Diskrete Mathematik Zusammenfassung

Umrechnung Kommazahl zu Bruch

$$\frac{\text{fixe Nachkommastelle}}{10^{\text{Länge}}} + \frac{\text{fortlaufende Nachkommastelle}}{10^{\text{Länge(fortlaufend)}} \cdot \text{wiederholende Anzahl 9}\text{ stelle}}$$

$$\Rightarrow 0.13\overline{72} = \frac{13}{100} + \frac{72}{99 \cdot 100} = \frac{1359}{9900} = \frac{151}{1100}$$

$$0.123\overline{45} = \frac{123}{1000} + \frac{45}{99 \cdot 1000} \overset{\text{gekürzt}}{\Rightarrow} \frac{679}{5500}$$

Umrechnung in Dezimalsystem

$$(x_n x_{n-1} \cdots x_1 x_0) = \sum_{j=0}^{n-1} x_j \, b^j$$

x_j: Ziffer der Zahl; b: Basis des Systems

$$\Rightarrow (123)_8 = 1 \cdot 8^2 + 2 \cdot 8^1 + 3 \cdot 8^0 = 64 + 16 + 3 = (83)_{10}$$

Umrechnung in andere Basis von Dezimal

$$\begin{aligned} y : b &= y_1 \quad \text{Rest } z_1 \\ y_1 : b &= y_2 \quad \text{Rest } z_2 \\ y_{n-1} : b &= 0 \quad \text{Rest } z_n \end{aligned} \Bigg\} \text{ umgerechnete Zahl} = (z_n z_{n-1} \cdots z_2 z_1)$$

$\Rightarrow (123)_{10}$ in $b = 16$

$123 : 16 = 7$ Rest $11 = B$

$7 : 16 = 0$ Rest $7 = 7$

$= (7B)_{16}$

ASCII

a	= 97	A	= 65	0	= 48
⋮		⋮		⋮	
z	= 122	Z	= 90	9	= 57

Gleichung mit modulo

Gleichung (modulo x) = alle Koeffizienten (modulo x)

$$\Rightarrow \underbrace{123}_{1} \cdot \underbrace{456}_{4} + \underbrace{78}_{1} \pmod 9 = \underline{\underline{6}}$$

$$= \underbrace{6 \cdot 6}_{36} + 6 \pmod 9$$

$$= \underbrace{36}_{0} + 6 \pmod 9$$

$$= 0 + 6 \pmod 9$$

$$= \underline{\underline{6}}$$

Euklid

GGT (40, 215)

$$\Rightarrow 215 = 5 \cdot 40 + \underline{15}$$

$$40 = 2 \cdot 15 + \underline{10}$$

$$15 = 1 \cdot 10 + \underline{5}$$

$$10 = 2 \cdot 5 + \underline{0} \Rightarrow \underline{\underline{\text{GGT ist } 5}}$$

Erweiterter Euklid

Berechnung von $ggT(a,b)$ und x,y sodass $ax+by=ggT(a,b)$

Aufgabe: finde alle $x,y \in \mathbb{N}$ sodass $68x+23y=1000$

wir definieren $68x + 23y = ggT(68,23)$

zuerst berechnen wir $ggT(68,23)$ mit Euklid

Iteration / $ggT(a,b)$ — Quotient wie viel b in a passen — Rest

i	a	b	q	r	x	y
1	68	23	2	22	-1	3
2	23	22	1	1	1	-1
3	22	1	22	0 ggT	0	1

$x_i = y_{i+1}$

$y_i = x_{i+1} - q_i \cdot y_{i+1}$

beginne von unten mit $x=0$ & $y=1$

Bei allen Schritten gilt: $a \cdot x + b \cdot y \overset{!}{=} ggT(a,b)$

$\Rightarrow$ da $x=-1$ und $y=3$ eine Lösung von $68x+23y=1$ ist, ist $x=-1000$ und $y=3000$ eine Lösung für $68x+23y=1000$

$\Rightarrow$ allgemein $x = -1000 + 23k$

$y = 3000 - 68k$

multiplikatives Inverses

Berechnung durch erw. Euklid

a^{-1} existiert, wenn $ggT(a,b) = 1$

nach erw. Euklid erhalten wir $ax + by = 1$

Inverses ist dann $x = a^{-1} \mod b$

Wochentag Formel

0 = Montag, 1 = Dienstag, ...

