Testfragen zur Vorlesung "Mathematische Grundlagen der Informatik"

Mengen und Reliationen

- Wie Zeigt man Mengnegleichheit?

  ▷ $A = B \iff A \subseteq B$ und $B \subseteq A$

- Wieviele Elemente hat die Menge $M = \Big\{2, \{\emptyset\}, \{1, 3\}\Big\}$?

  ▷ Drei

- Relationen können asymmetrsich oder antisymmetrisch sein. Was für ein Unterschied ist hier?

  ▷ Für antisymmetrischen Relation ist $a \sim_R a$ nicht verboten.

- Wie unterscheidet sich eine Äquivalenzrelation und eine Ordnungsrelation?

  ▷ Beide sind transitiv. Aber eine Ordnungsrelation weder reflexsiv noch symmetrisch ist.

- Warum sind je zwei verschiedene Äquivalenzklassen disjunkt?

  ▷ Hier sollte man den Beweis skizieren. Kurz kann man auch so antworten: Wären zwei Äquivalenzklassen $[a]$ und $[b]$ nicht disjunkt, so könnte man von Element a über ein Element $c \in [a] \cap [b]$ zu dem Element b übergehen (wegen der Transitivität). Da aber die Relation auch reflexiv und symmetrisch ist, bedeutet das, dass *jedes* Element aus $[a]$ äquivalent zu *jedem* Element in $[b]$ sein muss $\Rightarrow$ die beiden Klassen bilden eine einzige Äquivalenzklasse.

- Wenn eine Funktion bijektiv ist, ist dann sie auch surjektiv?

  ▷ Ja!

- Sei A eine endliche Menge. Gebe eine Funktion $f : A \to A$ an, die surjektiv aber nicht injektiv ist.

  ▷ Eine solche Funktion gibt es überhaupt nicht! (Aus Abzählgründen).

- Zwei unendlichen Mengen haben die gleiche Kardinalität, wenn ...?

  ▷ ... wenn es eine Bijektion zwischen diesen Mengen gibt.

- Sei $f \subseteq \{\text{Fahrgäste}\} \times \{\text{Sitzplätze}\}$ eine Relation. Wann ist f eine Funktion? Wann ist f injektiv? Wann ist f surjektiv? Wann ist f bijektiv?

  ▷ f ist eine Funktion $\Rightarrow$ kein Fahrgast nimmt mehr als einen Platz ein
  Injektiv $\Rightarrow$ kein Fahrgast stehen muss
  Surjektiv $\Rightarrow$ kein Platz ist frei
  Bijektiv $\Rightarrow$ alle Plätze sind besetzt und kein Fahrgast stehen muß.

- Sei A eine beliebige Menge. Warum gibt es keine surjektive Abbildung $f : A \to 2^A$?

  ▷ Betrachte die Menge $D := \{a \in A : a \notin f(a)\} \in 2^A$.
  Weil f surjektiv ist $\Rightarrow f(a_0) = D$ für ein $a_0 \in A$.
  Definition von $D \Rightarrow a_0 \in D \iff a_0 \notin f(a_0) = D \Rightarrow$ Widerspruch.

- Warum ist die Menge $\mathbb{R}$ nicht abzählbar?

  ▷ Kantor's Diagonalizierung ...

Graphen

- Wann ist ein Graph zusammenhängend? Wann sind zwei Graphen isomorph? Möge zwei Graphen isomorph sein, was kann man dann über die Grade ihrer Knoten sagen?

  ▷ Zusammenhängend = jeder Knoten von jedem anderen erreichbar ist. Isomorph = man kann den ersten Graphen dürch geeignete Umnummerierung von Knoten zu dem zweiten Graphen überführen. Sind zwei Graphen G_1 und G_2 isomorph, dann mssen für jedes k die beide Graphen die gleiche Anzahl der Knoten von Grad k enthalten.

- Wie unterscheiden sich Euler'sche und Hamilton'sche Kreise? Welche Graphen besitzen Euler'sche Kreise?

  ▷ Euler = jede Kante nur einmal. Hamilton = jeder Knoten nur einmal. Ein Graph hat ein Euler'schen Kreis $\iff$ alle Knoten geraden Grad haben.

- Entnimmt man eine Kante aus einem Baum. Was entsteht dann? Wird in einem Baum eine Kante hinzugefügt, was ensteht dann?

  ▷ Entnimmt man eine Kante aus einem Baum, so entsteht ein Wald. Wird in einem Baum eine Kante hinzugefügt, so ensteht ein Kreis.

- Ein Baum hat N Bläter. Wie tief muss er dann sein?

  ▷ Hat jeder Knoten höchstens b Kinder, so muss der Baum Tiefe mindesten $\log_b N$ haben.

Logik

- Wie lautet die Kontrapositionsregel?

  ▷ $A \to B \iff \neg B \to \neg A$

- Ist $\neg B \to \neg A$ eine Negation von $A \to B$?

  ▷ Nein! Da $\neg(A \to B) \iff \neg(\neg A \vee B) \iff A \wedge \neg B$ aber $\neg B \to \neg A \iff B \vee \neg A$.

- Wie negiert man die Aussagen mit Quantoren? Was ist $\neg(\exists x\ A(x) \to \forall y\ \neg B(y))$?

  ▷ Negiert man so: $\neg\exists P(x) \iff \forall x \neg P(x)$ und $\neg\forall x P(x) \iff \exists x \neg P(x)$. Insbesondare gilt: $\neg(\exists x\ A(x) \to \forall y\ \neg B(y)) \iff \neg(\neg\exists x A(x) \vee \forall y B(y)) \iff \exists x A(x) \wedge \exists y B(y)$

- Gebe die Aussageform (mit Quantoren) für die Aussage "Jede Primzahl ist ungerade" und negiere sie.

  ▷ $\forall x(P(x) \to U(x))$. Negation $\neg(\forall x(P(x) \to U(x))) \iff \exists x \neg(\neg P(x) \vee U(x)) \iff \exists x(P(x) \wedge \neg U(x))$

- Negiere die Induktionsformel $P(0) \wedge \forall n[P(n) \to P(n+1))]$. Wie lautet die Negation in Umgangssprache?

  ▷ Negation: $\neg P(0) \vee \exists n[P(n) \wedge \neg P(n+1)]$. Umgangssprachlich: entweder ist bereits Induktionsbasis falsch oder Induktionsschritt nicht für alle n gilt.

- Warum ist Induktion richtig?

  ▷ Falls $P(n)$ nicht für alle natürlichen Zahlen n gilt, so muß das Prädikat P für mindestens eine Zahl n falsch sein. Sei nun n_0 die *kleinste* von solchen Zahlen. Es muss $n_0 \neq 0$ gelten, da Induktionsbasis richtig ist. Induktionsschritt sagt, dass die Implikation $\neg P(n_0) \to \neg P(n_0 - 1)$ für alle n wahr ist. Also muss das Prädikat P auch für die kleinere Zahl $n_0 - 1$ falsch sein $\Rightarrow$ Widerspruch..

- Was ist schwer an der mathematischen Induktion? Warum ist sie ein *konstruktives* Beweisverfahren?

  $\triangleright$ Aus der Aussage $P(n-1)$ muss den Beweis der Aussage $P(n)$ *konstruieren.*

- Was hat die Induktion mit dem Entwurf von Algorithmen zu tun?

  $\triangleright$ Viele Algorithmen arbeiten *rekursiv*: Mann löst zuerst die kleinere Teilprobleme, dann kombiniert diese Teillösungen um ein größeres Problem zu lösen. Genau wir Induktion: Sie reduziert das Problem zu kleineren.

Kombinatorik

- Warum gilt $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$?

