Diskrete Mathematik

David Jäggli

16. Mai 2023

Inhaltsverzeichnis

1 Allg

1.1 Grundlagen der Logik und Beweise

- Die Regeln der Logik geben mathematischen Aussagen eine präzise Bedeutung.
- Konstruktion korrekter mathematischer Argumente

1.2 Aussagen (Propositionen)

Propositionen:

- Bern ist die Bundesstadt
- $1 + 1 = 2$
- Goldbachsche Vermutung: sie ist entweder wahr oder falsch, man weis es noch nicht

Keine Propositionen:

- Wie spät ist es?
- $x + 1 = 2$
- Dieser Satz ist falsch.

Begründung: Es handelt sich hier nicht um Aussagen, die entweder wahr oder falsch sind. Eine Aussage ist wahrheitsdefiniert. In einer Aussage darf nicht offen sein ob die Aussage wahr oder falsch sein kann. Sie darf sich auch nicht selbst widersprechen.

2 Operatoren

- Negotiationsoperator: $\neg$
- Konjunktion $\wedge$
- Disjunktion $\vee$
- Implikation $\rightarrow$
- Bikonditional $\leftrightarrow$

2.1 Diskunktion

$p \vee q$
Wenn p oder q wahr ist, ist die Aussage wahr (logic OR).

p	q	$p \vee q$
w	w	w
w	f	w
f	w	w
f	f	f

2.2 Implikation

$p \rightarrow q$
Wenn p dann q

p	q	$p \rightarrow q$
w	w	w
w	f	f
f	w	w
f	f	w

2.3 Bikonditional

$p \leftrightarrow q$
Wenn beide den gleichen Wahrheitswert haben ist die Aussage wahr.
Wahrheitstabelle:

p	q	$p \leftrightarrow q$
w	w	w
w	f	f
f	w	f
f	f	w

2.4 Prioritäten

Operator	Priorität
$\neg$	1
$\wedge$	2
$\vee$	2
$\rightarrow$	3
$\leftrightarrow$	3

3 Aussagen

3.1 Tautologie und Wiederspruch

Tautologie ist eine Aussage, welche immer wahr ist.
Ein Wiederspruch ist eine Aussage, welche immer falsch ist.

3.2 Logische Äquivalenzen

Die Aussage p und q heissen logisch äquivalent, falls $p \leftrightarrow q$ eine Tautologie ist. Man schreibt dann $p \Leftrightarrow q$ oder $p \equiv q$ bzw. $p \sim q$

3.3 Logische Äquivalenzregeln

$p \wedge \mathbf{T} \equiv p$ *)	$p \vee \mathbf{F} \equiv p$	Identität
$p \vee \mathbf{T} \equiv \mathbf{T}$	$p \wedge \mathbf{F} \equiv \mathbf{F}$	Dominanz
$p \vee p \equiv p$	$p \wedge p \equiv p$	Idempotenz
$\neg(\neg p) \equiv p$		Doppelnegation
$p \vee \neg p \equiv \mathbf{T}$	$p \wedge \neg p \equiv \mathbf{F}$	Tautologie/Kontradiktion
$p \vee q \equiv q \vee p$	$p \wedge q \equiv q \wedge p$	Kommutativität
$p \vee (p \wedge q) \equiv p$	$p \wedge (p \vee q) \equiv p$	Absorption
$(p \vee q) \vee r \equiv p \vee (q \vee r)$		Assoziativgesetz 1
$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$		Assoziativgesetz 2
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$		Distributivgesetz 1
$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$		Distributivgesetz 2
$\neg(p \wedge q) \equiv \neg p \vee \neg q$		De Morgan's Gesetz 1
$\neg(p \vee q) \equiv \neg p \wedge \neg q$		De Morgan's Gesetz 2

*) Duale Regeln: $\wedge$ mit $\vee$ vertauschen u. umgekehrt und T mit F.

