VISZAA02 vizsgatematika
a Számítástudomány alapjai c. tárgyhoz
a 2014/2015-as tanév I. félévre

Nem definiáltuk az ordó jelöléseket, a lépésszámoknál konstans szorzót emlegettünk. A *dőlten* szedett fogalmakat tudni kell definiálni, a bekeretezetteket bizonyítani. Az aláhúzottakat nem bizonyítottuk.

1. Leszámlálási alapfogalmak: *permutációk, variációk és kombinációk (ismétlés nélkül és ismétléssel)* példával, kiszámításuk, a binomiális tétel,
2. Gráfelméleti alapfogalmak: *pont, él, fokszám. Egyszerű gráf, részgráf, feszített részgráf, izomorfia, élsorozat, út, kör, összefüggő gráf, komponens.* Gráfok fokszámösszege, *fa, erdő*, fák egyszerűbb tulajdonságai.
3. Minimális költségű feszítőfa, Kruskal algoritmus, ez min. ktg-ű fát ad, *normál fák (két féle)*, hogyan keressük meg.
4. *Euler-séta és körséta*, létezésének szükséges és elégséges feltétele (öf gráf esetén). *Hamilton-kör és út* fogalma. Szükséges, illetve elégséges feltételek Hamilton-kör létezésére, Dirac és Ore tételei.
5. Legrövidebb utakat kereső algoritmusok (*BFS, Dijkstra, Ford, Floyd, legrövidebb utak fája*), ezen algoritmusok helyessége. Bejárásokkal kapcsolatos fogalmak: *bejárási fa, faél, előreél, visszaél, keresztél.* Legszélesebb utak irányított és irányítatlan gráfban,
6. Hálózati folyamok: *hálózat, folyam, folyamnagyság (folyamérték), st-vágás, vágás kapacitása (értéke).* Ford-Fulkerson tétel, *javító utas algoritmus (előre- és visszaélek).* Edmonds-Karp tétel.

   Többtermelős, többfogyasztós hálózatok, csúcskapacitások és irányítatlan élek visszavezetése szokásos hálózatra.
7. Páros gráfok, ekvivalens definíció. *Párosítások* (páros és nem páros gráfban), *teljes párosítás, adott ponthalmazt fedő párosítás*, Hall és Frobenius tételei, *alternáló utas algoritmus* maximális párosítás keresésére.
8. *Lefogó és független csúcsok ill. élek*, az *ezekből származó gráfparaméterek* $(\nu, \rho, \alpha, \tau)$ és összefüggéseik, Gallai két tétele. Kőnig-tétel.
9. *Pontszínezés, kromatikus szám, klikkszám*, alsó és felső korlát a kromatikus számra ($\omega(G)$ ill. $\Delta(G)$ segítségével).
10. *Síkbarajzolhatóság, gömbre rajzolhatóság, tartomány, sztereografikus projekció.* Külső tartomány nem kitüntetett volta. Az Euler-féle poliédertétel és következményei.
11. *Kuratowski gráfok*, Kuratowski gráf nem síkbarajzolható, *topologikus izomorfia*, Kuratowski tétele (könnyű irány biz.) és a Fáry-Wagner tétel.

    Síkbarajzolt gráf duálisa. Elvágó él, soros élek, vágás. A duális gráf tulajdonságai (élszám, csúcsszám, összefüggőség, kör-vágás dualitás, annak speciális esetei). Síkgráfok kromatikus száma, négyszíntétel.
12. *Mélységi keresés* és alkalmazásai (élek osztályozása, mélységi számozás, befejezési számozás, fa-, előre-, vissza- és keresztélek, irányított kör létezésének eldöntése DFS-sel), *alapkörrendszer*. *Aciklikus irányított gráfok (DAG-ok)*, jellemzésük a *topologikus sorrenddel*, topologikus sorrend keresése, *PERT-módszer*, *kritikus utak és tevékenységek.* (A PERT helyességét igazából nem bizonyítjuk.)
13. Algoritmusok bonyolultsága (*input mérete*, algoritmus lépésszáma az inputméret függvényében, *polinomidejű algoritmus*), *döntési problémák. P, NP, co-NP* bonyolultsági osztályok fogalma, feltételezett viszonyuk, példa ilyen problémákra. *Polinomiális visszavezethetőség (Karp-redukció)*, NP-teljesség, Cook-Levin tétel, nevezetes NP-teljes problémák.
14. *Oszthatóság, legnagyobb közös osztó,* euklideszi algoritmus, *prímek és felbonthatatlan számok*, a számelmélet alaptétele, *kanonikus alak* fogalma, lnko kanonikus alakja, osztók száma, nevezetes tételek prímszámokról.
15. *Kongruencia fogalma*, műveletek kongruenciákkal. *Teljes és redukált maradékrendszer, az Euler-féle φ-függvény*, $\varphi(n)$ kiszámítása (n kanonikus alakjából). Az Euler-Fermat tétel és a kis Fermat tétel. Lineáris kongruenciák megoldhatósága és megoldása, konkrét módszer a megoldásra. Lineáris diofantikus egyenlet megoldása (példán bemutatva).
16. Számelméleti algoritmusok: alapműveletek, (modulo m) hatványozás és az euklideszi algoritmus lépésszáma. Prímtesztelés, *Fermat-teszt. Nyilvános kulcsú titkosírás*, *digitális aláírás.* Az RSA titkosítási módszer (Az üzenetből számok képzése, p és q prímek generálása, n, m kiszámítása, e és d választása, titkos és nyílt adatok, kódoló és dekódoló függvények, dekódolás működik).