  $\triangleright$ Kombinatorische Definition von $\binom{n}{k} = \#\{$ aller k-Mengen in $[n]\}$ $\Rightarrow$

$$\begin{aligned} \binom{n}{k} &= \#\{\text{ aller } k\text{-Mengen}\} \\ &= \#\{\text{ aller } k\text{-Mengen, die } x \text{ enthalten}\} \\ &+ \#\{\text{ aller } k\text{-Mengen, die } x \text{ nicht enthalten}\} \\ &= \binom{n-1}{k-1} + \binom{n-1}{k} \end{aligned}$$

- Wieviele k-elementige Teilmengen hat eine n-elementige Menge?

  $\triangleright$ $\binom{n}{k} = \frac{n!}{k!(n-k)!}$

- Wieviele gibt es Vektoren $(x_1, \ldots, x_k)$ mit $x_i \in \{1, \ldots, n\}$?

  $\triangleright$ $= n^k$.

- Wieviele Möglichkeiten gibt es einen Vektor $(x_1, \ldots, x_k)$ mit $x_i \in \{1, \ldots, n\}$ und $x_i \neq x_j$ auszuwählen?

  $\triangleright$ $(n)_k = n \cdot (n-1) \cdot \ldots \cdot (n-k+1)$.

- Wieviele Lösungen hat eine Gleichheit $x_1 + \cdots + x_n = k$ unter der Bedignung, dass alle $x_i \geqslant 0$ sind?

  $\triangleright$ $\binom{n+k-1}{k}$

- Was ist $\sum_{i=0}^{n} \binom{n}{i} 2^i =$?

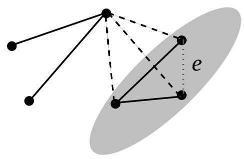
  $\triangleright$ Binomischer Lehrsatz $\Rightarrow$

$$\sum_{i=0}^{n} \binom{n}{i} 2^i = \sum_{i=0}^{n} \binom{n}{i} 2^i 1^{n-i} = (2+1)^n = 3^n$$

- Warum muss es in *jeder* Menge $S \subseteq \mathbb{N}$ von $|S| = 8$ ganzen Zahllen zwei Zahlen $x \neq y \in S$ geben, so dass $x - y$ durch 7 teilbar ist?

▷ Taubenschagprinzip: Tauben = Zahlen in S, Taubenlöcher = $\{0, 1, \ldots, 6\}$
Schicke Taube x in Taubenloch r, falls $x(\bmod 7) = r$
$\#$ Tauben $= 8 > 7 = \#$ Taubenlöcher
$\Rightarrow$ zwei Tauben $x \neq y$ müßen in einem Taubenloch sitzen
$\Rightarrow$ geteilt durch 7 beibe Zahlen denselben Rest ergeben
$\Rightarrow$ $x - y$ muß durch 7 teilbar sein.

- Warum muss es in jeder Gruppe von 6 Leuten 3 Leute geben, die paarweise befreundet oder die paarweise verfeindet sind?

▷ 

- Warum ist $|A \cup B \cup C| =$? Warum?

▷ $|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|$. Warum? Da jedes Element von $A_i \cap A_j$ ist in $|A_i| + |A_j|$ *doppelt* gezählt! Wir brauchen noch $|A_1 \cap A_2 \cap A_3|$ dazu zu addieren, da wir zu viel abgezogen haben!

- Sei K das dürchschnittliche Kapital (in Euro) eines deutchen Bürgers. Betrachte eine Person als "reich", falls sie mindestens $K/2$ Euro besitzt. Zeige, dass die reichen Personen mindestens die Hälfte aller Gelder haben.

▷ Sei $m = \#$ von Personen, $X_i =$ Kapital von Person i, und $X = \sum_{i=1}^{n} X_i$ das gesamte Kapital. Dann ist $K = X/m \quad \Rightarrow \quad X = mK \quad \Rightarrow$

$$\sum_{i \text{ reich}} X_i = X - \sum_{i \text{ arm}} X_i \geqslant mK - m\frac{K}{2} = \frac{1}{2}mK = \frac{1}{2}X.$$

Algebra

- Warum ist der Euklid-Alogorithmus korrekt?

▷ Da $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, a \bmod b)$ gilt.

- Wann hat $a \in \mathbb{Z}_n$ die multiplikative Inverse modulo n?

▷ Genau dann, wenn a relativ prim zu n ist.

- Was ist $2 - 3$ in $\mathbb{Z}_4$?

▷ In $\mathbb{Z}_4$ ist additive inverse von 3 gleich $-3 = 1 \quad \Rightarrow \quad 2 - 3 = 1$ in $\mathbb{Z}_4$.

- Was sind $3/2$ und $2/3$ in $\mathbb{Z}_5$?

▷ $2^{-1} = 3$ und $3^{-1} = 2$ in $\mathbb{Z}_5 \quad \Rightarrow \quad 3/2 = 3 \cdot 3 = 4$ und $2/3 = 2 \cdot 2 = 4$ in $\mathbb{Z}_5$.

- Wie findet man die multiplikative Inverse von 13 modulo 54?

▷ Lasse den Euklicd-Algorithmus laufen. Er findet $\mathrm{ggT}(13, 54) = 1$. Dann verfolge den Verlauf des Algorithmus zurück, um die Zahlen x, y mit $15x + 54y = 1$ zu finden. Dann ist $x \bmod 54$ die multiplikative Inverse von 13 modulo 54.

- Sei p prim. Was ist $a^{-1} \bmod p$?

  ▷ $a^{-1} \bmod p = a^{p-2}$

- Welche Bijektion beschreibt der Chinesischer Restsatz in dem Fall von zwei Gleichungen?

  ▷ Sind p und q relativ prim, so beschreibt dieser Satz eine Bijektion zwischen $\mathbb{Z}_{pq}$ und $\mathbb{Z}_p \times \mathbb{Z}_q$.

- Seien $1 \leqslant a \neq b \leqslant N$ zwei ganze Zahlen. Wieviele primzahlen p mit $p \geqslant M$ mit $a \equiv b(\bmod p)$ kann dann es geben?

  ▷ Höchstens $t \leqslant \log N / \log M$. Warum? Gilt $a \equiv b(\bmod p_i)$ für $i = 1, \ldots, t$, so muß (nach dem Chinesischen Restsatz) auch $a \equiv b(\bmod P)$ mit $P = \prod_{i=1}^{t} p_i$ gelten. Da $a \neq b \Rightarrow P$ muß kleiner als N sein $\Rightarrow M^t < N$ muß gelten $\Rightarrow t \leqslant \log N / \log M$.

- Ist $(\mathbb{Z} \setminus \{0\}, \cdot)$ eine Gruppe? Ist $(\mathbb{Q} \setminus \{0\}, \cdot)$ eine Gruppe? Wann ist $(\mathbb{Z}_n \setminus \{0\}, \cdot)$ eine Gruppe?

  ▷ Nein! Ja! Genau dann, wenn n prim ist.

- Wenn die Kürzungsregel in $(G, \circ)$ gilt, welche Eigenschaften G und $\circ$ noch haben müssen, um eine Gruppe zu bilden?

  ▷ G endlich und $\circ$ assoziativ

- $n \geqslant 2$ sei beliebig. Welche elemente $a \in \mathbb{Z}_n$ eine multiplikative Gruppe bilden?

  ▷ $\mathbb{Z}_n^* := \{a \in \mathbb{Z}_n : a \neq 0 \text{ und } \mathrm{ggT}(a, n) = 1\}$

- Wie lautet der Satz von Lagrange über die Gruppenordnung?

  ▷ $\forall\, U$ Untergruppe von $G \Rightarrow |G| = |U| \cdot \#(\text{Links-Nebenklassen von } U)$

- Sei $(G, \circ)$ eine endliche Gruppe und $a \in G$. Was ist $a^{|G|} =$?