Weiterführend:
$p \rightarrow q \equiv \neg p \vee q$

Beispiel angewandte logische Äquivalenzregeln
Beispiel 1:
$(p \vee \neg(q \wedge p)) \wedge (r \vee (s \vee r))$
$\equiv (p \vee \neg q \vee \neg p) \wedge (r \vee r \vee s)$
$\equiv (T \vee \neg q) \wedge (r \vee s)$
$\equiv T \wedge (r \vee s)$
$\equiv r \vee s$

Beispiel 2:
$(a \to (b \to c)) \to ((a \to b) \to (a \to c))$
$\equiv (a \to (\neg b \vee c)) \to ((\neg a \vee b) \to (\neg a \vee c))$
$\equiv (\neg a \vee (\neg b \vee c)) \to (\neg(\neg a \vee b) \vee (\neg a \vee c))$
$\equiv (\neg a \vee \neg b \vee c) \to ((a \wedge \neg b) \vee \neg a \vee c)$
$\equiv (\neg a \vee \neg b \vee c) \to ((a \vee \neg a) \wedge (\neg b \vee \neg a) \vee c)$
$\equiv (\neg a \vee \neg b \vee c) \to (\neg b \vee \neg a \vee c)$
$\equiv \mathrm{X} \to \mathrm{X}$
$\equiv \neg\mathrm{X} \vee \mathrm{X}$
$\equiv \mathrm{T}$

4 Quantoren

Wird ein Quantor auf die Variable x angewandt, dann nennt man diese Variable *gebunden*, ansonsten *frei*.

4.1 Prädikate

Ein Prädikat ist ein Wortkonstrukt, welches mindestens eine Variable enthält.
$P(x) =$ "$x > 3$"
Die Aussage $P(4) = 4 > 3$ ist wahr, während $P(2) = 2 > 3$ falsch ist.

4.2 Allquantor

Ist $P(x)$ wahr für alle x aus einer bestimmten Universalmenge, dann schreibt man $\forall x P(x)$. Gelesen wird dies, "für alle x gilt $P(x)$".
Falls es nur auf eine Bestimmte Zahlenmenge zutrifft (z.B. $\mathbb{Z}$) dann schreibt man:
$\forall x \in \mathbb{Z}$ ist wahr.

4.3 Existenzquantor

Ist $P(x)$ wahr für mindestens ein x aus einer bestimmten Universalmenge, dann schreibt man $\exists x P(x)$ und liest: ës existiert ein x für welches $P(x)$ wahr ist".

4.4 Verschachtelte Quantoren

Die Reihenfolge der Quantoren ist wesentlich; ausser alle Quantoren sind vom gleichen Typ (also Allquantoren oder Existenzquantoren)!

5 Beweise

- Ein Satz (Theorem) ist eine Aussage, von der man zeigen kann, dass sie wahr ist.
- Um zu zeigen, dass ein Satz wahr ist, verwendet man eine Abfolge (Sequenz) von Aussagen, die zusammen ein Argument, genannt Beweis ergeben.
- Aussagen können Axiome oder Postulate enthalten (grundlegende Annahmen der mathematischen Strukturen).
- Durch logisches (also gewissen Regeln gehorchendes) schliessen werden Folgerungen gemacht, die zusammen den Beweis ergeben.
- Ein Lemma ist ein einfacher Satz, der in Beweisen von komplizierteren Sätzen verwendet wird.
- Ein Korollar ist eine einfache Folgerung eines Satzes.

