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: $\leq 4n$
- Quicksort $\mathcal{O}(n \log n)$ worst-case:$\mathcal{O}(n^2)$, Merge-Heapsort $\mathcal{O}(n \log n)$, Dijkstra $\mathcal{O}(n^2 + m)$
- Algorithmus zur optimalen Klammerung (dynamische Programmierung). Laufzeit $\mathcal{O}(n^3)$ Kosten für Matrixmultiplikation $(k \times m) \cdot (m \times l)$ sind $k \cdot m \cdot l$.
  Tabelleneintrag $T_{i,j}$ enthält die minimalen Kosten die Matrizen M_i bis M_j zu multiplizieren.
  $T_{i,j} = \min_{i \leq m \leq j} \{T_{i,m} + T_{m+1,j} + n_{i-1} \cdot n_m \cdot n_j\}$.
  Tabelle B enthält die Trennpunkte, $T_{1,3} = 1$ bedeutet, dass die Trennstelle nach Matrix 2 kommt, d.h. $M_1(M_2M_3)$.
- Schnelle Multiplikation von $X = A \cdot b^n + B$ und $Y = C \cdot b^n + D$

$$XY = AC \cdot b^{2n} + (AD + BC) \cdot b^n + BD$$

  wir berechnen

$$\begin{aligned}
P_1 &= AC \\
P_2 &= BD \\
P_3 &= (A+B)(C+D) = AC + AD + BC + BD \\
&\rightarrow \quad P_3 - P_1 - P_2 = (AD + BC).
\end{aligned}$$

  damit $o(n^{1.6})$.
- Bottom-Up Heapsort in $(1.5 \cdot n \log n)$ und Ultimatives Heapsort $(n \log n) + \mathcal{O}(n)$
- Randomisierte Algorithmen: Monte Carlo, Fehler ist erlaubt (Primzahltest) und Las Vegas, Kein Fehler erlaubt aber keine Aussage ist auch möglich (Quicksort).
- Primzahltest nach Fermat. Wähle $a \in \{1, \ldots, n\}$, $x = a^{n-1} \mod n$. Wenn $x \not\equiv 1 \mod n$, dann ist n keine Primzahl. Sonst keine Aussage.
- Sei $n \geq 2$ und $n \in \mathbb{N}$. Falls für alle Primzahlen p mit $n \equiv 1 \mod p$ eine Zahl $a \in Z$ existiert, so dass

$$a^{n-1} \equiv 1 \mod n \quad \text{und} \quad a^{\frac{n-1}{p}} \not\equiv 1 \mod n$$

  gilt, dann ist n eine Primzahl.
- 1. Große Primzahlen p, q mit $p < q$
  2. Berechne $n = p \cdot q$
  3. setze $\varphi(n) = (p-1)(q-1)$,
  4. wähle $e > 1$ mit $\mathtt{ggT}(e, \varphi(n)) = 1$
  5. Berechne $s < n$ mit $e \cdot s \equiv 1 \mod \varphi(n)$, d.h. $e \cdot s = k \cdot \varphi(n) + 1$.

  Das Paar (n, e) bildet den *öffentlichen Schlüssel*. Die Nachricht sei x. Die verschlüsselte Nachricht ist dann y

$$y = x^e \mod n \quad x' = y^s \mod n$$

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

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

  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**

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

$$\sum_{i=1}^{n} i = \frac{n^2 + n}{2}$$

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 $\circ$: $x \sim x' \wedge y \sim y' \Rightarrow x \circ y \sim x' \circ y'$

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

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

- $|(\mathbb{Z}/n\mathbb{Z})^*| = \varphi(n)$ und $\varphi(p) = p - 1$ und falls $\mathtt{ggT}(a, b) = 1$, dann $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ und $\varphi(n) = n \cdot \prod_{p|n}(1 - \frac{1}{p})$
- $\mathbb{Z}/n\mathbb{Z}$ 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

$$\begin{aligned}
x &\equiv a_1 \mod m_1 \\
x &\equiv a_2 \mod m_2
\end{aligned}$$

  finden. Bestimme die Inversen x_i

$$\begin{aligned}
m_2 \cdot x_1 &\equiv 1 \mod m_1 \\
m_1 \cdot x_2 &\equiv 1 \mod m_2
\end{aligned}$$

  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

P_n ist der Pfad, C_n ist der Kreis, K_n ist der vollständige Graph, $K_{m,n}$ ist der vollständige bipartite Graph. Stier ist $\forall$ mit 5 Knoten.

- 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.
- **Satz von Ramsey**

6 Zahlen und Abschätzungen

- **Fibonacci-Zahlen** $F_0 = 0, F_1 = 1$.

$$F_n \leq 2^n \leq F_{2n} \quad \forall n \geq 3$$

$$F_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right)$$

$$\mathtt{ggT}(F_n, F_m) = F_{\mathtt{ggT}(m,n)}$$

- **Catalanzahlen**
- **Partitionszahlen**
- **Dyckwörter**
- **Saturierte Binärbäume**
-

$$n^n \in \omega(n^c n!)$$
$$\log(n!) \in \Theta(n \log n)$$
$$\log(\sqrt{n}) \in \Theta(\log(\sqrt{n}))$$

7 Sonstiges

- **Markov-Ungleichung**, Sei $\forall \omega : X(\omega) \geq 0$ und $E(X) > 0$, dann

$$\forall \lambda > 0 : \quad P(X \geq \lambda E(X)) \leq \frac{1}{\lambda}$$

- $Var(X) = E(X^2) - E(X)^2 = E((X - E(X))^2)$.
- $Var(a \cdot X + b) = a^2 \cdot X, Var(X + Y) = Var(X) + Var(Y)$
- Zurücklegen / Reihenfolge
  - Ja/Ja: n^k
  - Nein/Ja: $k!\binom{n}{k}$
  - Ja/Nein: $\binom{n+k-1}{k}$
  - Nein/Nein: $\binom{n}{k}$