  ▷ $= e$ (das neutrale Element)

- Wann ist eine endliche Gruppe $(G, \circ)$ zyklisch?

  ▷ Wenn $|G|$ eine Primzahl ist

- Wann sind zwei endliche Gruppen $(G, \circ)$ und $(H, *)$ isomorph?

  ▷ Wenn es eine Bijektion $f : G \to H$ mit $f(a \circ b) = f(a) * f(b) =$ gibt.

- Wann sind zei *zykliche* Gruppen $(G, \circ)$ und $(H, *)$ isomorph?

  ▷ Genau dann, wenn $|G| = |H|$

- Was ist die Charakteristik eines endlichen Körpers?

  ▷ Kleinstes n mit $\underbrace{1 + 1 + \cdots + 1}_{n\text{-mal}} = 0$

- Wann ist $(\mathbb{Z}_n, +, \cdot)$ ein Körper?

  ▷ Genau dann, wenn n prim ist. Ist n nicht prim $\Rightarrow$ ist $(\mathbb{Z}_n \setminus \{0\})$ keine Gruppe $\Rightarrow$ ist $(\mathbb{Z}_n, +, \cdot)$ kein Körper. Ist n prim $\Rightarrow$ a^{n-2} ist die multiplikative Inverse von a (kleiner Satz von Fermat) $\Rightarrow$ ist $(\mathbb{Z}_n, +, \cdot)$ ein Körper.

- Wie dividiert man zwei Polynome?

▷ Genau wie ganze Zahlen (mit Rest)

- Wieviele Nullstellen ein Polynom vom Grad n haben kann?

  ▷ $\leqslant n$

- Polynome $p(x)$ und $q(x)$ mögen Grad höchstens d haben. Wie groß kann dann die Menge $A = \{a \in \mathbb{R} : p(a) = q(a)\}$ sein?

  ▷ $|A| \leqslant d+1$. Warum? Da Polynom $p(x) - q(x)$ Grad $\leqslant d$ hat $\Rightarrow$ kann nur $\leqslant d$ verchiedene Nullstellen haben.

- Seien n verschiedene Stellen $a_1, a_2, \ldots, a_n \in \mathbb{R}$ und $b_1, b_2, \ldots, b_n \in \mathbb{R}$ beliebige n Werte. Gebe ein Polynom $p(x)$ vom Grad $\leqslant n-1$ mit $p(a_i) = b_i$ für alle $1 \leqslant i \leqslant n$ an. Viewiele soche Polynome p gibt es?

  ▷ Interpoliationsformel von Lagrange:

$$p(x) := \sum_{i=1}^{n} b_i \prod_{\substack{j=1 \\ j \neq i}}^{n} \frac{x - a_j}{a_i - a_j}.$$

  Es gibt nur einziges solches Polynom. Warum?

Folgen und Reihen

- Wie unterscheiden sich arithmetische und geometrische Folgen?

  ▷ Die Folge (a_n) ist arithmetisch bzw. geometrisch, falls die Differenz $a_{n+1} - a_n$ bzw. der Quotient a_{n+1}/a_n *konstant* ist.

- $\sum_{k=1}^{n} k =$? Wie zeigt man dass?

  ▷ Gauß-Trick: Umkehrung

- $\sum_{k=0}^{n} x^k =$? Wie zeigt man dass?

  ▷ Verschiebungs-Trick: Ist $S_n = \sum_{k=0}^{n} x_k$, dann ist

$$S_n + x^{n+1} = 1 + \sum_{k=0}^{n} x^{k+1} = 1 + x \cdot \overbrace{\sum_{k=0}^{n} x^k}^{S_n} = 1 + x \cdot S_n$$

  $\Rightarrow \ S_n \cdot (x-1) = x^{n+1} - 1 \ \Rightarrow \ S_n = \frac{1-x^{n+1}}{1-x}$ für $x \neq 1$.

- $\sum_{k=1}^{n} \frac{1}{k} = \Theta(?)$

  ▷ Harmonische Reihe $\Rightarrow \sum_{k=1}^{n} \frac{1}{k} = \Theta(\log n)$ [Integralkriterium]

- Warum divergiert die harmonische Reihe $\sum_{k=1}^{\infty} \frac{1}{k}$?

  ▷ Da die Reihe $H_n = \sum_{k=1}^{n} \frac{1}{k}$ monoton und unbeschränkt ist: $H_n = \Omega(\ln n)$.

- Was ist eine Nullfolge? Was ist $\lim_{n\to\infty} x^n$ für eine Zahl x mit $|x| < 1$? Und mit $x > 1$?

  ▷ Nullfolge = eine Folge (a_n) mit $\lim_{n\to\infty} a_n = 0$
  Ist $|x| < 1 \ \Rightarrow \ \lim_{n\to\infty} x^n = 0$
  Ist $x > 1 \ \Rightarrow \ \lim_{n\to\infty} x^n = \infty$

- Eine Folge sei monoton. Wann konvergiert sie?

  ▷ Monotoniekriterium $\Rightarrow$ Genau dann, wenn sie beschränkt ist.

- Was ist $\lim_{n\to\infty}\left(1+\frac{1}{n}\right)^n = ?$

  ▷ Die Euler-Zahl e.

- (a_n) sei eine monoton fallende und $\lim_{n\to\infty} a_n = 0$. Konvergiert dann die Reihe $\sum_{n=1}^{\infty} a_n$?

  ▷ Nicht unbedingt! Gegenbeispiel: Harmonische Reihe $H_n = \sum_{k=1}^{n} \frac{1}{k}$.

- (a_n) sei *keine* fallende Nullfolge. Kann dann die Reihe $\sum_{n=1}^{\infty} a_n$ immer noch konvergent sein?

  ▷ Nein!

- Was besagt das Cauchy-Kriterium für Folgen?

  ▷ Für Folgen $\Rightarrow$ Egal wie klein die (von ϵ bestimmte) Umgebung ist, kommt die Folge irgendwann mal hinein und bleibt für immer da.

- f ist stetig und die Folge $a_{n+1} = f(a_n)$ konvergiert . Wie bestimmt man dann den Grenzwert $a = \lim_{n\to\infty} a_n$?

  ▷

$$\begin{aligned} a &= \lim_{n\to\infty} a_n = \lim_{n\to\infty} a_{n+1} = \lim_{n\to\infty} f(a_n) \\ &\overbrace{=}^{\text{stetigkeit}} f\big(\lim_{n\to\infty} a_n\big) \\ &= f(a) \end{aligned}$$

- Sei $b \in \mathbb{R}$, $b > 0$ fest. Sei $a_0 > 0$ und $a_{n+1} = \frac{1}{2}\left(a_n + \frac{b}{a_n}\right)$ Warum $\lim_{n\to\infty} a_n = \sqrt{b}$ gilt?

  ▷ Die Folge ist monoton fallend $a_n \geqslant a_{n+1}$ (warum?!) und beschränkt: Aus $a_0 > 0$ folgt $a_n > 0$ für alle n. Nach dem Monotoniekriterium existiert $a = \lim_{n\to\infty} a_n$. Dann ist mit $f(x) := \frac{1}{2}\left(x + \frac{b}{x}\right)$

$$\begin{aligned} a &= \lim_{n\to\infty} a_n = \lim_{n\to\infty} a_{n+1} = \lim_{n\to\infty} f(a_n) \\ &\overbrace{=}^{\text{stetigkeit}} f\big(\lim_{n\to\infty} a_n\big) = f(a) \\ &= \frac{1}{2}\left(a + \frac{b}{a}\right) \end{aligned}$$

  und damit gilt $a^2 = b$.