6 Mengen

Eine Menge ist eine ungeordnete Zusammenfassung wohldefinierter, unterscheidbarer Objekte, genannt *Elemente*, zu einem Ganzen. Für irgendein Objekt x gilt dann bezüglich der Menge A entweder $x \in A$ oder dann $x \notin A$.
Beispiel:
Endliche Mengen lassen sich durch Aufschreiben der in ihnen enthaltenen Elemente beschreiben. z.B. die Menge aller natürlichen Zahlen kleiner als 101:
$A = 0, 1, 2, ..., 99, 100$ (aufzählend notiert)
$99 \in A$ aber $101 \notin A$ (beschreibend notiert)

andere Schreibweisen sind:

$A = n \in \mathbb{N} | n < 101 = n \in \mathbb{N} : n <= 100 = n | n \in \mathbb{N} \wedge n <= 100$

6.1 Gleichheit, elementare Mengen

Zwei Mengen A und B sind **gleich** ($A = B$), falls sie dieselben Elemente enthalten. $(A \subset B) \wedge (B \subset A)$

Einige bekannte Mengen:
$\mathbb{N}$ - Menge der natürlichen Zahlen ($\mathbb{N}^* = \mathbb{N} \setminus \{0\}$)
$\mathbb{Z}$ - Menge der ganzen Zahlen
$\mathbb{Z}^+$ - Menge der positiven ganzen Zahlen
$\mathbb{Q}$ - Menge der Brüche
$\mathbb{R}$ - Menge der reellen Zahlen
$\mathbb{C}$ - Menge der komplexen Zahlen

6.2 Spezielle Mengen

Teilmenge: A ist Teilmenge von B, geschrieben $A \subset B$, genau dann, wenn $\forall x(x \in A \rightarrow x \in B)$: es gilt $A \subset A$!

Leere Menge: Für jede Menge A gilt: $\emptyset \subset A$.

Kardinalität: Ist S eine endliche Menge, dann bezeichnet $|S|$ die Kardinalität. Die Kardinalität ist die Anzahl Elemente von S.

Potenzmenge: Die Potenzmenge $P(S)$ oder 2^S der Menge S besteht aus der Menge aller Teilmengen $A \subset S$.

Beispiel:
Bestimmen Sie die Potenzmenge von $S = \{1, 2\}$
$S = \{1, 2\}$
$P(S) = 2^S = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$
Es gilt allgemein $|2^S| = 2^{|S|}$

6.3 Das Kreuzprodukt zweier Mengen / kartesisches Produkt

$A \times B = \{(a, b)|a \in A \wedge b \in B\}$
Reihenfolge ist entscheidend, $A \times B \neq B \times A$
$|A \times B| = |A| \cdot |B|$

Beispiel: $A \times B = \{(1, a), (2, a), (3, a), (1, b), (2, b), (3, b)\}$

6.4 Mengenoperationen

6.4.1 Komplement

Ist A eine Teilmenge der Menge M, so bezeichnet

$A^c = \overline{A} = \{m \in M|m \notin A\}$

das Komplement von A bezüglich M.

6.4.2 Durchschnitt

Sind A und B Teilmengen einer Menge M, so bezeichnet

$A \cap B = \{m \in M|m \in A \wedge m \in B\}$

den Durchschnitt von A und B.

6.4.3 Vereinigung

Sind A und B Teilmengen einer Menge M, so bezeichnet

$A \cup B = \{m \in M|m \in A \vee m \in B\}$

die Vereinigung von A und B.

6.4.4 Differenz

Sind A und B Teilmengen einer Menge M, so bezeichnet

$$B \setminus A = \{m \in M | m \in B \wedge m \notin A\}$$

die Differenz

6.5 Set Operatoren

Allg. Operator	Set Operator
$p \vee q$	$A \cup B$
$p \wedge q$	$A \cap B$
$\neg p$	$\overline{A}$

6.5.1 Rechenregeln

Theorem

Für das Rechnen mit Mengen $\mathrm{A}, \mathrm{B}, \mathrm{C} \subseteq \mathrm{M}$ *gelten die folgenden Regeln:*

