Simon König 3344789 - Klausurzettel Theoretische Informatik 3

1 Wichtige Algorithmen

- Quickselect wählt das k kleinste Element aus einer unsortierten Liste aus. Laufzeit w-c: $\mathcal{O}(n^2)$ und a-c: $\leq 4n$

2 Laufzeitanalyse

- **Mastertheorem 1** Für $a, b \in \mathbb{N}$, $b > 1$ und eine Funktion $g : \mathbb{N} \to \mathbb{N}$ mit $g \in \Theta(n^c)$ gelte

$$t(1) = g(1)$$
$$t(n) = a \cdot t\left(\frac{n}{b}\right) + g(n)$$

Dann gilt

$$t(n) \in \begin{cases} \Theta(n^c) & \text{falls } a < b^c \\ \Theta(n^c \log n) & \text{falls } a = b^c \\ \Theta(n^{\frac{\log a}{\log b}}) & \text{falls } a > b^c \end{cases}$$

- **Mastertheorem 2** Sei $r > 0$ und die Zahlen $\alpha_1 \geq 0$ für alle i und erfüllen $\sum_{i=1}^r \alpha_i < 1$. Wenn die Rekursive Funktion t die Ungleichung

$$t(n) \leq \left(\sum_{i=1}^{r} t(\lceil \alpha_i \cdot n \rceil)\right) + c \cdot n$$

für ein $c > 0$ erfüllt, dann ist $t(n) \in \mathcal{O}(n)$.
- **Summenformeln**

$$\sum_{i=0}^{n} x^i = \frac{1 - x^{n+1}}{1 - x}$$

$$?$$

3 Diskrete Strukturen

- Halbgruppe: assoziativ
- Monoid: neutrales Element
- Gruppe: beidseitig Inverse
- Abelsche Gruppe: kommutativ
- Ring: $(R, +, 0)$ ist abelsche Gruppe, $(R, \cdot, 1)$ ist Monoid, Distributivgesetze
- Körper: $(R \setminus \{0\}, \cdot, 1)$ ist Gruppe und $\cdot$ ist kommutativ
- Eigenschaften einer Kongruenzrelation:
  - Reflexivität: $a \sim a$
  - Symmetrie: $a \sim b \Rightarrow b \sim a$
  - Transitivität: $a \sim b, b \sim c \Rightarrow a \sim c$
  - Kongruenzeigenschaft mit Abbildung $\circ$: $x \sim x' \land y \sim y' \Rightarrow x \circ y \sim x' \circ y'$

4 Modulare Arithmetik

- Es gilt
$$ca \equiv cb \mod m \Rightarrow a \equiv b \mod \frac{m}{\mathtt{ggT}(m, c)}$$
- Allgemein gilt
$$\mathtt{ggT}(ca, cb) = c \cdot \mathtt{ggT}(a, b)$$
- **Lemma von Bezout** Für alle $m, n \in \mathbb{Z}$ existieren $a, b \in \mathbb{Z}$ so, dass

$$\mathtt{ggT}(m, n) = am + bn$$

das heißt, der größte gemeinsame Teiler lässt sich als Linearkombination darstellen.
- **Fundamentalsatz der Arithmetik** Die Primfaktorzerlegung jeder natürlichen Zahl ist eindeutig.
- Die multiplikative Gruppe besteht aus den Elementen, die teilerfremd zum Modul sind

$$(\mathbb{Z}/n\mathbb{Z})^* = \{k + n\mathbb{Z} \mid \mathtt{ggT}(k, n) = 1\}$$

- $\mathbb{Z}/n\mathbb{Z}$ ist ein Körper genau dann, wenn n eine Primzahl ist.
- Die lineare Abbildung $x \mapsto kx$ auf $\mathbb{Z}/n\mathbb{Z}$ ist genau dann bijektiv, wenn $\mathtt{ggT}(k, n) = 1$.
- Sind m, n teilerfremd, d.h. $\mathtt{ggT}(m, n) = 1$, dann ist

$$\pi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, x \mapsto (x + m\mathbb{Z}, x + n\mathbb{Z})$$

surjektiv. Damit erhält man eine bijektive Abbildung

$$(x \mod mn) \mapsto (x \mod m, x \mod n)$$

- **Chinesischer Restsatz** Für teilerfremde Zahlen m, n ist die Abbildung

$$\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, x + mn\mathbb{Z} \mapsto (x + m\mathbb{Z}, x + n\mathbb{Z})$$

ein Isomorphismus (bijektiver Homomorphismus).
Lösung des Kongruenzsystems

$$x \equiv a_1 \mod m_1$$
$$x \equiv a_2 \mod m_2$$

finden. Bestimme die Inversen x_i

$$m_2 \cdot x_1 \equiv 1 \mod m_1$$
$$m_1 \cdot x_2 \equiv 1 \mod m_2$$

Dann ist die Lösung

$$x \in (x_1 m_2 a_1 + x_2 m_1 a_2) + m_1 m_2 \mathbb{Z}$$

Es gibt eine Lösung genau dann, wenn für alle Paare $i \neq j$ gilt

$$a_i \equiv a_j \mod \mathtt{ggT}(m_i, m_j)$$

- **Der kleine Satz von Fermat** Für alle Primzahlen p und alle $a \in \mathbb{Z}$ gilt

$$a^p \equiv a \mod p$$

Falls a und p teilerfremd sind, gilt sogar

$$a^{p-1} \equiv 1 \mod p$$

- **Satz von Euler** Für teilerfremde ganze Zahlen a, n gilt

$$a^{\varphi(n)} \equiv 1 \mod n$$

Verallgemeinert man den Satz (die multiplikative Gruppe $(\mathbb{Z}/n\mathbb{Z})^*$ ist kommutativ), erhält man den **Satz von Lagrange** Es gilt sogar für jede kommutative Gruppe G und jedes $a \in G$

$$a^{|G|} = 1$$

- Summe über die $\varphi(t)$ der Teiler von n ist gleich n

$$\sum_{t|n} \varphi(t) = n$$

- **Satz von Wilson** Für alle natürlichen Zahlen $n \geq 2$ gilt

$$(n-1)! \equiv -1 \mod n \quad \Leftrightarrow \quad n \text{ ist Primzahl}$$

5 Graphen

- Die Summe aller Knotengrade in einem ungerichteten Graphen ist immer gerade.
- In jedem endlichen Graph ist die Anzahl der Knoten mit ungeradem Grad gerade.
- Ein zusammenhängender endlicher Graph hat genau dann einen Eulerpfad, wenn die Anzahl der Knoten mit ungeradem Grad maximal 2 ist. Ein Eulerkreis existiert genau dann, wenn alle Knoten geraden Grad haben.
- **Eulerformel** In endlichen zusammenhängenden planaren Graphen mit $n \geq 1$ Knoten, m Kanten und f Facetten gilt

$$n - m + f = 2 \quad \text{bezeihungsweise} \quad n - m + f = z + 1$$

für z Zusammenhangskomponenten. Wichtige Folgerungen hieraus sind
  - Ein planarer Graph mit $n \geq 3$ Knoten hat höchstens $3n - 6$ Kanten.
  - Ein planarer bipartiter Graph mit $n \geq 4$ Knoten hat höchstens $2n - 4$ Kanten
  - In jedem planaren Graph gibt es mindestens einen Knoten mit Grad kleiner oder gleich 5.
  - Der K_5 und der $K_{3,3}$ sind nicht planar.

(Folie 25.4)
- **Satz von Kuratowski** Ein Graph ist genau dann planar, wenn er keine Unterteilung des K_5 oder des $K_{3,3}$ enthält.