VPRAŠANJA ZA MAGISTRSKI IZPIT

DISKRETNA MATEMATIKA – A

1 Kombinatorika

Delno urejene množice. Incidenčne algebre. Möbiusova funkcija delno urejene množice. Möbiusova obratna formula. Mreže. Razdelitve in razčlenitve. Simetrične funkcije in Youngove tabele.
Literatura: [10] (pogl. 10, 15, 25).

Permutacijske grupe. Delovanje grupe na množici. Burnsideova lema. Polyajev izrek. Tranzitivno in primitivno delovanje. ⟦Klasifikacija končnih enostavnih grup.⟧ ⟦Algoritmi na permutacijskih grupah.⟧
Literatura: [10] (pogl. 10, 35), [3].

Rekurzivne enačbe. Linearne rekurzivne enačbe. Sistemi rekurzivnih enačb. Navadne in eksponentne rodovne funkcije. Asimptotika. Seštevanje v zaključeni obliki. Gosperjev in Zeilbergerjev algoritem. Avtomatsko dokazovanje kombinatoričnih identitet.
Literatura: [10] (pogl. 13, 14), [7] (pogl. 5, 7, 9).

Načrti. Končne geometrije. Hadamardove matrike. Načrti. Steinerjeve trojke. Kodi za odpravljanje napak. Hammingovi, Reed-Mullerjevi in linearni kodi.
Literatura: [10] (pogl. 16–20).

Matroidi. Baza, cikel, neodvisna množica, zaprta množica. Matroidi in matrike. Vektorske reprezentacije matroidov. Grafovski matroidi. Prostor ciklov grafa in prerezi. Matroidi in ravninski grafi.
Literatura: [11] (pogl 1, 2, 6).

Ramseyeva teorija. Ramseyev izrek in Ramseyeva števila. Verjetnostne metode v kombinatoriki. Lovászova lokalna lema.
Literatura: [10] (pogl. 3), [6] (pogl. 9), [1] (pogl. 1, 5.1, 5.3).

Dodatna literatura: [14, 15, 21, 23].

2 Teorija grafov

Osnovno o grafih. Osnovni pojmi. Osnovne družine grafov in konstrukcije (produkti grafov, krovi kot napetostni grafi, grafi grup). Drevesa in cikli. Podgrafi in minorji. Prostor ciklov in prerezi. Eulerjevi obhodi. Hamiltonove poti in cikli. Usmerjeni grafi in turnirji. ⟦Problem rekonstrukcije grafa. Hipergrafi.⟧

Literatura: [6] (pogl. 1, 10), [2] (pogl. 19).

Prirejanja v grafih. Osnovno o prirejanjih. Tutteov izrek o popolnem prirejanju. Petersenov izrek o 2-faktorju in o popolnem prirejanju v kubičnih grafih. Königov in Hallov izrek. Prirejanja in pokritja v dvodelnih grafih. Postopek alternirajočih poti. Pokritja s potmi v usmerjenih grafih (Gallai-Milgramov izrek).

Literatura: [6] (pogl. 2).

Povezanost. Bloki in 2-povezani grafi. Struktura 3-povezanih grafov. Tutteov izrek. k-povezani grafi. Mengerjev izrek. Maderjev izrek. Disjunktna vpeta drevesa. Obstoj poti med danimi pari točk.

Literatura: [6] (pogl. 3).

Ravninski grafi in vložitve grafov v sklenjene ploskve. Grafi v ravnini, maksimalni ravninski grafi. Lica 3-povezanih grafov. Whitneyev izrek o enoličnosti vložitev. Karakterizacije ravninskih grafov. Geometrijski in abstraktni dual. Celične vložitve grafov v sklenjene ploskve. Eulerjeva formula. Rod grafa. Heawoodova formula. ⟦Prepovedani minorji (izrek Robertsona in Seymourja).⟧ ⟦Presečno število grafa.⟧

Literatura: [6] (pogl. 4, 12.5), [19] (razdelka 1.4, 1.6).

Barvanja grafov. Dvodelni grafi. Barvanja ravninskih grafov. Brooksov izrek. Kritični grafi. Barvanje povezav in Vizingov izrek. ⟦Snarki.⟧ ⟦Kromatični polinom grafa.⟧ Seznamska barvanja. Galvinov izrek. Popolni grafi. Lovászov izrek. Povsod neničelni pretoki in barvanja grafov. Tutteove hipoteze o pretokih. Seymourjev izrek o 6-pretoku.