$\mathrm{A} \cup \mathrm{B} = \mathrm{B} \cup \mathrm{A}$	*Kommutativgesetz*
$\mathrm{A} \cap \mathrm{B} = \mathrm{B} \cap \mathrm{A}$	*Kommutativgesetz*
$\mathrm{A} \cup (\mathrm{B} \cup \mathrm{C}) = (\mathrm{A} \cup \mathrm{B}) \cup \mathrm{C}$	*Assoziativgesetz*
$\mathrm{A} \cap (\mathrm{B} \cap \mathrm{C}) = (\mathrm{A} \cap \mathrm{B}) \cap \mathrm{C}$	*Assoziativgesetz*
$\mathrm{A} \cap (\mathrm{B} \cup \mathrm{C}) = (\mathrm{A} \cap \mathrm{B}) \cup (\mathrm{A} \cap \mathrm{C})$	*Distributivgesetz*
$\mathrm{A} \cup (\mathrm{B} \cap \mathrm{C}) = (\mathrm{A} \cup \mathrm{B}) \cap (\mathrm{A} \cup \mathrm{C})$	*Distributivgesetz*
$\overline{\mathrm{A} \cup \mathrm{B}} = \overline{\mathrm{A}} \cap \overline{\mathrm{B}}$	*De Morgan's Gesetz*
$\overline{\mathrm{A} \cap \mathrm{B}} = \overline{\mathrm{A}} \cup \overline{\mathrm{B}}$	*De Morgan's Gesetz.*

Die duale Rechenregel (jeweils auf den Zeilen 2, 4, 6 *und* 8, *erhält man, indem man* $\cap$ *und* $\cup$ *vertauscht und* $\emptyset$ *mit der Universalmenge* M *(falls diese vorkommen).*

6.5.2 Mengen Identitäten

TABLE 1 Set Identities.

Identity	*Name*
$A \cap U = A$ $A \cup \emptyset = A$	Identity laws
$A \cup U = U$ $A \cap \emptyset = \emptyset$	Domination laws
$A \cup A = A$ $A \cap A = A$	Idempotent laws
$\overline{(\overline{A})} = A$	Complementation law
$A \cup B = B \cup A$ $A \cap B = B \cap A$	Commutative laws
$A \cup (B \cup C) = (A \cup B) \cup C$ $A \cap (B \cap C) = (A \cap B) \cap C$	Associative laws
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	Distributive laws
$\overline{A \cap B} = \overline{A} \cup \overline{B}$ $\overline{A \cup B} = \overline{A} \cap \overline{B}$	De Morgan's laws
$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$	Absorption laws
$A \cup \overline{A} = U$ $A \cap \overline{A} = \emptyset$	Complement laws

7 Funktionen

Wird jedem Element x einer Menge X genau ein Element y einer Menge Y zugeordnet, so heisst die Zuordnung **Funktion**.

7.1 Die ceiling- und floorfunction

$\lceil\cdot\rceil : \mathbb{R} \to \mathbb{Z},\ x \mapsto \lceil x \rceil = \min\{n \in \mathbb{Z} | x \leq n\}$
$\lfloor\cdot\rfloor : \mathbb{R} \to \mathbb{Z},\ x \mapsto \lfloor x \rfloor = \max\{n \in \mathbb{Z} | n \leq x\}$

7.2 Injektive Funktionen

Eine Funktion heisst injektiv, wenn jedes x auf eine eigenes y zeigt.

7.3 Surjektive Funktionen

Eine Funktion heisst surjektiv, falls für jedes Element y ein Element x existiert, so dass $f(x) = y$ gilt.

7.4 Bijektive Funktionen

Eine Funktion heisst bijektiv, falls sie injektiv und surjektiv ist. Das bedeutet, dass jedes Element y genau ein zugehöriges Element x hat.

Bijektive Funktionen sind umkehrbar. Man muss einfach die Pfeile umkehren und damit entsteht aus f die Umkehrfunktion f^{-1}.

