör a G-ben?
~~HAM ≤ 3-SAT~~ 3-SAT ≤ HAM

3-SAT ≤ 3-SZÍN

3-SZÍN: input: G gráf
kérdés: színezhető-e G 3-színnel?

k-SZÍN: ~~3-~~input: G-gráf, $k \in \mathbb{N}^+$, $k > 3$
kérdés: színezhető G k színnel?
~~3-SAT~~ 3-SZÍN ≤ k-SZÍN

MAXFTN: input: G gráf, $k \in \mathbb{N}^+$
kérdés: $\alpha(G) \geq k$
3-SZÍN ≤ MAXFTN

MAXKLIKK: input: G-gráf, $k \in \mathbb{N}^+$
kérdés: $\omega(G) \geq k$
MAXFTN ≤ MAXKLIKK

3-SAT: input: f 3-változós boole fgv. KNF-ben
kérdés: $\exists x_1, x_2, x_3 \in \{0,1\}$: $f(x_1, x_2, x_3) = 1$
SAT ≤ 3-SAT

13. Oszthatóság

a osztható b-vel, ha $\exists c : b \cdot c = a$

jelölés: $b \mid a$

Triviális osztók: $\forall n : n, 1 \mid n$

Valódi osztók: nem triviális osztók

Felbonthatatlan szám: az n szám felbonthatatlan, ha nincs valódi osztója, és $|n| \neq 1$.

Számelmélet alaptétele: ha egy n egész számra $|n| > 1$, akkor n előáll felbonthatatlan egész számok szorzataként, sorrendtől és előjelektől eltekintve egyértelműen.

$n = \prod_i p_i^{\alpha_i}$: kanonikus alak

Prímtulajdonságú szám: ha $n \mid ab \Rightarrow n \mid a \vee n \mid b$

akkor az n prímtulajdonságú.

A prímtulajdonságú számokat prímszámoknak hívjuk.

A számelmélet alaptételéből következik, hogy

A szám prím $\Leftrightarrow$ a felbonthatatlan

legnagyobb közös osztó: az a legnagyobb szám, ami osztója a-nak és b-nek is.

$(a, b) = \prod_i p_i^{\min(\alpha_i, \beta_i)}$

Legkisebb közös többszöröse az a legkisebb szám, amelynek az a és a b is osztója.

$$[a, b] = \prod_i p_i^{\max(\alpha_i, \beta_i)}$$

Egy szám osztóinak a száma: $\prod_i (\alpha_i + 1)$

Euklideszi algoritmus:

$$a = q_1 b + m_1$$

$$b = q_2 m_1 + m_2$$

$$m_1 = q_3 m_2 + m_3$$

$$\dots$$

$$m_n = q_{n+2} m_{n+1} + m_{n+2}$$

Ha $m_{n+2} = 0$ akkor $(a, b) = m_{n+1}$

Lépésszám: $O(\log_{10} b)$

Tétel: végtelen sok prímszám van

Biz: indirekt Tétel: tetszőlegesen sok egymást követő összetett szám van

Ikerprímek: két szomszédos páratlan szám, amik prímek $(2k-1, 2k+1)$ Sejtés: végtelen sok ikerprím van

Csebisev-tétel: $\forall n$-re: $\exists$ prímszám $\in [n, 2n]$

Dirichlet-tétel: $\{a + kb \mid (a, b) = 1, k \in \mathbb{N}^{+}\}$ végtelen sok prímet tartalmaz

$\pi(x) = \langle$ prímek száma $[2, x]$-ben $\rangle$

$$\lim_{x \to \infty} \pi(x) = \infty$$

Nagyprím-tétel: $\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1$

Goldbach-sejtés:

$n = p + q$

$\forall n = 2k + 2$-re

14. kongruencia

kongruencia: a kongruens b modulo m $\Leftrightarrow m \mid a-b$

jele: $a \equiv b \pmod m$, $a \equiv b \ (m)$

$a \equiv b \ (m)$, $c \equiv d \ (m) \Rightarrow a+c \equiv b+d \ (m)$, $b \equiv a \ (m)$

$a \equiv b \ (m) \Rightarrow ac \equiv bd \ (m)$

$ka \equiv kb \ (m) \Rightarrow a \equiv b \left(\frac{m}{(m,k)}\right)$

$a \equiv b \ (m) \Rightarrow da \equiv db \ (md)$

Lineáris kongruencia: $ax \equiv b \ (m)$

Megoldható $\Leftrightarrow (a,m) \mid b$

egyértelműen

Megoldás: $x \equiv c \ (m)$

Teljes maradékrendszer: (TMR): $\forall$ mod m maradékosztályból egy-egy tetszőleges szám

$\{a_1, a_2, \dots a_k\}$ = TMR (mod m) $\Leftrightarrow \forall i \neq j: a_i \not\equiv a_j \ (m)$ és $k = m$

Redukált maradékrendszer: (RMR) $\forall$ m-hez relatív prím mod m maradékosztályból pontosan egy számot tartalmaz

$\{a_1, \dots a_k\}$ RMR (mod m) $\Leftrightarrow \forall i \neq j: a_i \not\equiv a_j \ (m)$ és $(a_i, m) = 1$ és $k = \varphi(m)$.