Anzah Tage $\mod 7$

$\Rightarrow$ 1.1.1900 – 15.5.1955

$= \underbrace{55 \cdot 365}_{\text{ganze Jahre}} + \underbrace{13}_{\text{Schaltjahre}} + \underbrace{31 + 28 + 31 + 30 + 14}_{\text{von 1.1. – 15.5}} \mod 7$

$= 6 =$ Sonntag

$ISBN_{10}$

$ISBN_{10} = z_1 z_2 \cdots z_{10}$

Prüfgleichung

$$\sum_{i=1}^{10} (11-i) z_i = 0 \pmod{11}$$

Berechnung Prüfziffer

$$\sum_{i=1}^{9} i z_i \mod 11 = -\sum_{i=1}^{9} (11-i) z_i \pmod{11} = z_{10}$$

ISBN$_{13}$

ISBN$_{13}$ = $z_1 z_2 \dots z_{13}$

Prüfgleichung

$$\underbrace{(z_1 + z_3 + z_5 + \dots + z_{11} + z_{13})}_{\text{Summe aller ungeraden Stellen}} + 3\underbrace{(z_2 + z_4 + z_6 + \dots + z_{10} + z_{12})}_{\text{Summe aller geraden Stellen}} = 0 \mod 10$$

Berechnung Prüfziffer

$$-(z_1 + z_3 + z_5 + \dots + z_{11}) + 3(z_2 + z_4 + z_6 + \dots + z_{10} + z_{12}) = z_{13} \mod 10$$

RSA

- wähle zwei grosse primzahlen p und q
- multipliziere diese $n = pq$
- wähle eine Zahl e, die coprime ist zu $(p-1)(q-1)$
- berechne das Inverse $d = e^{-1} \mod((p-1)(q-1))$

⇒ privater key = d

public key = n und e

Verschlüsselung von Nachricht m als c

$$c = m^e \mod (n)$$

Entschlüsselung

$$m = c^d \mod (n)$$

Chinesischer Restsatz

Sind n_1 und n_2 coprime, dann gibt es nur eine Lösung für

$x = a \mod n_1$

$x = b \mod n_2$

$\Rightarrow x = a t n_2 + b s n_1$ || s und t sind die Resultate vom erweiterten Euklid, sodass $s n_1 + t n_2 = 1$

Fermats Theorem

Ist p eine Primzahl, gilt für alle $a \in \mathbb{N}$

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

Eulers Funktion & Theorem

Euler Funktion $\varphi(n) \rightarrow$ alle Zahlen die coprime zu n und kleiner als n sind.

Ist p prim gilt: $\varphi(p) = p-1$

Für $k \in \mathbb{N}$ gilt: $\varphi(p^k) = p^{k-1}(p-1)$

Für p und q coprime gilt: $\varphi(pq) = (p-1)(q-1)$

Euler Theorem

Für alle $a, n \in \mathbb{N}$ wenn $GGT(a,n) = 1$ gilt:

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

Gruppe

$(G, \circ)$ ist genau dann eine Gruppe, wenn

$a, b \in G$ sind und die Verknüpfung der zwei Elementen

$a \circ b \in G$

kann jede Operation sein $(+, -, \cdot)$

und folgendes gilt:

1. $(a \circ b) \circ c = a \circ (b \circ c)$ → assoziativ
2. $\exists n \in G: n \circ a = a \circ n = a \quad \forall a \in G$

   (neutrales Element n ist 1 bei Multiplikation und 0 bei Addition)
3. $\forall a \in G \; \exists a^{-1} \in G: a \circ a^{-1} = a^{-1} \circ a = n$ → inverses Element

gilt ausserdem noch

4. $a \circ b = b \circ a \quad \forall a, b \in G$ → kommutativ

dann ist $(G, \circ)$ eine kommutative / Abelsche Gruppe

Körper

(z.B $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_{prim}$)

$(K, +, \cdot)$ heisst genau dann Körper, wenn

1. $(K, +)$ ist eine kommutative Gruppe mit neutralem Element 0
2. $(K \setminus \{0\}, \cdot)$ ist eine kommutative Gruppe mit neutralem Element 1
3. $\forall a, b, c \in K: a \cdot b + a \cdot c = a(b + c)$ → Distributivgesetz

Ringe (z.B $(\mathbb{Z}, +, \cdot)$)