7.5 Zusammengesetzte Funktionen

Gegeben seien zwei Funktionen, so dass der Wertebereich von g im Definitionsbereich von f enthalten ist. Dann kann man die so genannte **zusammengesetzte Funktion** oder **Komposition** von f und g bilden:
$F = f \circ g : X \longmapsto Y,\ x \longmapsto f(g(x))$

7.6 Die Caesar-Chiffre

1. **Kodierung:** Buchstaben auf Zahlen abbilden
   K:$\{a,b,c,...,z\} \mapsto \{0,1,2,...,25\}$, wobei $a \mapsto 0, b \mapsto 1, c \mapsto 2, z \mapsto 25$

2. **Verschlüsseln:** die eigentliche Caesar-Verschlüsselung
   V:$\{0,1,2,...,25\} \mapsto \{0,1,2,...,25\}$, $m \mapsto c := (m + 3) \bmod 26$.

3. **Dekodierung:** Zahlen auf Buchstaben abbilden
   D:$\{0,1,2,...,25\} \mapsto \{0,1,2,...,25\}$, wobei $0 \mapsto a, 1 \mapsto b, 2 \mapsto c, 25 \mapsto z$

7.7 Umkehrfunktionen

Wenn man die Umkehrfunktion auf das Ergebnis der Ursprungsfunktion mit einem x-Wert anwendet erhält man wieder x. Heisst:
$f^{-1}(f(x)) = x$

8 Folgen

8.1 Definition

Eine **Folge** ist eine Abbildung von $\mathbb{N}$ (oder auch $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$) in eine Menga A:
$\{\cdot\}:\mathbb{N} \mapsto A$, $n \mapsto a_n$
Man nennt a_n das Glied der Folge mit der Nummer n. Die Folge wird auch mit $\{a_n\}$ oder (a_n) bezeichnet.

Example:
Man schreibe die ersten sechs Glieder der Folge auf, deren k. Glied gegeben ist durch $a_k = \frac{1}{k}$.

$$a_k = \left(1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5} \dots\right)$$

8.2 Die geometrische Folge

Bei einer geometrischen Folge ist der Quotient zweier aufeinander folgender Glieder immer gleich, nämlich q. Das bedeutet, dass $\frac{a_{k+1}}{a_k}$ immer gleich ist.

8.3 Summen

Dank Summenzeichen lassen sich Summen einfacher schreiben:

$$\sum_{j=m}^{n} a_j = a_m + a_{m+1} + a_{m+2} + \cdots + a_n$$

$$\sum_{j=m}^{n} a_j = \sum_{i=0}^{n-m} a_{m+i} = \sum_{k=1}^{n-m+1} a_{m+k-1}$$

Addiert man die Glieder einer arithmetischen Folge (a_k), entsteht die **arithmetische Reihe:**

$$\sum_{k=0}^{n-1} a_k = n\frac{a_0 + a_{n-1}}{2}$$

Nützliche Summenformeln:

Summe	geschlossene Form
$\sum_{k=0}^{n} x^k$	$\frac{x^{n+1}-1}{x-1}$
$\sum_{k=0}^{n} 2^k$	$2^{k+1}-1$
$\sum_{k=1}^{n} k$	$\frac{n(n+1)}{2}$
$\sum_{k=1}^{n} k^2$	$\frac{n(n+1)(2n+1)}{6}$
$\sum_{k=1}^{n} k^3$	$\frac{n^2(n+1)^2}{4}$
$\sum_{k=0}^{\infty} x^k$, $\lvert x\rvert < 1$	$\frac{1}{1-x}$
$\sum_{k=1}^{\infty} kx^{k-1}$, $\lvert x\rvert < 1$	$\frac{1}{(1-x)^2}$

8.4 Produkte

Dank dem Produktzeichen lassen sich Produkte einfacher schreiben:

$$a_m \cdot a_{m+1} \cdot a_{m+2} \ldots a_n = \prod_{j=m}^{n} a_j \qquad n \geqslant m$$

Die Fakultät lässt sich mithilfe des Produktzeichens wie folgt schreiben:

$$n! = \begin{cases} 1 & n = 0 \\ n(n-1)(n-2)\ldots 2 \cdot 1 = \prod_{k=1}^{n} k & n > 0 \end{cases}$$

Nützliche Abkürzung:

$$\prod_{i=1}^{n} i = \frac{n \cdot (n+1)}{2}$$

9 Algorithmen

Ein Algorithmus ist eine endliche Menge von präzisen Instruktionen mit deren Hilfe eine Berechnung ausgeführt oder ein Problem gelöst wird.
Algorithmen haben folgende Eigenschaften:

1. einen genau spezifizierten Input und daraus berechneten Output
2. die Instruktionen sind präzise, korrekt für jeden möglichen Input und in endlicher Zeit durchführbar

Greedy Algorithmen wählen in jedem Schritt, die zu diesem Zeitpunkt die effizienteste ist.