- $\sum_{k=0}^{\infty} x^k = ?$

  ▷ $= \frac{1}{1-x}$ für $|x| < 1$; divergiert für $|x| \geqslant 1$.

- Wann konvergiert bzw. divergiert die Reihe $\sum_{n=1}^{\infty} \frac{1}{n^a}$?

  ▷ Konvergiert für $a > 1$, sonst divergiert.

- Warum gilt $0,9999999\ldots = 1$?

  ▷ Da $0,9999999 = \sum_{k=0}^{\infty} 0,9 \cdot 10^{-k}$ eine geometrische Reihe mit dem Grenzwert $0,9 \cdot \frac{1}{1-\frac{1}{10}} = 1$ ist.

- Wozu ist *absolute* Konvergenz gut?

  ▷ Mit absolut konvergierenden Reihen kann man alles was man will machen: Man kann mit solchen Reihen wie mit *endlichen* Summen umgehen. Insbesondare kann man solche Reihen beliebig umordnen.

- Majoranten-, Wurzel- und Quotientenkriterien für absolute konvergenz.

  ▷ Die Reihe $\sum_{k=0}^{\infty} a_k$ ist absolut konvergent,wenn für fast alle k und für eine Konstante $0 < \theta < 1$ entweder $\sqrt[k]{|a_k|} < \theta$ (Wurzelkriterium) oder $\left|\frac{a_{k+1}}{a_k}\right| \leqslant \theta$ und $a_k \neq 0$ (Quotientenkriterium) gilt. Außerdem, ist $\sum_{k=0}^{\infty} a_k$ absolut konvergent auch wenn eine eine konvergente Reihe $\sum_{k=0}^{\infty} b_k$ gibt, so dass $|a_k| \leqslant b_k$ für fast alle k gilt (Majorantenkriterium).

- Wann konvergiert bzw. divergiert die Potenzreihe $\sum_{n=0}^{\infty} a_n(x-x_0)^n$?

  ▷ Konvergenzradius R ist durch $R = \frac{1}{r}$ gegeben wobei $r = \limsup\limits_{n\to\infty} \sqrt[n]{|a_n|}$ Die Reihe absolut konvergiert, falls $|x - x_0| < R$ und divergiertz, falls $|x - x_0| > R$.

- Was sag die Regel von der l'Hospital? Wozu ist diese Regel gut?

  ▷ Gut für Grenzwertbestimmung unbestimmten Ausdrücke der Form $\frac{0}{0}$ oder $\frac{\infty}{\infty}$.

Asymptotische Notation $\Rightarrow$ **klein-o und groß-O**

- Sei $f = o(g)$. Gilt dann $f = O(g)$? Und wie mit $g = O(f)$?

  ▷ $f = O(g)$ aber $g = O(f)$ gilt nicht! Z.B. ist $f = \sqrt{x}$ und $g = x$, so gilt $f = o(g)$ aber $x \neq O(\sqrt{x})$, da $\frac{g}{f} = \sqrt{x} \to \infty$

- Sei $f = O(g)$. Kann dann auch $f = o(g)$ gelten? Und wie mit $g = o(f)$?

  ▷ $f = o(g)$ kann dann auch gelten, $g = o(f)$ aber nicht! Warum? Weil $f = O(g) \quad \Rightarrow \quad f(x) \leqslant c \cdot g(x)$ $\Rightarrow \quad \frac{g}{f} \geqslant \frac{1}{c} > 0$.

- Sei $f = \Theta(g)$. Gilt dann $f = O(g)$? Und wie mit $g = O(f)$?

  ▷ $f = \Theta(g) \iff f = O(g)$ und $g = O(f)$.

- Folgt aus $f_1(n) = O(n), \ldots, f_n(n) = O(n)$, dass auch $f_1(n) + \ldots + f_n(n) = O(n)$?

  ▷ Nicht unbedingt! Wir haben nur die Ungleichungen $f_1 \leqslant c_1 g_1, \ldots, f_n \leqslant c_n g_n$, was uns $\sum_{i=1}^{n} f_i(n) \leqslant \sum_{i=1}^{n} c_i g_i(n)$ liefert. Und $c_1 + \ldots + c_n$ kann mit wachsendem n wachsen, d.h. keine absolute Konstante mehr sein.

- Ist $(\log_2 n)^{100} = o(n^{1/100})$?

  ▷ Ja! Es gilt $(\log n)^a = o(n^b)$ für beliebige Konstanten $0 < b \leqslant a$, auch wenn a sehr groß und b sehr klein ist (Skript)

- Ist $n^{100} = o(2^{n/1000})$?

  ▷ Ja1 Skript.

- Ist $\sqrt{n} = o\left(2^{\sqrt{\log_2 n}}\right)$?

  ▷ Nein, da $\sqrt{n} = 2^{(\log_2 n)/2}$

- Ist $\sqrt{n}^{\log_2 n} = o\left(n^{\sqrt{\log_2 n}}\right)$?

▷ Nein, da $\log(\sqrt{n}^{\log n}) = (\log^2 n)/2$ und $\log\left(n^{\sqrt{\log_2 n}}\right) = \log^{3/2} n = o(\log^2 n)$

- Folgt aus $f(n) = o(g(n))$ auch $\ln f(n) = o(\ln g(n))$?

▷ Nicht unbedingt! Beispiel: $f(n) = n$, $g(n) = n^2 \quad \Rightarrow \quad \ln f(n) = \Theta(\ln g(n))$

- Sei $\ln f(n) = o(\ln g(n))$. Gilt dann auch $f(n) = o(g(n))$?

▷ Ja! Denn:

$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = \lim_{n\to\infty} \frac{e^{\ln f(n)}}{e^{\ln g(n)}} = \lim_{n\to\infty} e^{\ln f(n) - \ln g(n)} = e^{-\infty} = 0$$

- Wir wissen, dass $4^n \neq O(2^n)$. Und wie mit $\left(\frac{5}{4}\right)^n = O\left(\frac{3}{2}\right)^n$?

▷

$$\left(\frac{5}{4}\right)^n / \left(\frac{3}{2}\right)^n = \left(\frac{5}{6}\right)^n \to 0 \quad \text{da } 5/6 \text{ kleiner als 1 ist}$$

Also gilt nicht nur $\left(\frac{5}{4}\right)^n = O\left(\frac{3}{2}\right)^n$, sondern auch $\left(\frac{5}{4}\right)^n = o\left(\frac{3}{2}\right)^n$

Wahrscheinlichkeit

- Sei $(\Omega, \Pr)$ ein diskreter Wahrscheinlichkeitsraum. Welche Eigenschaften muss Pr haben?

▷ $\sum_{\omega\in\Omega} \Pr(\omega) = 1$

- Wie berechnet man $\Pr\{A \cup B\}$?

▷ $\Pr\{A \cup B\} = \Pr\{A\} + \Pr\{B\} - \Pr\{A \cap B\}$

- Die Ereignisse A und B seien disjunkt. Gilt dann $\Pr\{A \cup B\} = \Pr\{A\} + \Pr\{B\}$? Und wie mit $\Pr\{A \cap B\} = \Pr\{A\} \cdot \Pr\{B\}$?

▷ $\Pr\{A \cup B\} = \Pr\{A\} + \Pr\{B\}$ gilt, aber $\Pr\{A \cap B\} = \Pr\{A\} \cdot \Pr\{B\}$ gilt im Allgemenen nicht, da in diesem Fall $\Pr\{A \cap B\} = 0$ ist.

- Warum werden in jeder Gruppe von 28 Leuten mindesten zwei denselben Geburtstag mit Wahrscheinlichkeit $> 1/2$ haben? Was ist hier der Wahrscheinlichkeitsraum? Was ist das für uns interessante Ereignis E? Wie berechnet man $\Pr\{E\}$?
- Wann sind zwei Ereignisse (stochastisch) unabhängig?