Eine Menge R mit Verknüpfungen $+, \cdot$ heisst Ring, wenn

1. $(R, +)$ ist ein **kommutative Gruppe** mit **neutralem Element** 0
2. $\forall a,b,c \in R: \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$ → **assoziativ**
3. $\forall a,b,c \in R: \quad a \cdot b + a \cdot c = a \cdot (b + c)$ → **distributiv**

gilt zusätzlich

4. $\forall a,b \in R: \quad a \cdot b = b \cdot a$
5. $\exists 1 \in R: 1 \cdot a = a \cdot 1 = a \quad \forall a \in R$

dann ist R ein **kommutativer Ring mit 1**

Polynome

beliebiger Körper

Funktion $p: K \to K$ der Form

$p(x) = \sum_{i=0}^{d} a_i x^i$ mit $a \in K$ und $d \in \mathbb{N}_0$ heisst polynom.

Wenn $a_d \neq 0$, dann ist $d = \underset{\text{Grad}}{\deg}(p)$

(Grad eines Nullpolynoms ist per def $-\infty$)

Wenn $a_d = 1$, dann ist das polynom normiert/monisch $(x^2 + 2x + 3)$

$K[x] = \{ \sum_{i=0}^{n} a_i x^i \mid a_i \in K \}$

Koeffizienten sind in K

Ist ein kommutativer Ring mit 1 (auch Polynomring über K)

(z.B $x^4 + 2x^3 + 1 \in \mathbb{Z}_3[x]$ ⇒ Operationen werden in $\mathbb{Z}_3$ ausgeführt, also mod 3)

Restklassenring $K[x]\ m(x)$

Zwei Polynome $p(x), q(x) \in K[x]$ heissen kongruent modulo $m(x)$ wenn die Division durch $m(x)$ den gleichen Rest $r(x)$ $r \in K[x]$ gibt

$$p(x) \equiv q(x) \mod m(x)$$

$$\Leftrightarrow p(x) = q(x) + k(x)\, m(x) \quad \text{für ein } k(x) \in K[x]$$

Alle modulo $m(x)$ kongruenten Polynome bilden eine Restklasse modulo $m(x)$

Es gelten die gleichen Regeln wie in $\mathbb{Z}_n$ für Addition, Multiplikation (mit reduktion mod $m(x)$ zusätzlich)

$$\Rightarrow m(x) = 0 \mod m(x)$$

$$\Rightarrow \sum_{i=0}^{\deg(m)} m_i x^i = 0 \mod m(x)$$

$$\Rightarrow x^{\deg(m)} = -\sum_{i=0}^{\deg(m)-1} m_i x^i \mod m(x)$$

Bsp

$m(x) = x^4 - x - 1$

$\Rightarrow x^4 = -(-x-1)$

$x^4 \equiv x+1 \mod x^4-x-1$

Freshmans Dream

$$(a+b)^p = a^p + b^p \mod p$$

Standardrepräsentanten

$$K_{[x]}m(x) = \left\{ \sum_{i=0}^{k-1} m_i x^i \mid m_i \in K \right\}$$

Hat $m(x)$ Grad k dann sind alle möglichen Reste, Polynome in $K_{[x]}$ mit Grad $< k$.

$\Rightarrow$ Dies sind die Standardrepräsentanten der Restklasse mod $m(x)$.

(z.B $m(x) = x^2+1$ in $\mathbb{Z}_3 \Rightarrow \mathbb{Z}_{3[x]}m(x) = \{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}$)

Restklassenring

$(K_{[x]}\, m(x), +, \cdot)$ ist ein Ring (Restklassenring) mit Polynom-Addition und Multiplikation.

Es können 2 Tabellen (mit den Standardrepräsentanten) für die Operationen erstellt werden

(modulo $[x]$ nicht vergessen) + +

⇒ gibt es für jedes nicht-null-Element ein Inverses (resultat = 1 in Tabelle)

ist $K_{[x]}\, m(x)$ ein Körper mit c Elementen.

(nur Dann!)