10 Wachstum von Funktionen

10.1 Definition

Seien f und g Funktion von $\mathbb{Z}$ oder $(\mathbb{R})$. Dann sagt man "$f(x)$ ist $\mathcal{O}(g(x))$", falls es Konstanten C und k gibt, so dass gilt:
$|f(x)| \leq C|g(x)|, \forall x > k$ Lies: "f(x) ist gross-O von g(x), man schreibt: $f(x) \in \mathcal{O}(g(x))$.

- Meist ist f eine komplizierte Funktion, wie z.B. $f(x) = (x^2 + 1)lnx + (2^x + x^4)$
- Man möchte für g eine möglichst einfache, nicht zu schnell wachsende Funktion, wie z.B. x, x^2 ...
- Ziel ist es herauszufinden, wie sich f(x) für sehr, sehr grosse x verhält, und zwar verglichen mit der einfacheren Funktion g.
- k ist der kleinste Wert von x, für den die obige Ungleichung noch gilt!

Also wir wollen für sehr grosse x, eine einfachere Funktion zu finden.

10.2 Example

Für $f(x) = x^2 + 2x + 1$ ist $\mathcal{O}(x^2)$.
Das heisst bei sehr grossen x entspricht die Funktion $f(x) = x^2$

Example

Zeige: $f(x) = x^2 + 2x + 1$ ist $\mathcal{O}(x^2)$.

Lösung: Wir betrachten **nur** reelle Zahlen x mit $x > 1$. Für diese Zahlen gilt auch $x^2 > x$ und $x^2 > 1$ und weiterhin (da f in diesem Bereich nur positive Werte annehmen kann):

$$|f(x)| = |x^2 + 2x + 1| = x^2 + 2\underbrace{x}_{<x^2} + \underbrace{1}_{<x^2} \leq x^2 + 2x^2 + x^2 = 4x^2$$

Insgesamt haben wir also gezeigt: Für alle $x > \underbrace{1}_{=k}$ gilt

$$\underbrace{|x^2 + 2x + 1|}_{=|f(x)|} \leq \underbrace{4}_{=C} \underbrace{|x^2|}_{=|g(x)|}$$

also $f(x) = x^2 + 2x + 1$ ist $\mathcal{O}(x^2)$ mit den Zeugen $k = 1$ und $C = 4$.

Example

Zeige: $f(x) = 7x^2$ ist $\mathcal{O}(x^3)$.

Lösung: Falls $x > 7$ ist, so gilt sicher auch

$$x^3 = x \cdot x \cdot x > 7 \cdot x \cdot x = 7x^2$$

also

$$|7x^2| = 7x^2 \leqslant 1 \cdot x^3$$

$|f(x)| = 7x^2 \leqslant 7x^3$ für $x \geqslant 1$

$C = 7$, $k = 1$

Insgesamt haben wir also gezeigt: Für alle $x > \underbrace{7}_{=k}$ gilt

$$\underbrace{|7x^2|}_{=|f(x)|} \leqslant \underbrace{1}_{=C} \underbrace{|x^3|}_{=|g(x)|}$$

In der Tat: f ist $\mathcal{O}(x^2)$

also $f(x) = 7x^2$ ist $\mathcal{O}(x^3)$ mit den Zeugen $k = 7$ und $C = 1$.