Literatura: [6] (pogl. 5).

Ekstremalna teorija grafov. Turánov izrek. Erdős-Stonov izrek. Szemerédijeva lema o regularnosti.

Literatura: [6] (pogl. 7).

Minorji in subdivizije. Minor grafa. Topološka vsebovanost. Subdivizije polnih grafov in minimalna stopnja. Subdivizija grafa in dolžina najkrajšega cikla. Polni grafi kot minorji. Hadwigerjeva hipoteza.

Literatura: [6] (pogl. 8).

Spekter grafa. Matrika sosednosti in Laplaceova matrika grafa. ⟦Perron-Frobeniusov izrek.⟧ Osnovne lastnosti spektra grafa. Spekter regularnih grafov. Uporaba na krepko regularnih in razdaljno-regularnih grafih. Druga lastna vrednost Laplaceove matrike grafa, razširjanje grafa in njegove izoperimetrične lastnosti.

Literatura: [2] (razdelki 2, 3, 20, 21).

Grupa avtomorfizmov. Delovanje grupe na množici. Grupa avtomorfizmov grafa. Cayleyjevi grafi. Tranzitivni grafi (po točkah, povezavah, 1-tranzitivni).

Literatura: [2] (razdelki 15, 16, 17).

Slučajni grafi. Modeli slučajnih grafov. Osnovne lastnosti skoraj vseh grafov (stopnje točk, velikost maksimalne klike, kromatično število, število kratkih ciklov). Funkcije praga za nekatere lastnosti grafov.

Literatura: [6] (pogl. 11).

Dodatna literatura: [16, 19, 21, 23].

3 Matematične osnove računalništva in algoritmi

Formalni jeziki in avtomati. Nizi in jeziki. Končni avtomati, regularni izrazi in regularni jeziki. Lastnosti in karakterizacija regularnih jezikov. ⟦Kontekstno neodvisni jeziki in skladovni avtomati. Lastnosti in karakterizacija kontekstno neodvisnih jezikov.⟧ Turingov stroj. Churcheva teza. Neodločljivi problemi. Rekurzivne in rekurzivno preštevne množice. ⟦Hierarhija Chomskega.⟧

Literatura: [8] (pogl. 1–9).

Teorija računske zahtevnosti. Časovna in prostorska zahtevnost algoritma. ⟦Izreki o linearni pospešitvi in o redukciji števila trakov.⟧ Savitchev izrek. ⟦Borodinov izrek o vrzelih in Blumov izrek o pospešitvi.⟧ Razreda P in NP. NP-polni problemi. Cookov izrek. Razred co-NP. #P-polni problemi. PSPACE-polni problemi. Aproksimacijski algoritmi.

Literatura: [8] (pogl. 12 in 13), [9] (pogl. 21–27), [5] (razd. 37).

Kriptografija. Klasični tajnopisi. Statistična kriptoanaliza. Simetrični tajnopisi, DES in diferenčna kriptoanaliza. Koncept javnega kriptosistema (Diffie in Hellman) in enosmerne funkcije. Praštevila, faktorizacija, kriptosistemi RSA. Končni obsegi, diskretni logaritem, algoritmi za računanje diskretnega logaritma, ElGamalovi kriptosistemi, eliptične krivulje. Zgoščevalne funkcije, celovitost podatkov, digitalni podpisi, identifikacija, overjanje.

Literatura: [12] (razdelki 1, 3.1–3.2, 4.1–4.3, 4.8, 5.1–5.2, 6.1–6.3, 7.1–7.4).

Podatkovne strukture. Sklad, vrsta, urejeni seznam, razpršene tabele. Iskalna drevesa, uravnotežena drevesa, kopica (običajna, ⟦binomska, Fibonaccijeva⟧). Množice (Union-Find). Predstavitve grafov.

Literatura: [5, 9].

Metode načrtovanja algoritmov. Deli in vladaj. Dinamično programiranje. Požrešna metoda in zveza z matroidi.

Literatura: [5, 9], [11] (pogl. 1.6).