▷ $\Pr\{A \cap B\} = \Pr\{A\} \cdot \Pr\{B\}$

- Die Ereignisse A und B seien unabhängig. Sind dann auch die Ereignisse A und $\overline{B}$ unabhängig? Und wie mit $\overline{A}$ und $\overline{B}$?

▷ Ja! $\Pr\{A\} \cdot \Pr\{\overline{B}\} = \Pr\{A\}(1 - \Pr\{B\}) = \Pr\{A\} - \Pr\{A\} \cdot \Pr\{B\} = \Pr\{A \cap \overline{B}\}$, da aus $A \cap B$ und $A \cap \overline{B}$ disjunkt $\quad \Rightarrow \quad \Pr\{A\} = \Pr\{A \cap B\} + \Pr\{A \cap \overline{B}\}$.

- Sind zwei Ereignisse unabhängig, so müssen die Ereignisse disjunkt sein. Ist das richtig?

▷ Das ist falsch! Nimm z.B. die Gleichverteilung auf $\Omega = \{1, 2, 3, 4\}$ und Ereignisse $A = \{1, 4\}$, $B = \{2, 4\}$. Dann ist $\Pr\{A \cap B\} = \Pr\{\{4\}\} = \frac{1}{4} = \frac{1}{2} \cdot \frac{1}{2} = \Pr\{A\} \cdot \Pr\{B\}$.

- Sind zwei Ereignisse disjunkt, so müssen die Ereignisse unabhängig sein. Ist das richtig?

▷ Das ist falsch! Nimm einfach ein Ereignis A mit $\Pr\{A\} > 0$ und $\Pr\{\overline{A}\} > 0 \quad \Rightarrow$ stochastische Unabhängigkeit hat nichts mit der Disjunkheit zu tun!

- Wir haben eine Gleichverteilung (Laplace-Verteilung). Wie ist dann die bedingte Wahrscheinlichkeit $\Pr\{A \mid B\}$ zu interpretieren?

  ▷ $\Pr\{A \mid B\}$ ist der Anteil von $A \cap B$ in B, $\Pr\{A \mid B\} = \frac{|A\cap B|}{|B|}$.

- Ich kenne nur die Wahrscheinlichkeiten $\Pr\{A\}$, $\Pr\{B \mid A\}$ und $\Pr\{C \mid A \cap B\}$. Wie sieht dann die Wahrscheinlichkeit $\Pr\{A \cap B \cap C\}$ aus?

  ▷ $\Pr\{A \cap B \cap C\} = \Pr\{A\} \cdot \Pr\{B \mid A\} \cdot \Pr\{C \mid A \cap B\}$ (Multiplikationssatz für Wahrscheinlichkeiten)

- Ich werfe dreimal eine faire Münze. Sei A das Ereignis "es gibt mehr Wappen als Köpfe" und $B =$ "Wappen im dritten Schritt". Sind diese Ereignise unabhängig?

  ▷ Nein! Da $\Pr\{A\} = \Pr\{B\} = 4/8 = 1/2$ und $\Pr\{A \cap B\} = 3/8$

- Ich kenne nur die bedingte Wahrscheinlichkeiten $\Pr\{A \mid B\}$ und $\Pr\{A \mid \overline{B}\}$. Was brauche ich noch, um $\Pr\{A\}$ zu bestimmen? Wie sieht dann $\Pr\{A\}$ aus?

  ▷ Ich brauche nur $\Pr\{B\}$ und $\Pr\{\overline{B}\}$ zu wissen. Dann ist $\Pr\{A\} = \Pr\{B\}\Pr\{A \mid B\} + \Pr\{\overline{B}\}\Pr\{A \mid \overline{B}\}$ (Satz von der totalen Wahrscheinlichkeit)

- Warum sollte der Zuschauer in einem Game-Show (a la "Gehe auf Ganze") die bereits gewählte Tür stets wechseln?

  ▷ Da die Wahrscheinlichkeit 2/3 eine *falsche* Tür auszuwählen viel größer als die 1/3 für die *richtige* Tür.

Zufallsvariablen

- Was hat eine Zufallsvariable mit dem "Zufall" und "Variable" zu tun? Was ist eine Indikatorvariable? Wann sind zwei Zufallsvariablen unabhängig?
- Wann sind zwei Zufallsvariablen X und Y unabhängig?

  ▷ Wenn die Ereignisse $X^{-1}(s)$ und $Y^{-1}(r)$ für alle $s, r \in \mathbb{R}$ unabhängig sind.

- Wie ist die Erwartungswert $\mathrm{E}[X]$ einer Zufallsvariable X definiert? Wie kann man diesen Wert mechanisch interpretieren?

  ▷ Als Maß-Zentrum (ein "gewichteter" Mittelwert).

- Kann der Erwartungswert negativ sein?

  ▷ Ja! Z.B. wenn X nur negative Werte annnimt.

- Sei $X : \Omega \to S$ eine Zufallsvariable mit $S \subseteq \mathbb{N}$. Kann $\mathrm{E}[X]$ kliener als $\min\{s : s \in S\}$ sein? Und wie mit $\max\{s : s \in S\}$?

  ▷ Nein! Sei $S = \{s_1, \ldots, s_n\}$ mit $s_1 < s_2 < \ldots < s_n$, und $p_i = \Pr\{X = s_i\}$. Dann gilt

  $$\mathrm{E}[X] = \sum_{i=1}^{n} s_i p_i < s_1 \iff \sum_{i=2}^{n} s_i p_i < s_1(1 - p_1)$$

  Aber $1 - p_1 = \sum_{i=2}^{n} p_i$. Also sollte dann

  $$\sum_{i=1}^{n} s_i p_i < s_1 (\sum_{i=2}^{n} p_i) = \sum_{i=2}^{n} s_1 p_i$$

  gelten, was unmöglich ist, da s_1 kleiner als alle anderen Zahlen s_i ist. Genauso für $\max\{s : s \in S\}$.

- Sei $X : \Omega \to S$ eine Zufallsvariable. Dann gilt: $X(\omega) = \mathrm{E}[X]$ für mindestens ein $\omega \in \Omega$. Stimmt das?

  ▷ Nein! Gegenbeispiel: Sei $\Pr\{X = 0\} = \Pr\{X = 1\} = 1/2$. Dann ist $\mathrm{E}[X] = 1/2$, weder 0 noch 1.

- X sei eine Indikatorvariable für ein Ereignis A. Wie sehen dann $\mathrm{E}[X]$ und $\mathrm{Var}[X]$ aus?

  ▷ $\mathrm{E}[X] = \Pr\{A\}$ und $\mathrm{Var}[X] = \Pr\{A\} \cdot \Pr\{\overline{A}\}$

- C sei eine Zufallsvariable, die nur einen Wert $c \in \mathbb{R}$ annimt, und X sei eine beliebige Zufallsvariable. Was sind dann: $\mathrm{E}[C] =?$, $\mathrm{Var}[C] =?$, $\mathrm{E}[CX] =?$ und $\mathrm{Var}[CX] =?$

  ▷ $\mathrm{E}[C] = c$, $\mathrm{Var}[C] = 0$, $\mathrm{E}[CX] = c\mathrm{E}[X]$ und $\mathrm{Var}[CX] = c^2\mathrm{Var}[X]$

- X und Y seien beliebige Zufallsvariablen. Was ist dann $\mathrm{E}[X + Y] =?$ Was kann man dann über $\mathrm{Var}[X \cdot Y]$ sagen?