10.3 Polynome

Für das Polynom $\sum_{k=0}^{n} a_k x^k$ gilt $f(x)$ ist $\mathcal{O}(x^n)$. Das heisst die höchste Potenz von x gibt den Ton an.

Beispiel:
Es gilt immer: $|a + b| \leq |a| + |b|$

$f(x) = 5x^6 - 3x^2 + x - 10$
$|f(x)| \leqslant 5x^6 + 3x^2 + x + 10$
$|f(x)| \leqslant 5x^6 + 3x^6 + x^6 + 10x^6$
$|f(x)| \leqslant 5x^6 + 3x^6 + x^6 + 10x^6$ für $x \geqslant 1$
$|f(x)| = 19x^6$

also f ist $\mathcal{O}(x^6)$ mit Zeugen $k = 1$ und $C = 19$

11 Zahlen und Division

11.1 Definition

Falls a, $b \in \mathbb{Z}$ mit $a \neq 0$ dann sagt man: *a teilt b*, falls $\exists c(b = ac)$ in der Universalmenge $\mathbb{Z}$. Dann ist a ein *Faktor* von b und b ein *Vielfaches* von a. Man schreibt dann $a \mid b$ und anderenfalls $a \nmid b$

Theorem:
Falls a, b, c $\in \mathbb{Z}$
(a) $a \mid b \wedge a \mid c \rightarrow a \mid (b + c)$, $\rightarrow 6 \mid 12 \wedge 6 \mid 24 \rightarrow 6 \mid (12 + 24)$
(b) $a \mid b \rightarrow \forall c(a \mid bc)$,
(c) $a \mid b \wedge b \mid c \rightarrow a \mid c$,

11.2 ggt kgV

Der ggT von a und b beschreibt das grösste d für welches gilt $d \mid a$ und $d \mid b$.
Zwei zahlen sind teilerfremd (relaitv prim) falls ggT(a,b) = 1, dann schreibt man $a \perp b$.

Das kgV zweier Zahlen a und b ist die kleinste positive Zahl, welche durch a und b teilbar ist. Es gilt:

ab = ggT(a,b) $\cdot$ kgV(a,b)

Für ggT finden:

1. a und b jeweils in Primfaktoren zerlegen
2. alle gemeinsamen Primfaktoren multiplizieren

Eigenschaften:

- $ggT(a, 0) = |a|$
- $\forall a, b \in \mathbb{Z}(ggT(a, b) = ggT(\pm a, \pm b))$
- ggT(a, b) = ggT(a + b $\cdot$ k, b), k $\in \mathbb{Z}$
- ggT(a, b) = ggT(b, R_b(a))

11.3 Modulare Arithmetik

Sei $m \in \mathbb{N}\backslash\{0\}$, dann nennt man zwei ganze Zahlen a und b kongruent modulo m, falls $m \mid (a - b)$. Das heisst a und b liegen ein Vielfaches von m auseinander. Man schreibt dann $a \equiv b \bmod m$ und sagt: “a ist kongruent zu b modulo m”.

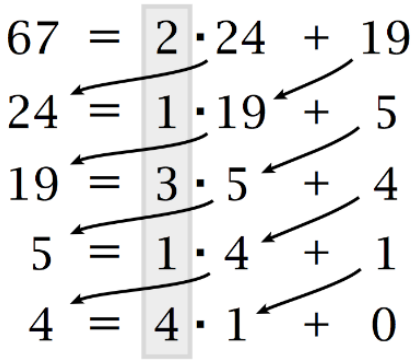
$13 \equiv 1 \bmod 4$ denn $4 \mid (13-1)$
$13 \equiv 1 \bmod 3$ denn $3 \mid (13-1)$
$13 \not\equiv 1 \bmod 5$ denn $5 \nmid (13-1)$

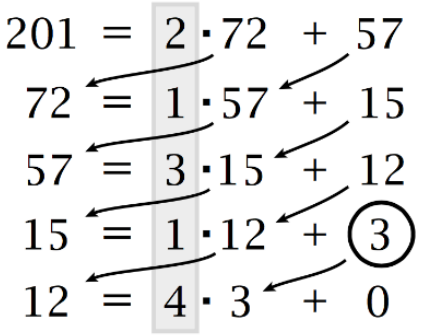
Die Schreibweise bedeutet $13-1$ (12) ist ein Vielfaches von 4.

