VISZA 105 vizsgatematika
a Számítástudomány alapjai c. tárgyhoz

a 2013/2014-as tanév I. félévre

1. Leszámlálási alapfogalmak: permutációk, variációk és kombinációk (ismétlés nélkül és ismétléssel); binomiális együtthatók közti egyszerű összefüggések, a binomiális tétel, skatulya-elv, szita-formula.
2. Alapvető adatstruktúrák: tömb, láncolt lista, bináris fa. Lineáris és bináris keresés, ezek lépésszáma, minimumkeresés, beszúrási feladat, rendezési feladat. Buborék-, kiválasztásos, beszúrásos, összefésüléses és gyorsrendezés, alsó korlát, lépésszámbecslések.
3. Ládarendezés, bináris keresőfák. Keresés, beszúrás, törlés, minimumkiválasztás, pre-, in- és posztorder bináris keresőfában, rendezés bináris keresőfával. Kupac, kupacos rendezés.
4. Gráfelméleti alapfogalmak: pont, él, fokszám, szomszédossági mátrix, éllista. Egyszerű gráf, részgráf, feszített részgráf, izomorfia, élsorozat, séta, út, kör, összefüggő gráf, komponens. Gráfok fokszámösszege, fák egyszerűbb tulajdonságai.
5. Cayley tétele fák számáról, Prüfer kód. Minimális költségű feszítőfa, Kruskal algoritmus, normál fák.
6. Euler-séta és körséta, létezésének szükséges és elégséges feltétele. Hamilton-kör és út; szükséges, illetve elégséges feltételek Hamilton-kör létezésére, Dirac és Ore tételei.
7. Legrövidebb utakat kereső algoritmusok (BFS, Dijkstra, Ford, Floyd). Legszélesebb utak irányított és irányítatlan gráfban.
8. Hálózati folyamok: hálózat, folyam, folyamnagyság (folyamérték), st-vágás, vágás kapacitása. Ford-Fulkerson tétel, javító utas algoritmus. Egészértékűségi lemma, Edmonds-Karp tétel (biz. nélkül).
9. Többtermelős, többfogyasztós hálózatok, csúcskapacitások és irányítatlan élek kezelése. Él- és pontidegen utak. Menger négy tétele, gráfok többszörös összefüggősége, kapcsolata a Menger tételekkel.
10. Páros gráfok, ekvivalens definíció. Párosítások, Hall, Frobenius és Kőnig tételei, alternáló utas algoritmus maximális párosítás keresésére. Lefogó és független csúcsok ill. élek, Gallai két tétele. Tutte tétele párosításokról (csak a triviális irányban bizonyítva).
11. Pont- és élszínezés, kromatikus szám, klikkszám, alsó és felső korlátok a kromatikus és élkromatikus számra, Brooks tétel (biz. nélkül), Myczielski-konstrukció (biz. nélkül), Vizing tétel (biz. nélkül).
12. Síkbarajzolhatóság, gömbre rajzolhatóság. Az Euler-féle poliédertétel és következményei: egyszerű, síkbarajzolható gráfok élszáma és minimális fokszáma. Kuratowski gráfok, Kuratowski tétele (csak könnyű irányban biz.), Fáry-Wagner tétel (biz. nélkül).
13. Dualitás, tulajdonságai. Elvágó él, soros élek, vágás. Gyenge izomorfia, absztrakt dualitás, Whitney három tétele (biz. nélkül), síkgráfok kromatikus száma, ötszíntétel.
14. Mélységi keresés és alkalmazásai (élek osztályozása, irányított kör létezésének eldöntése), alapkörrendszer. Aciklikus irányított gráfok jellemzése, topologikus sorrend, PERT-módszer, kritikus utak és tevékenységek.
15. Algoritmusok bonyolultsága, döntési problémák. $P, NP, co\text{-}NP$ bonyolultsági osztályok fogalma, feltételezett viszonyuk, polinomiális visszavezethetőség, NP-teljesség, Cook-Levin tétel (biz. nélkül), nevezetes NP-teljes problémák: SAT, HAM, 3-SZÍN, k-SZÍN, MAXFTN, MAXKLIKK, HAMÚT.
16. Oszthatóság, legnagyobb közös osztó, legkisebb közös többszörös, euklideszi algoritmus, prímek és felbonthatatlan számok, a számelmélet alaptétele, osztók száma, nevezetes tételek prímszámokról: prímek száma, prímek közti hézag mérete és a prímszámtétel (biz. nélkül).
17. Kongruencia fogalma, műveletek kongruenciákkal. Teljes és redukált maradékrendszer, az Euler-féle φ-függvény, Euler-Fermat tétel és kis Fermat tétel. Lineáris kongruenciák megoldhatósága és megoldása. Lineáris diofantikus egyenletek megoldása.
18. 2-változós művelet, félcsoport, csoport, példák számokon és nem számokon. Csoport rendje, csoportok izomorfiája, részcsoport, generált részcsoport, elem rendje, ciklikus csoport, diédercsoport, Lagrange tétele (biz. nélkül).
19. Gyűrűk. 0, 1, ellentett fogalma, 0-val szorzás gyűrűben. Kommutatív, egységelemes gyűrű. Példák gyűrűkre számokon és polinomokkal. Ferdetest, test fogalma, példák.
20. Számelméleti algoritmusok: alapműveletek, (modulo m) hatványozás és az euklideszi algoritmus. Prímtesztelés. Nyilvános kulcsú titkosírások, digitális aláírás. Az RSA titkosítási módszer.