GRUNDLAGEN DER THEORETISCHEN INFORMATIK

Wintersemester 2013/2014
Inhalt

1. Elementare Kombinatorik (Permutation, Variation, Kombination), Binomischer Satz, Eigenschaften von Binomialkoeffizienten, Pascalsches Dreieck, homogen lineare Rekursionen, Fibonacci-Folge

2. Grundbegriffe der Graphentheorie (Graph, Knoten, Kante, Grad, Isomorphie, Teilgraph, Kantenzug, Weg, Kreis, Zusammenhang, Baum, Wald), Anzahl von Kanten in zusammenhängenden bzw. kreisfreien Graphen, Spannbäume, Satz von Cayley, Prüfer-Code, Kruskal-Algorithmus

3. Graphdurchlauf (BFS, DFS), günstigste Wege (Kostenfunktionen, Optimalitätsprinzip, Relax-Schritt, Algorithmus von Bellman und Ford, Algorithmus von Dijkstra)

4. Anwendungen der Tiefensuche (Kirchhoffsche Maschengleichungen, gerichtete Kreise in gerichteten Graphen, topologische Ordnung), DAG (günstigste bzw. ungünstigste Wege, Methode des kritischen Pfades)

5. Paarungen in allgemeinen Graphen (Satz von Berge*, Satz von Tutte* – Beweis nur für die einfache Richtung) und in bipartiten Graphen (Algorithmus von Kőnig, Satz von Hall, Satz von Frobenius)

6. Unabhängige und überdeckende Knoten- und Kantenmengen (α, ν, ϱ, τ, Sätze von Gallai, Sätze von Kőnig)

7. Netzwerkflüsse (Netzwerk, Fluss, st-Schnitt, Algorithmus von Ford und Fulkerson, Satz von Edmonds und Karp*, MFMC-Satz, ganzzahlige Kapazitäten)

8. Sätze von Menger – Beweis nur für den ersten Satz, mehrfacher Zusammenhang und Kantenzusammenhang (Äquivalenz der Definitionen mit disjunkten Wegen bzw. Weglassen von Knoten/Kanten, Eigenschaften von 2-fach zusammenhängenden Graphen, Sätze von Menger über den 2-fachen Zusammenhang, Satz von Dirac*)

9. Planarität (planare Zeichnung, Gebiete, Ränder der Gebiete, Euler-Formel für zusammenhängende bzw. nicht zusammenhängende* planare Graphen, Zeichnung auf Kugeloberfläche, obere Schranken für die Anzahl der Kanten in planaren Graphen, K_5 und $K_{3,3}$, Unterteilung, Satz von Kuratowski* – Beweis nur für die einfache Richtung, Satz von Fáry und Wagner*), Dualität (duale Begriffspaare, minimale Schnittmengen), schwache Isomorphie (Sätze von Whitney*), abstrakte Dualität

10. Knotenfärbung (chromatische Zahl, untere Schranken, Cliquenzahl, Mycielski-Konstruktion, gierige Färbung mit $\Delta + 1$ Farben, Satz von Brooks*, 5-Farbensatz, 4-Farbensatz*)

11. Perfekte Graphen (induzierter Teilgraph, Kreise ungerader Länge ≥ 5 und deren Komplement, bipartite Graphen, Intervallgraphen, Strong Perfect Graph Theorem*, Satz von Lovász*), Kantenfärbung (chromatischer Index, untere Schranken, Satz von Vizing*, Satz von Kőnig*)

12. Eulersche „Kreise" und „Wege" in gerichteten und ungerichteten Graphen (hinreichende und notwendige Bedingungen, Algorithmus), Hamiltonsche Kreise und Wege (notwendige Bedingung für die Existenz von Hamiltonschen Kreisen bzw. Wegen, Satz von Dirac, Satz von Ore)

13. Komplexitätstheorie ($\mathcal{P}$, $\mathcal{NP}$, co-$\mathcal{NP}$, Karp-Reduktion und ihre Eigenschaften, $\mathcal{NP}$-Vollständigkeit, Satz von Cook und Levin*, mögliche Beziehungen zwischen den Komplexitätsklassen, Satz von Ladner*, bekannte $\mathcal{NP}$-vollständige bzw. in Polynomialzeit lösbare Probleme)

14. Grundlagen der Zahlentheorie (Teilbarkeit, größter gemeinsamer Teiler, kleinster gemeinsamer Vielfache, Primzahlen und irreduzible Zahlen, Satz von Bézout, Fundamentalsatz der Arithmetik, Anzahl der Teiler einer Zahl), Eigenschaften von Primzahlen (Satz von Euklid, Satz von Dirichlet*, Primzahlsatz*, Lücken zwischen nacheinander folgenden Primzahlen, Goldbachsche Vermutung*)

15. Kongruenzen (Restklassen, Rechnen mit Kongruenzen, Lösung von linearen Kongruenzen und simultanen Kongruenzsystemen, lineare diophantische Gleichungen, nichttriviale Lösungen von $x^2 \equiv 1\ (m)$, Satz von Wilson), zum Modul teilerfremde Restklassen (φ-Funktion und ihre Berechnung, Satz von Euler und Fermat bzw. die Umkehrung des Satzes, kleiner Satz von Fermat und seine Verallgemeinerung)

16. Arithmetische Algorithmen (Grundrechenarten, Potenzbildung, Grundrechenarten und Potenzbildung modulo m, Euklidischer Algorithmus), Primtests (Sieb des Eratosthenes, Fermat-Test, Miller-Rabin-Test*), Kryptographie mit öffentlichen Schlüsseln (geheime Übertragung, digitale Signatur, RSA-Algorithmus, Diffie-Hellman-Schlüsselaustausch)

17. Algebraische Strukturen und Operationen, Assoziativität, Kommutativität, Halbgruppen (Definition, Beispiele), Gruppen (Definition, Beispiele, Eindeutigkeit des neutralen Elements und der Inverse)

18. Gruppentheorie (Untergruppe, Isomorphismus, von einem Element generierte Untergruppe, zyklische Gruppe, Ordnung der Gruppe, Ordnung eines Elements), Nebenklassen (Eigenschaften von Nebenklassen, Satz von Lagrange, Folgerungen aus dem Satz von Lagrange)

19. Ringe (Definition, Beispiele, Nullteiler, Integritätsbereich, Arithmetik in Ringen), Körper (Definition, Beispiele, endliche Körper), Kryptographie mit öffentlichen Schlüsseln basierend auf elliptischen Kurven, Körpererweiterungen (einfache Erweiterung, algebraische und transzendente Erweiterung), Fundamentalsatz der Algebra

* = Ohne Beweis