⇒ Für $p(x) \in K_{[x]}\, m(x)$ gibt es ein Inverses, wenn $ggT(p(x), m(x)) = 1$

kann mit erw. Euklid berechnet werden

Endliche Körper

Ein Polynom heisst irreduzibel, wenn kein anderes Polynom existiert, das es teilt. (Polynom äquivalent zu Primzahl)

reduzible, normierte Polynome kann man als Produkt von irreduziblen Polynomen schreiben: $p(x) = \prod_{i=1}^{n} q_i(x)$ (z.B $x^4+3x^3+2 = (x^2+1)(x^2+2)$)

Isomorphismus

⇒ äquivalenz

⇒ $\mathbb{F}_q = \mathbb{F}_{p^k} = \mathbb{Z}_{p[x]}\, m(x)$ $\quad \| \; k = \deg(m)$ (m irreduzibel)

$\exists$ Isomorph als Vektorraum

(z.B $\mathbb{Z}_{2[x]}\, x^3+x^2+1 \rightarrow \mathbb{F}_2^3$)

Hamming - Metrik

d_H → in wie vielen Koordinaten unterscheiden sich 2 Vektoren: z.B $\begin{pmatrix}1\\2\\3\end{pmatrix}, \begin{pmatrix}1\\3\\2\end{pmatrix} \rightarrow d_H = 2$

Hamming - Gewicht

wt_H → Distanz von Vektor zum null-Vektor

z.B $\begin{pmatrix}0\\1\\2\end{pmatrix} \rightarrow wt_H = 2$ | $\begin{pmatrix}0\\0\\1\end{pmatrix} \rightarrow wt_H = 1$

Minimaldistanz

$d_H(C)$ → minimum aller Distanzen zwischen allen Codewörtern in C // C ist ein Code über $\mathbb{F}_q$ mit Länge n

Fehlerkorrekturkapazität

$r = c + e$ ~ Fehlervektor

r: empfangenes Wort; c: Codewort

$\Rightarrow d_H(r, c) = wt_H(r - c) = wt_H(e)$

$\Rightarrow$ ist $d_H(C) = d$, dann kann C $d-1$ Fehler erkennen und $\left\lfloor \frac{d-1}{2} \right\rfloor$ Fehler korrigieren

Lineare Codes C

$C \subseteq \mathbb{F}_q^n$ ~ Anzahl Spalten von G

Teilmenge

$\dim(C) = \dim(G)$

$d_H(C)$ = kleinstes Gewicht der Zeilen von H

Generatormatrix G

Zeilen sind die Basis für C

Sie wird verwendet um Nachrichten in ein Codewort zu verwandeln: $c = m \cdot G \quad \forall c \in C$

(c: Codewort, m: Nachricht, G: Matrix)

$c \rightarrow 1 \times n \qquad m \rightarrow 1 \times k$

$G \in \mathbb{F}_q^{k \times n}$ $(k \times n \rightarrow$ Zeilen × Spalten$)$

Dimension von G $\Rightarrow$ $\dim(G) = k$

Anzahl generierbare Codewörter $= q^k$

G in Standardform: $(I_k \mid P)$ $\rightarrow I_k$ = Identitätsmatrix $k \times k$

Kontrollmatrix H

Wenn G in Standardform $\Rightarrow$ $H = (-P^T \mid I_{n-k})$

allgemein: $H^T \cdot G \stackrel{!}{=} \vec{0}$

$\forall c \in C: \quad c \cdot H^T \stackrel{!}{=} \vec{0}$

Kugelpackungsschranke

$$|C| \leq \frac{q^n}{\sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} (q-1)^i}$$

$\Rightarrow$ Anzahl mögliche Codewörter ohne Überschneidungen

$\Rightarrow$ hat es genau so viele Codewörter wie möglich sind

$\Rightarrow$ perfekter Code

Singelton - Schranke

$|C| \leq q^{n-d+1}$ // $d = d_H(C)$

Wenn C Linear ist m.t Dimension k: $k \leq n-d+1$

⇒ erreicht ein Code diese Schranke

↳ maximum distance seperable (MDS)

Kardinalität

⇒ Mächtigkeit → Anzahl Elemente in Menge $M = |M| = \#M$

Kardinalität von Differenzen: $|S \setminus T| = |S| - |S \cap T|$

Inklusion & Exklusion Prinzip

$|S \cup T| = |S| + |T| - |S \cap T|$

∪ = Vereinigung (A oder B)
∩ = Gemeinsamkeit (A und B)

⇒ folgt dem Prinzip inkludiert / exkludiert / inkludiert / ...

⇒ alle Mengen inkludiert, dann alle Schnitte von 2 Mengen exkludiert

dann alle Schnitte von 3 Mengen inkludiert usw. ...