Maradékosztály: $\forall m \geq 1$ esetén $\mathbb{Z}$ előáll m db halmaz diszjunkt uniójaként. Az egyes halmazokban azok a számok vannak, amik ugyanakkora maradékot adnak m-mel osztva.

Az i-edik halmaz: $\{i + km \mid k \in \mathbb{Z}\}$

Ezek az m szerinti maradékosztályok.

Euler-féle fgv: $\varphi(n)$

„Szép maradékosztályok" száma: a $0, 1 \ldots n-1$ számok között az n-hez relatív prímek száma

$$\varphi(n) = \left|\{i \mid 0 \leq i < n, (i, n) = 1, i \in \mathbb{Z}^+\}\right|$$

Ha p prím: $\varphi(p) = p - 1$

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

$$\varphi(n) = n \prod_i \left(1 - \frac{1}{p_i}\right) = \prod_i \varphi(p_i^{\alpha_i})$$

~~Ha p, q prím: $\varphi(p) \cdot \varphi(q) =$~~

Ha $(p, q) = 1$: $\varphi(p \cdot q) = \varphi(p) \cdot \varphi(q)$

Lineáris kongruencia: $ax \equiv b \ (m)$

~~pm~~ megoldható $\Leftrightarrow (a, m) \mid b$

Megoldásai: ~~(a,m)~~ (a, m) darab mod m maradékosztály

Módszerek:

- euklideszi algoritmus
- behelyettesítés, ha a TMR elég kicsi
- ekvivalens átalakítások
  - a, b helyettesítése kongruens számokkal
  - osztás
  - ~~[illegible]~~
  - ~~[illegible]~~

Euler - Fermat tétel:

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

Kis - Fermat tétel:

Ha p prím $\Rightarrow$ $a^p \equiv a \quad (p)$

15. Számelméleti algoritmusok

Számelméleti algoritmusok:

	egész számok	mod m
összeadás	lineáris	négyzetes
kivonás	lineáris	négyzetes
szorzás	négyzetes	négyzetes
osztás	négyzetes	poli.
hatványozás	exponenciális	poli.

Euklidészi algoritmus: polinomiális idejű $p(\log b)$

Prímtesztelés:

- Naiv. Eratoszthenészi-szita: 2^n
- Brute force $\sqrt{n}$-ig: $2^{\frac{1}{2}n}$
- Fermat-teszt: polinomiális

Fermat-teszt: Input: x kérdés: x prím-e?

Algoritmus:

0. Ha legyen $0 < a < x$ a véletlenszám
1. ha $a^{x-1} = 1 \ (x)$
2. legyen $0 < a < x$, új véletlenszám
3. ugrás 1.
4.

1. ha $(a, x) = 1$
2. ha $a^{x-1} \equiv 1 \ (x)$ (kis-Fermat tétel)
3. legyen a új random $0 < a < x$
4. ugrás 1 (maximum 300 körig)
5. különben: nem prím, STOP
6. különben nem prím, osztó: a, STOP

300 körök után:

$p(< x \text{ összetett} >) \leq \frac{1}{2^{300}}$

Lépésszám: polinom

Az a tanúja x-nek, ha $a^{x-1} \not\equiv 1 \ (x)$

Cinkos $a^{x-1} \equiv 1 \ (x)$

Ha x nem prím, és van tanúja, akkor legalább annyi tanúja van, mint cinkos.

Charmichael-féle szám: olyan összetett szám, aminek nincs tanúja, pl: $561 = 3 \cdot 11 \cdot 17$ (álprím)

RSA algoritmus

Legyen p, q prímek, $p \neq q$

Ekkor $N = p \cdot q$ $\varphi(N) = (p-1)(q-1)$

$e \cdot d \equiv 1 \ (\varphi(N))$ $(e, \varphi(N)) = 1$

$1 \leq e \leq N$

Nyilvános kulcsok: n, e

Privát kulcsok: p, q, d

Titkosítás: $C(x) = x^e \ (N)$ $\left(D = C^{-1}\right)$

Dekódolás: $D(y) = y^d \ (N)$

$D(C(x)) = x \rightarrow$ jól működik

- Kódolni bárki tud (nyilvános kulcs)
- Dekódolni csak a fogadó tud (privát kulcs)

Egyirányú függvény: $f: [1, n] \rightarrow [1, n]$ bijekció kattintással

számolható, de f^{-1} kiszámítása pontán f ismeretében nehéz.

Ha f^{-1} kiszámítható plusz információ egyértelműen kattintással, akkor f egy kiskapus egyirányú fgv.

pl.: $C(x)$

Nyilvános kulcsú titkosítás:

M üzenet kódolása számok segítségével.

Legyen Σ egy ABC, ennek a jeleivel írjuk le az üzenetet. Feltehető, hogy $M \in \Sigma^t$ (blokkokra bontható)

Feltehető, hogy Σ^t szavai 1 és $|\Sigma^t|$ közé eső természetes számoknak feleltek meg.

Nyilvános kulcsú titkosítási rendszer: f kiskapus egyirányú fgv. határozza meg, bárki képes kódolni, de csak a címzett képes dekódolni.

Digitális aláírás:

A

M üzenet

$z = D_A(M)$

$y = C_B(z)$ → y →

B

$z = D_B(y)$

$M = C_A(z)$

M üzenet

Titkos kulcsok felfedése nélkül igazolható az üzenet feladója.