  ▷ $\mathrm{E}[X + Y] = \mathrm{E}[X] + \mathrm{E}[Y]$ gilt immer!
  Aber $\mathrm{E}[X \cdot Y] = \mathrm{E}[X] \cdot \mathrm{E}[Y]$ gilt nur, wenn X und Y unabhängig sind.

- Sei X die Summe von n unabhängigen Bernoulli-Variablen. Dann ist $\Pr\{X = 0\} \leqslant ?$

  ▷ Ist $X = X_1 + \ldots + X_n$ mit $\Pr\{X_i = 1\} = p$, so gilt $\Pr\{X = 0\} = (1 - p)^n$, da das Ereignis $X = 0$ nur dann antreten kann, wenn $X_1 = X_2 = \ldots = X_n = 0$ ist.

- Für welche Zufallsvariablen X gilt $\mathrm{E}[X] = \sum_{i=0}^{\infty} \Pr\{X > i\}$?

  ▷ Für Zufallsvariablen $X : \Omega \to \mathbb{N}$

- Wie ist die Varianz $\mathrm{Var}[X]$ einer Zufallsvariable definiert? Was beschreibt diese Zahl? Kann die Varianz negativ sein?

  ▷ Varianz von X = Erwartunswert von $(X - \mathrm{E}[X])^2$. Diese Zahl ist gleich $\mathrm{E}\left[X^2\right] - \mathrm{E}[X]^2$. Aus $(X - \mathrm{E}[X])^2 \geqslant 0$ folgt $\mathrm{Var}[X] \geqslant 0$.

- Wir wissen, dass $\mathrm{E}[X + Y] = \mathrm{E}[X] + \mathrm{E}[Y]$ für beliebigen Zufallsvariablen gilt. Gilt auch $\mathrm{Var}[X + Y] = \mathrm{Var}[X] + \mathrm{Var}[Y]$?

  ▷ Nur wenn X und Y unabhängig sind! Ist z.B. $Y = -X$ und $\mathrm{Var}[X] > 0$, so gilt $\mathrm{Var}[X + Y] = \mathrm{Var}[0] = 0$ aber $\mathrm{Var}[X] + \mathrm{Var}[Y] = \mathrm{Var}[X] + \mathrm{Var}[-X] = 2\mathrm{Var}[X] > 0$.

- Ich würfle einen Spielwürfel bis eine 5 rauskommt und summieren die bis dahin erschienene Augenzahlen. Welchen Erwartungswert hat diese Summe?

  ▷ Erwartete Augenzahl in einem Wurf ist $\frac{1}{6}(1 + 2 + 3 + 4 + 5 + 6) = 3,5$.
  Erwartete Anzahl der Wurfe bis eine 5 kommt ist $1/(1/6) = 6$.
  Walds Theorem $\Rightarrow$ erwartete Zahl der gesammelten Augenzahlen ist $3,5 \cdot 6 = 21$.

Verteilungen

- Ich werfe eine faire Münze. Wieviel mal im Durschnitt muss ich die Münze werfen, bis ein "Kopf" kommt?

▷ Zweimal.

- Ich werfe eine unfaire Münze. Die Wahrscheinlichkeit für "Kopf" sei p. Wieviel mal im Durschnit muss ich die Münze werfen, bis ein "Kopf" kommt?

▷ $1/p$ mal, geometrische Verteilung

- Ich werfe n mal eine unfaire Münze. Die Wahrscheinlichkeit für "Kopf" sei p. Wie sieht die Wahrscheinlichkeit dafür aus, dass es genau k mal ein Wappen kommt?

▷ $\binom{n}{k}p^{n-k}(1-p)^k$

- **Binomialverteilung**. Was ist das? Wie sehen $\Pr\{X=k\}$, $\mathrm{E}[X]=$ und $\mathrm{Var}[X]=$ aus?

▷ X = Anzahl der Erfolge in n unabhängigen Versuche mit Erfolgswahrscheonlichkeit p.
$X = X_1 + \ldots + X_n$ mit $\mathrm{E}[X_i] = \Pr\{X_i = 1\} = p$ und $\mathrm{Var}[X_i] = p - p^2 = p(1-p)$
$\Rightarrow$ $\mathrm{E}[X] = \sum_{i=1}^n \mathrm{E}[X_i] = np$
$\Rightarrow$ $\mathrm{Var}[X] = \sum_{i=1}^n \mathrm{Var}[X_i] = np(1-p)$

k Erfolge und $n-k$ Misserfolge können in genau $\binom{n}{k}$ Reihenfolgen geschehen sein
Jede Reihenfolge tritt mit W'keit $p^k(1-p)^{n-k}$ auf
$\Rightarrow$ $\Pr\{X=k\} = \binom{n}{k}p^k(1-p)^{n-k}$

- **Geometrische Verteilung**. Was ist das? Wie sehen $\Pr\{X=k\}$, $\mathrm{E}[X]=$ und $\mathrm{Var}[X]=$ aus?

▷ X = Anzahl der Schritte eines 0-1 Experiments mit Erfolgswahrscheinlichkeit p bis zum *ersten* Erfolg.
$\Pr\{T=t\} = q^{t-1}p$, $\mathrm{E}[X] = 1/p$ und $\mathrm{Var}[X] = (1-p)/p^2$
Wie beweist man das? $\Rightarrow$ erzeugende Funktionen!

- **Poison Verteilung** mit Parameter λ. Was ist das? Wie sehen $\Pr\{X=k\}$ und $\mathrm{E}[X]=$ aus?

▷ Grenzwert der binomiellen Verteilung $B(n,p)$, wenn $n\to\infty$ und $p=\lambda/n$.
$\Pr\{X=k\} = \frac{\lambda^k}{k!}\mathrm{e}^{-\lambda}$ und $\mathrm{E}[X] = \lambda$.

Das Urnen-Model $\Rightarrow$ Hashing

- m Kugeln sind rein zufällig in n Urnen geworfen.
$X =$ Anzahl der Kugel in der *ersten* Urne $\Rightarrow$ $\mathrm{E}[X] =?$

▷ X_i = die Indikatorvariable für das Ereignis "i-te Kugel fliegt in die erste Urne" $\Rightarrow$

$$\mathrm{E}[X] = \sum_{i=1}^m \mathrm{E}[X_i] = \sum_{i=1}^m \frac{1}{n} = \frac{m}{n}.$$

- m Kugeln sind rein zufällig in n Urnen geworfen.
$X =$ Anzahl der Urnen mit *genau einer* Kugel $\Rightarrow$ $\mathrm{E}[X] =?$

▷ Y_j = Indikatorvariable für das Ereignis "j-te Urne enthält genau eine Kugel" $\Rightarrow$

$$\mathrm{E}[Y_j] = \Pr\{Y_j = 1\} = m\cdot\frac{1}{n}\left(1-\frac{1}{n}\right)^{m-1}$$

$\Rightarrow$

$$\mathrm{E}[X] = \sum_{j=1}^n \mathrm{E}[Y_j] = m\left(1-\frac{1}{n}\right)^{m-1} \sim me^{-(m-1)/n}.$$

- Die Anzahl der Kugeln ist unbegrenzt und k Urnen sind bereits besetzt.
  $Z_k =$ Anzahl Versuche bis bis die Kugel in eine *leere* Urne fliegt $\Rightarrow$ $\mathrm{E}[Z_k] =?$

  $\triangleright$ Die Wahrscheinlichkeit eine leere Urne zu treffen ist $p = (n-k)/n$.
  $\Rightarrow$ Bernoulli-Experiment mit der Erfolgswahrscheinlichkeit p
  $\Rightarrow$ $\mathrm{E}[Z_k] = 1/p = n/(n-k)$ (geometrische Verteilung)

- Die Anzahl der Kugeln ist unbegrenzt.
  $X =$ Anzahl der Versuche bis *keine* Urne leer wird $\Rightarrow$ $\mathrm{E}[X] =?$

  $\triangleright$ Aus $X = Z_0 + Z_1 + \ldots + Z_{n-1}$ $\Rightarrow$

$$
\begin{aligned}
\mathrm{E}[X] &= \sum_{k=0}^{n-1} \mathrm{E}[Z_k] = \sum_{k=0}^{n-1} \frac{n}{n-k} = n \cdot \sum_{k=0}^{n-1} \frac{1}{n-k} \\
&= n \cdot \sum_{j=0}^{n} \frac{1}{j} = nH_n \quad \text{(harmonische Reihe)} \\
&\approx n \ln n.
\end{aligned}
$$

Abweichungen von $\mathrm{E}[X]$

- Wie kann man die Abweichung der Zufallsvariable X von ihrem Erwartungswert $\mathrm{E}[X]$ um mehr als $\pm k$ abschätzen?