Anzahl teilbare Zahlen

Es gibt $\left\lfloor \frac{n}{m} \right\rfloor$ viele Zahlen von 1 - n, die durch m teilbar sind.

Kartesisches Produkt

$|S| = n \Rightarrow |P(S)| = 2^n$

$|P(S)|$ → alle möglichen Kombinationen von den Elementen in S

$S \times T = \{(s,t) \mid s \in S, t \in T\}$

Kombinatorik

	mit Reihenfolge	ohne Reihenfolge
ohne Zurücklegen	$\frac{n!}{(n-k)!}$	$\binom{n}{k} = \frac{n!}{(n-k)! \cdot k!}$
mit Zurücklegen	n^k	$\binom{n+k-1}{k}$

$\binom{n}{k}$ → Kombination ⇒ nCr auf TR

$\frac{n!}{(n-k)!}$ → Permutation ⇒ nPr auf TR

n = gesamt

$r = k$ = entnommen

Eigenschaften von Binomialkoeffizienten

Für $0 \leq k \leq n$: $\binom{n}{k} = \binom{n}{n-k}$

Für $k \geq 1$: $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$

Vandermondsche Identität

$$\sum_{i=0}^{k} \binom{m}{i}\binom{n}{k-i} = \binom{m+n}{k}$$

Binomischer Lehrsatz

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$$

⇒ Pascalisches Dreieck ⇒

$n=0$ 1

$n=1$ 1 1

$n=2$ 1 2 1

$n=3$ 1 3 3 1

$n=4$ 1 4 6 4 1

$n=5$ 1 5 10 10 5 1

$n=6$ 1 6 15 20 15 6 1

$n=7$ 1 7 21 35 35 21 7 1

$n=8$ 1 8 28 56 70 56 28 8 1

$n=9$ 1 9 36 84 126 126 84 36 9 1

$n=10$ 1 10 45 120 210 252 210 120 45 10 1

Leplace

Wahrscheinlichkeit $P(A) = \frac{|A|}{|\Omega|}$ ~ Erwünschte Elemente / ~ Alle möglichen Elemente

g.U falls · $|\Omega| < \infty$

· $P(\{\omega\}) = \frac{1}{|\Omega|}$ für $\forall \omega \in \Omega$ (alle Ergebnisse sind gleich Wahrscheinlich)

$\Omega \rightarrow$ Ereignisraum

$A \rightarrow A \subseteq \Omega \rightarrow$ Ereigniss

Diskrete Wahrscheinlichkeit

(Ω, P) wird diskreter Wahrscheinlichkeitsraum genannt, wenn

1. $P(A) \in [0,1]$ für alle $A \in P(\Omega)$
2. Falls $A \cap B = \{\}$, dann $P(A \cup B) = P(A) + P(B)$
3. $P(\Omega) = \sum_{i=1}^{|\Omega|} P(\omega_i) = 1$ → Wahrscheinlichkeiten aller zu erreichenden Ergebnissen ist 1

   ↳ $P(A) = \sum_{a \in A} P(a)$ für jedes $A \in \Omega$

Bedingte Wahrscheinlichkeit

Raum (Ω, P), Ereignisse $A, B \in \Omega$

Die Wahrscheinlichkeit, dass A eintritt, wenn B ebenfalls eintritt:

$$P(A|B) = \frac{P(A \cap B)}{P(B)}$$

Z.B: Bedingte Wahrscheinlichkeit, dass eine Person Vanille Eis mag wenn er bereits Schokolade mag : $P(\text{Vanille} \mid \text{Schokolade})$

Satz von Bayes

$$P(A|B) = \frac{P(B|A)\,P(A)}{P(B)}$$

generell:

$$P(A) = \sum_{k=1}^{n} P(A \cap E_k) = \sum_{k=1}^{n} P(E_k)\,P(A|E_k)$$

$$P(E_j|A) = \frac{P(E_j)\,P(A|E_j)}{P(A)} = \frac{P(E_j)\,P(A|E_j)}{\sum_{k=1}^{n} P(E_k)\,P(A|E_k)}$$

unabhängige Ereignisse

A und B sind unabhängig, wenn

$$P(A \cap B) = P(A)\,P(B)$$

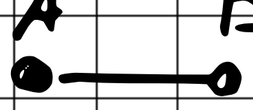
↳ $P(A|B) = P(A)$

↳ $P(B|A) = P(B)$

Graph

$G(V,E)$ || $V \rightarrow$ Menge knoten

|| $E \rightarrow$ Menge kanten $\rightarrow \{a,b\}$ $a,b \in V$



$\Rightarrow$ $V = \{A,B\}$ $E = \{\{A,B\}\} = \{AB\}$

adjazent → zwei knoten durch kante verbunden (benachbart)

