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- und Heapsort** $\mathcal{O}(n \log n)$, **Dijkstra** $\mathcal{O}(n^2+m)$. **Bottom-Up Heapsort** in $(1.5 \cdot n \log n)$ und **Ultimatives Heapsort** $(n \log n) + \mathcal{O}(n)$
- 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
  $$\begin{aligned} &P_1 = AC \\ &P_2 = BD \\ &P_3 = (A+B)(C+D) = AC + AD + BC + BD \\ &\quad \rightarrow \quad P_3 - P_1 - P_2 = (AD + BC). \end{aligned}$$
  damit $o(n^{1.6})$.
- 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 $a \in \{1, \dots, n\}$, $x = a^{n-1} \mod n$. Wenn $x \not\equiv 1 \mod n$, dann ist $n$ keine Primzahl. Sonst keine Aussage.
- **Primzahlzertifikat** 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.
- **RSA**
  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 $y$
  $$y = x^e \mod n \quad x' = y^s \mod n$$
- **String-Matching** Text der Länge $n$, Muster $m$. Knuth-Morris-Pratt: Rabin-Karp (Hashing zur Basis $|\Sigma|$ mit Modulus $p$): a-c:$\mathcal{O}(m+n) + k\mathcal{O}(m)$ bei $k$ Kollisionen, w-c: $\Theta(m \cdot n)$. BruteForce: $\Theta(m \cdot n)$. Endlicher Automat: $\Theta(|\Sigma| \cdot m + n)$. Knuth-Morris-Pratt: w-c: $\mathcal{O}(n \cdot m)$.

# 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**
  $$\sum_{i=0}^{n} x^i = \frac{1 - x^{n+1}}{1 - x}$$
  $$\sum_{i=1}^{n} i = \frac{n^2 + n}{2}$$
  $$\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$$
- **Rekursionsgleichung** $T(n) = 2 \cdot T(n-b) + c, T(0) = d > 0$, dann ist $T(n) = (d+c)a^{\frac{n}{b}} - c$
- **Landausymbole** Damit $f \in \Lambda(g)$ gilt

| | | |
|---|---|---|
| $\mathcal{O}$ | $\limsup f/g < \infty$ | $\exists c, N : \forall n \geq N : f(n) \leq c \cdot g(n)$ |
| $o$ | $\lim f/g = 0$ | $\forall c \exists N : \forall n \geq N : f(n) \leq c \cdot g(n)$ |
| $\Omega$ | $\liminf f/g > 0$ | $\exists c, N : \forall n \geq N : f(n) \geq c \cdot g(n)$ |
| $\omega$ | $\lim f/g = \infty$ | $\forall c \exists N : \forall n \geq N : f(n) \geq c \cdot g(n)$ |
| $\Theta$ | $\mathcal{O} \cap \Omega$ | |

  Man darf immer $f$ und $g$ in Betragsstriche setzen.

# 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
  $$ca \equiv cb \mod m \Rightarrow a \equiv b \mod \frac{m}{\mathtt{ggT}(m, c)}$$
- Möchte man $ax \equiv b \mod m$ lösen und man kann nicht durch $a$ teilen, kann man mit dem Inversen von $a$ multiplizieren. Man erhält dann $x \equiv a^{-1}b \mod m$.
- Ist bei der Kongruenz $ax \equiv b \mod m$ der $\mathtt{ggT}(a, m)$ kein Teiler von $b$, dann ist die Kongruenz nicht lösbar.
- 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
  $$(\mathbb{Z}/n\mathbb{Z})^* = \{k + n\mathbb{Z} \,|\, \mathtt{ggT}(k, n) = 1\}$$
- $|(\mathbb{Z}/n\mathbb{Z})^*| = \varphi(n)$ 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** Fur alle $n \in N$ gibt es ein $N \in \mathbb{N}$, so dass jeder Graph mit $N$ Knoten eine Clique der Größe $n$ oder eine unabhängige Menge der Größe $n$ enthält.

# 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**
$$C_n = \frac{1}{n+1}\binom{2n}{n} = \frac{1}{2n+1}\binom{2n+1}{n} \sim \frac{4^n}{n\sqrt{\pi n}}$$
**Dyckwörter** $D_n$ ist die Menge der Dyckwörter mit $n$ Klammerpaaren, d.h. Länge $2n$. $|D_n| = C_n$.
**Saturierte Binärbäume** Binärbäume, dessen Knoten entweder zwei oder keine Nachfolger haben. Zuordnung von Saturierten Bäumen zu normalen Binärbäumen ist bijektiv durch Weglassen aller Blätter. Es gibt $C_n$ viele saturierte Binärbäume mit $n$ inneren Knoten.
- **Abschätzungen von Laufzeiten**
$$n^n \in \omega(n^c n!) \text{ bzw } n! \in o(n^n)$$
$$\log(n!) \in \Theta(n \log n) = \Theta(\log(n^n))$$
$$\log(\sqrt{n}) \in \Theta(\log n))$$
$$a^n \in \omega(b^n) \text{ für } a > b$$
- **Binomialkoeffizient** Durchschnittswert der Binomialkoeffizienten
$$\binom{n}{\lfloor \frac{n}{2} \rfloor} = \binom{n}{\lceil \frac{n}{2} \rceil} > \frac{2^n}{n}$$
- **Stirlingformel**
$$n! \sim \sqrt{2\pi n} \cdot (\frac{n}{e})^n$$
- **Kleinstes Gemeinsames Vielfaches** $\mathtt{kgV}(n) = \mathtt{kgV}(2, \ldots, n)$.
$$2^{n-1} < \mathtt{kgV}(n) < 4^{n-1}$$
das zweite falls $n \geq 7$ und für alle $m, n \in \mathbb{N}$, $1 < m < n$ gilt
$$m\binom{n}{m} \text{ teilt } \mathtt{kgV}(n)$$
- **Primzahldichte** $\pi(n)$ sind die Zahlen kleiner gleich $n$.
$$\frac{n}{\log_2 n} \leq \pi(n) \leq \frac{(1+\epsilon)n}{\log_2 n}$$
**Bertrand'sches Postulat** Für alle $n \in \mathbb{N}$ existiert eine Primzahl $n < p \leq 2n$

# 7 Sonstiges

- **Markov-Ungleichung** Sei $\forall \omega : X(\omega) \geq 0$ und $E(X) > 0$, dann
$$\forall \lambda > 0 : \quad P(X \geq \lambda E(X)) \leq \frac{1}{\lambda}$$
- **Bernoulli-Ungleichung** $x \geq -1$, dann ist $(1+x)^n \geq 1 + nx$
- $Var(X) = E(X^2) - E(X)^2 = E((X - E(X))^2)$.
- $Var(a \cdot X + b) = a^2 \cdot X, Var(X + Y) = Var(X) + Var(Y)$
- **Kombinatorik** Zurücklegen / Reihenfolge
  - Ja/Ja: $n^k$
  - Nein/Ja: $k!\binom{n}{k}$
  - Ja/Nein: $\binom{n+k-1}{k}$
  - Nein/Nein: $\binom{n}{k}$

  **Partitionszahlen** Auf wieviele Arten kann man $n$ als Summe von $k \in \mathbb{N}$ schreiben? Diese Anzahl nennen wir $P(n, k)$. Z.B. Aufteilung einer $n$-elementigen Menge in $k$ nichtleere Teilmengen.
$$P(n,k) = P(n-1, k-1) + P(n-k, k) = \sum_{j \leq k} P(n-k, j)$$