  $\triangleright$ Tschebyschev-Ungleichung: $\Pr\{|X - \mathrm{E}[X]| \geqslant k\} \leqslant \frac{\mathrm{Var}[X]}{k^2}$. Es muss nur $\mathrm{E}[X^2] < \infty$ gelten.

- Sei X eine beliebige nicht-negative Zufallsvariable, und $K = \mathrm{E}[X]$ sei ihr Erwartungswert. Wie groß ist dann $\Pr\{X \geqslant 2K\} \leqslant ?$ Und was kann man über $\Pr\{X \leqslant K/2\} \leqslant ?$ sagen?

  $\triangleright$ Markov: $\Pr\{X \geqslant 2K\} \leqslant 1/2$ und $\Pr\{X \leqslant K/2\} = 1 - \Pr\{X > K/2\} > 1/2$.

  Tschebyschev: $\Pr\{X \leqslant K/2\} \leqslant \Pr\{|X - \mathrm{E}[X]| \geqslant K/2\} \leqslant \frac{4\mathrm{Var}[X]}{K^2}$.

- Seien $A_1, A_2, \ldots, A_n$ unabhängige Ereignisse. Wie groß ist die Wahrscheinlichkeit, dass es *kein* der Ereignisse vorkommen wird?

  $\triangleright$ Seien $X_1, \ldots, X_n$ Indikatorvariablen für die Ereignisse $A_1, \ldots, A_n$ und sei $X = X_1 + \ldots + X_n$. Dann ist die Wahrscheinlichkeit, dass kein der Ereignisse vorkommt, gleich $\Pr\{X = 0\}$. Und Chernoff liefert uns: $\Pr\{X = 0\} \leqslant \mathrm{e}^{-\mathrm{E}[X]}$.

- Warum braucht man noch Markov- oder Tschebyschev-Ungleichungen, wenn Chernoff die beste Abschätzung gibt?

  $\triangleright$ Chernoff kann man nur für sehr speziellen Zufallsvariablen – nähmlich für Summen unabhängiger Bernoulli-Variablen – anwenden!

- Wir ziehen rein zufällig und unabhängig von einander zwei k-elementige Teilmengen $\mathbf{A}$ und $\mathbf{B}$ aus $\{1, \ldots, n\}$. Mit welcher W'keit wird ein Element x in $\mathbf{A}$ liegen? Ab welchem k können wir nicht mehr erwarten, dass die Mengen $\mathbf{A}$ und $\mathbf{B}$ disjunkt sind?
  Für welchen k gilt $\Pr\{\mathbf{A} \cap \mathbf{B} = \emptyset\} \leqslant 2^{-100}$? Und $\Pr\{\mathbf{A} \cap \mathbf{B} = \emptyset\} \geqslant 3/4$?

  $\triangleright$ $p := \Pr\{x \in \mathbf{A}\} = \Pr\{x \in \mathbf{B}\} = \binom{n-1}{k-1} / \binom{n}{k} = k/n$

  $X = |\mathbf{A} \cap \mathbf{B}|$ ist eine Summe von n unabhängigen Bernoulli Variablen mit Erfolgswahrscheinlichkeit p^2
  $\Rightarrow$ $\mathrm{E}[X] = p^2 n = k^2/n$ $\Rightarrow$ ab $k \geqslant \sqrt{n}$ werden sich die Mengen (vermutlich) schneiden.

Cherhoff $\Pr\{X=0\} \leqslant \mathrm{e}^{-\mathrm{E}[X]} \quad \Rightarrow$

$$\Pr\{\mathbf{A}\cap\mathbf{B}=\emptyset\} \leqslant \mathrm{e}^{-np^2} = \mathrm{e}^{-k^2/n} \leqslant 2^{-100} \qquad \text{für } k \geqslant 10\sqrt{n}$$

Markov $\Pr\{X \geqslant a\} \leqslant \mathrm{E}[X]/a \quad \Rightarrow$

$$\Pr\{\mathbf{A}\cap\mathbf{B}\neq\emptyset\} = \Pr\{|\mathbf{A}\cap\mathbf{B}| \geqslant 1\} \leqslant np^2 = k^2/n \leqslant 1/4 \qquad \text{für } k \leqslant \sqrt{n}/2$$

- Seien $X_1, X_2, \ldots, X_n$ unabhängige ± 1 Zufallsvariablen mit $\Pr\{X_i=+1\} = \Pr\{X_i=-1\} = 1/2$ und sei $X = \sum_{i=1}^n X_i$. Wie sieht dann $\Pr\{|X| \geqslant 2\sqrt{n}\} \leqslant$ aus?

▷ $\mathrm{E}[X_i]=0$ und $\mathrm{Var}[X_i] = \mathrm{E}\left[X_i^2\right] - \mathrm{E}[X_i]^2 = 1 \quad \Rightarrow \quad \mathrm{Var}[X] = \sum_{i=1}^n \mathrm{Var}[X_i] = n$ (unabhängigkeit!) $\Rightarrow$ (Tschebyschev)

$$\Pr\left\{|X| \geqslant 2\sqrt{n}\right\} \leqslant \frac{n}{(2\sqrt{n})^2} = \frac{1}{4}.$$

- Wie oft muss eine Münze mindestens geworfen werden, damit mit einer Wahrscheinlichkeit von mindestens $3/4$ die relative Häufigkeit von Kopf von erwarteten Wert $p=1/2$ um weniger als $0,1$ abweicht?

▷ Der Münzwurf wird durch eine Folge unabhängiger Zufallsvariablen $X_1, X_2, \ldots$ beschreiben mit $\Pr\{X_i=1\} = \Pr\{X_i=0\} = p = 0,5$. Die relative Häufigkeit von Eins ist durch die Zufallsvariablen $Y_n = (X_1+\ldots+X_n)/n$ gegeben. Gesuch ist n minimal, so dass $\Pr\{|Y_n - 0,5| \geqslant 0,1\} \leqslant 1/4$. Es gilt $\mathrm{E}[Y_n] = \frac{1}{n}\sum_{i=1}^n \mathrm{E}[X_i] = p = 0,5$ und $\mathrm{Var}[Y_n] = \frac{1}{n^2}\sum_{i=1}^n p(1-p) = \frac{1}{4n}$. Aus Tschebyschev $\Rightarrow$

$$\Pr\{|Y_n - 0,5| \geqslant 0,1\} \leqslant \frac{\mathrm{Var}[Y_n]}{0,1^2} = \frac{25}{n}$$

und für $\frac{25}{n} \leqslant 1/4$ muss nun $n \geqslant 100$ gelten.