inzident → zwei: kanten gleichen Endknoten

↳ kante und knoten, wenn es der Endknoten der kante ist

Grad $deg(A)$ → Anzahl kanten an knoten

isoliert → $deg(A) = 0$

Die Summe aller Grade = 2x alle kanten

$$\sum_{a \in V} deg(a) = 2|E|$$

Äquivalenz

bijektive Abbildung $f: V \rightarrow V'$

$ab \in E \Leftrightarrow f(a)f(b) \in E'$

↳ gleiche Anzahl knoten

↳ gleiche Anzahl kanten

↳ gleide Anzahl knoten mit Grad i für alle i

↳ (die Nachbarschaft muss ebenfalls gleich sein im Grad)

Wege und Kreise

Kantenzug → Folge von inzidenten Kanten (ab, bc, cd)

geschlossener Kantenzug → Endpunkt = Startpunkt

Länge → Anzahl durchlaufene Knoten

Weg → alle Knoten sind voneinander verschieden

Kreis → Weg ausser erster und letzter Knoten sind gleich

Adjazenzmatrix A

$A = (a_{ij}) \Rightarrow a_{ij}$ (von i zu j)

(gibt es keine explizite Kante von einem Knoten zu sich selbst dann $a_{ii} = 0$)

in Matrix: 1 wenn Kante existiert
0 wenn nicht

⇓ ist der Graph gewichtet schreiben wir Gewicht

$A^m \Rightarrow$ jeder Eintrag zählt die Menge der Kantenzüge mit Länge n von i nach j

↳ $a_{jj}^2 = deg(a)$

Zusammenhängende Graphen

ungerichtet

zwischen allen zwei Knoten gibt es einen Weg

gerichtet

stark: für alle $u, v \in V$ ein Weg $(u,v) \& (v,u)$

schwach: Richtung entfernen, Kante behalten

Zusammenhang

- Ein Graph mit n Knoten muss mindestens $n-1$ Kanten haben
- Ein Graph mit $\frac{(n-1)(n-2)}{2}$ Kanten ist (schwach) zusammenhängend

Euler Zug (Euler kreis)

geschlossener Kantenzug der jede Kante genau einmal enthält

- zsm. hängend, ungerichtet → Eulerzug wenn alle Grade gerade sind
- stark zsm. hängend, gerichtet → Eulerzug wenn alle Eingang Grad = Ausgang Grad

geschlossener Eulerzug: Anfang und Ende sind verbunden

Hamilton kreis

ein kreis der jeden Knoten genau einmal enthält

- zsm. hängend, ungerichtet → Hamilton kreis, wenn n Knoten und mindestens $\frac{(n-1)(n-2)}{2} + 2$ Kanten

↳ Einen Hamilton kreis zu finden ist NP-vollständig

⇒ überprüfen easy, finden schwer

Bäume & Wälder

Baum: zsm. hängender Graph ohne kreise

Wald: nicht zsm. hängender Graph; Komponenten sind Bäume

aufspannender Baum → zsm. hängender Graph n Knoten
↳ Baum mit allen n Knoten bilden

Suchbaum

aufstellen: mittleres Element = Wurzel

grösser als Wurzel → rechts, kleiner → links

Quellkodierung & kompression

⇒ mit möglichst wenig Bits infos darstellen

minimale Länge für eine kodierung:

$\lceil \log_{\text{kodierung in Bits (0,1)}} (\text{Anzahl Nachrichten}) \rceil$

mittlere Codelänge

$$L(X,C) = \sum_{i=1}^{n} p_i l_i$$

l_i ~ länge von Codewort c_i

p_i ~ Wahrscheinlichkeit das c_i gesendet wird

wenn alle Codewörter gleiche Länge ℓ haben:

$$L(X,C) = \ell \sum_{i=1}^{n} p_i = \ell$$

Präfixfreie Codierung

kein Codewort ist Präfix eines Anderen

↳ macht eine eindeutige Zerlegung möglich

kompletter kommunikationskanal

Quelle → kompression → Verschlusselung → Entschlusselung → dekompression →