Optimizacijski problemi in algoritmi. Metode za urejanje podatkov (s primerjavami, z upoštevanjem strukture podatkov). Računska geometrija (konveksna ovojnica, najbližji par). Hitra Fourierova transformacija, hitro množenje. Množenje matrik. Linearno programiranje (postopek simpleksov, dualnost, matrične igre).

Literatura: [5, 9], [4] (pogl. 2–5, 15).

Algoritmi na grafih. Pregledi grafov in povezanost grafa (2-povezanost, krepka povezanost). Topološko urejanje, Floyd-Warshall. Najcenejše vpeto drevo. Najkrajše poti, Dijkstra, Bellman-Ford. Maksimalni pretok. Maksimalno prirejanje v dvodelnih in splošnih grafih. Separatorji v ravninskih grafih. ⟦Vložitev grafa v ravnino.⟧ ⟦Minorji in problem disjunktnih poti.⟧

Literatura: [5, 9].

Vzporedni algoritmi. Modeli vzporednega računanja. Razred NC. Zgledi učinkovitih vzporednih algoritmov (aritmetične operacije, operacije z matrikami). Vzporedno urejanje.

Literatura: [5, 9].

Verjetnostni algoritmi. Tipi verjetnostnih algoritmov. Millerjev test praštevilskosti. Verjetnostni testi s polinomi. Lubyjev algoritem. ⟦Računanje prostornine konveksnih teles.⟧

Literatura: [9].

Dodatna literatura: [13, 17, 18, 20, 22].

Viri

[1] N. Alon, J. Spencer, *The Probabilistic Method*, Wiley, 1992.

[2] N. L. Biggs, *Algebraic Graph Theory*, Cambridge Univ. Press, Cambridge, 1974.

[3] G. A. Butler, J. J. Cannon, Computing in permutation and matrix groups I, II, *Math. Comput.* **39** (1982) 663–680.

[4] V. Chvátal, *Linear Programming*, Freeman, 1983.

[5] T. H. Cormen, C. E. Leiserson, R. L. Rivest, *Introduction to Algorithms*, MIT Press, 1990.

[6] R. Diestel, *Graph Theory*, Springer-Verlag, 1997.

[7] R. L. Graham, D. E. Knuth, O. Patashnik, *Concrete Mathematics*, 2nd ed., Addison-Wesley, 1994.

[8] J. E. Hopcroft, J. D. Ullman, *Introduction to Automata Theory, Languages, and Computation*, Addison-Wesley Publishing Co., Reading, Mass., 1979.

[9] D. C. Kozen, *The Design and Analysis of Algorithms*, Springer-Verlag, 1992.

[10] J. H. van Lint, R. M. Wilson, *A Course in Combinatorics*, Cambridge Univ. Press, 1992.

[11] B. Mohar, *Teorija matroidov*, DMFA Slovenije, 1996.

[12] D. R. Stinson, *Cryptography – Theory and Practice*, CRC Press, 1995.

Dodatna literatura

[13] A. V. Aho, J. E. Hopcroft, J. D. Ullman, *The Design and Analysis of Computer Algorithms*, Addison-Wesley, Reading, Mass., 1974.

[14] V. Batagelj, *Kombinatorika*, Ljubljana, 1997.

[15] N. L. Biggs, *Discrete Mathematics*, The Clarendon Press, Oxford University Press, New York, 1989.

[16] J. A. Bondy, U. S. R. Murty, *Graph Theory with Applications*, North-Holland, 1976.

[17] M. R. Garey, D. S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-completeness*, Freeman, San Francisco, CA, 1979.

[18] A. Gibbons, *Algorithmic Graph Theory*, Cambridge Univ. Press, 1985.

[19] J. L. Gross, T. W. Tucker, *Topological Graph Theory*, Wiley, New York, 1987.

[20] D. E. Knuth, *The Art of Computer Programming, Vol. II, Seminumerical Algorithms*, Addison-Wesley, Reading, MA, 1973.

[21] D. Veljan, *Kombinatorika s teorijom grafova*, Školska knjiga, Zagreb, 1988.

[22] *Handbook of Theoretical Computer Science, Volume A*, J. van Leeuwen, Ed., Elsevier, 1990. (Poglavja 10, 12.4, 12.5).

[23] *Handbook of Combinatorics*, R. L. Graham, M. Grotschel in L. Lovász, Eds., Elsevier Science B.V., Amsterdam; MIT Press, Cambridge, MA, 1995.