Lineare Algebra

- Sei $V \subseteq \mathbb{R}^n$ ein Vektorraum und $A \subseteq \mathbb{R}^n$ eine Teilmenge der Vektoren. Welche Relation besteht zwischen den Aussagen $A \subseteq V$ und $\mathrm{span}(A) \subseteq V$?

▷ Die Aussagen sind Äquivalent! Warum? Da V alle Linearkombinationen seiner Vektoren enthält.

- $V \subseteq \mathbb{R}^n$ ist ein Vektorraum. Wann ist $B \subseteq V$ eine Basis von V? Wie ist die Dimension $\dim(V)$ definiert?

▷ Wenn die Vektoren in B linear unabhängig sind und den ganzen Vektorraum aufspannen. Dimension $\dim(V)$ = Anzahl der Vekoren in einer Basis von V

- Wie *beweist* man, dass eine Menge $\{\mathbf{u}_1, \ldots, \mathbf{u}_k\} \subseteq \mathbb{R}^m$ linear unabhängig sind?

▷ Indem man zeigt, dass die Gleichungssystem $A\mathbf{x} = \mathbf{0}$ nur die triviale Lösung $\mathbf{x} = \mathbf{0}$ haben kann, wobei A eine $m \times k$ Matrix mit Spalten $\mathbf{u}_1, \ldots, \mathbf{u}_k$ ist. Warum reicht das?

- Sei A eine $m \times n$ Matrix, und $\mathbf{b} \in \mathbb{R}^m$ ein Vektor, $\mathbf{b} \neq \mathbf{0}$. Ist dann die Menge $U = \{\mathbf{x} : \ \mathbf{x} \in \mathbb{R}^n,\ A\mathbf{x} = \mathbf{0}\}$ ein Vektorraum? Ist dann die Menge $V = \{\mathbf{x} : \ \mathbf{x} \in \mathbb{R}^n,\ A\mathbf{x} = \mathbf{b}\}$ ein Vektorraum?

▷ Die Menge U *ist* ein Vektorraum (da $A(\sum_{i=1}^k \lambda_i \mathbf{x}_i) = \sum_{i=1}^k \lambda A\mathbf{x}_i$ gilt) aber V ist *kein* Vektorraum (denn z.B. aus $A\mathbf{x} = \mathbf{b}$ und $A\mathbf{y} = \mathbf{b}$ folgt $A(\mathbf{x}+\mathbf{y}) = A\mathbf{x} + A\mathbf{y} = 2\mathbf{b} \neq \mathbf{b}$). Die Menge V heißt ein *affiner Raum*.

- Sei A eine $m \times n$ Matrix über $\mathbb{R}$, deren Zeilen linear unabhängig sind. Wie groß ist dann der Spaltenrang von A?

  ▷ Der Spaltenrang ist dann m.

- Sei A eine $m \times n$ Matrix über einem endlichen Körper $\mathbb{F}$ mit $K = |\mathbb{F}|$ Elementen? Wieviele Lösungen hat dann das Gleichungssystem $A\mathbf{x} = \mathbf{0}$?

  ▷ $K^{n-\mathrm{rk}(A)}$ Lösungen, falls $m \leqslant n$, und keine Lösungen sonst. Warum?

- Man kennt $\mathrm{rk}(A)$ und $\mathrm{rk}(A|\mathbf{b})$. Was kann man dann über die Lösungen des Gleichungssystems $A\mathbf{x} = \mathbf{b}$ sagen?

  ▷ $A\mathbf{x} = \mathbf{b}$ ist lösbar $\iff$ $\mathrm{rk}(A) = \mathrm{rk}(A|\mathbf{b})$ gilt.

- Wie funktioniert das Gauß Verfahren für lineare Gleichungssysteme?
- Wir haben eine $m \times n$ Matrix A und haben bereits die erweiterte Matrix $(A|\mathbf{b})$ zu einer Zeilenstufenform transformiert. Wann ist die Gleichungssystem $A\mathbf{x} = \mathbf{b}$ lösbar, universell lösbar, eindeutig lösbar?

  ▷ Lösbar $\iff$ kein Pivotelement in der letzten Spalte (zu $\mathbf{b}$); universell lösbar $\iff$ Anzahl der Pivotelemente = Anzahl der Zeilen; eindeutig lösbar $\iff$ Anzahl der Pivotelemente = Anzahl der Zeilen = Anzahl der Spalten in A

- Was besagt die Cauchy-Schwarz-Ungleichung?

  ▷ $|\langle \mathbf{x}, \mathbf{y}\rangle| \leqslant \|\mathbf{x}\|\|\mathbf{y}\|$

- Was ist eine orthonormale Basis? Warum sind solche Basen gut?

  ▷ $\mathbf{v}_1, \ldots, \mathbf{v}_n$ ist orthonormal, wenn $\|v_i\| = 1$ und $\langle \mathbf{v}_i, \mathbf{v}_j\rangle = 0$ für alle $i \neq j$ gilt.

  Warum sind gut? Ist $\mathbf{v}_1, \ldots, \mathbf{v}_n$ Orthonormalbasis von V $\Rightarrow$ für jedes $\mathbf{x} \in V$:

  $$\mathbf{x} = \sum_{i=1}^{n} \langle \mathbf{x}, \mathbf{v}_i\rangle \, \mathbf{v}_i.$$

  $\Rightarrow$ Darstellung von Vektoren leicht berechenbar ist.

- Was ist ein lineares Code? Was ist seine minimale Distanz? Generator Matrix? Kontorllmatrix?

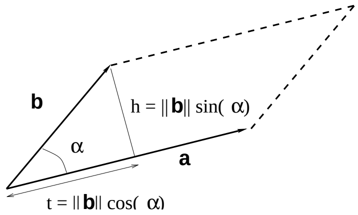
  ▷ Lineares Code = Vektorraum $C \subseteq \mathbb{F}^n$. Minimale Distanz = minimaller Hammingabstand zwischen zwei Vektoren $\mathbf{c} \neq y \in C$. G ist Generatormatrix $\Rightarrow$ $C = \{\mathbf{y}^T \cdot G \,:\, \mathbf{y} \in \mathbb{F}^k\}$. H ist Kontrollmatrix $\Rightarrow$ $C = \{\mathbf{x} \in \mathbb{F}^n \,:\, H \cdot \mathbf{x} = \mathbf{0}\}$

- Was sind Eigenwerte und Eigenvektoren einer Matrix?

  ▷ $M \cdot \mathbf{v} = \lambda \mathbf{v}$

- Wie kann man die Determinante 2×2 Matrizen interpretieren?

  ▷ $\det(\mathbf{a}, \mathbf{b})$ = die Fläche des von $\mathbf{a}$ und $\mathbf{b}$ aufgespannten Parallelogramms



- Was ist die Determinante einer Dreiecksmatrix?

  ▷ Produkt der Diagonaleinträge

- Ist Matrixprodukt kommutativ? Falls nicht, gebe ein Gegenbeispiel.

  ▷ Ist nicht kommutativ! Gegenbeispiel:

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \neq \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

- A ist eine $m \times n$ Matrix und B ist eine $n \times k$ Matrix. Dann ist AB eine $s \times r$ Matrix mit $s =$? und $r =$?

  ▷ Mit $s = m$ und $r = k$

- Wie berechnet man die Inverse A^{-1}? Was ist $(AB)^{-1}$?

  ▷ $(AB)^{-1} = B^{-1}A^{-1}$

- Wann ist eine $n \times n$ Matrix A invertierbar?

  ▷ Genau dann, wenn sie den vollen Rang hat, d.h. $\mathrm{rk}(A) = n$ gilt.

- A sei die Adjazenzmatrix eines Graphen G. Was sind dann die Einträge der k-ten Potenz A^k von A?

  ▷ $A^k[i, j] =$ Anzahl der Wege der Länge von i nach j