11.4 Der Euklidische Algorithmus

Effiziente Methode um ggT zu finden.

Berechne $\mathrm{ggT}(67, 24)$ und $\mathrm{ggT}(201, 72)$.





ggT ist jeweils 1 und 3.

11.5 Erweiterter Euklidische Algorithmus

Lösung der Gleichung mit der diophantischen Gleichung.

Finde x,$y \in \mathbb{Z}$ mit $211 \cdot x + 13 \cdot y = 1$

Example

Finde $x, y \in \mathbb{Z}$ mit $211 \cdot x + 13 \cdot y = 1$.

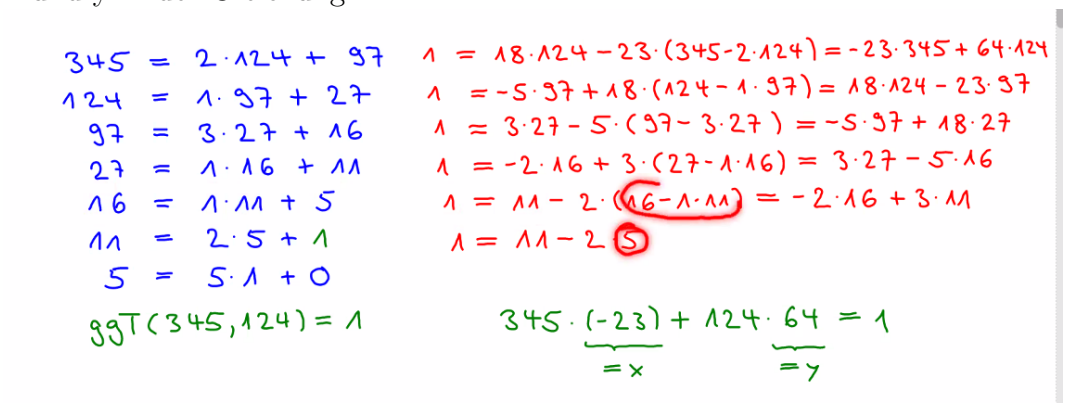
- Führe den (normalen) Euklidischen Algorithmus mit Zahlen $n_1 = 211$ und $n_2 = 13$ durch:

$$211 = 16 \cdot 13 + \mathbf{3} \quad \Longleftrightarrow \quad 3 = 211 - 16 \cdot 13$$
$$13 = 4 \cdot 3 + 1 \quad \Longleftrightarrow \quad 1 = 13 - 4 \cdot 3$$

- Löse die letzte Gleichung nach 1 auf und Nutze die restlichen Gleichungen in umgekehrter Reihenfolge, um *störende Terme* zu eliminieren.

$$\begin{aligned} 1 &= 1 \cdot 13 - 4 \cdot \mathbf{3} && \text{letzte Gleichung} \\ &= 1 \cdot 13 - 4 \cdot (211 - 16 \cdot 13) && \text{letzte mit vorletzter Gleichung} \\ &= 1 \cdot 13 - 4 \cdot 211 + 64 \cdot 13 \\ &= \underbrace{-4}_{x} \cdot 211 + \underbrace{65}_{y} \cdot 13 \end{aligned}$$

Mit einem nächsten Beispiel: zuerst (blau) der normale euklidische Algorithmus machen und danach der erweiterte machen (rot) von unten nach oben. Dann hat man am Schluss x und y in der Gleichung.



12 Matrizen

12.1 Definition

Eine m × n-Matrix ist eine rechteckige Anordnung von Zahlen in m Zeilen und n Spalten.

$$\mathbf{A} = \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{bmatrix}$$

Kurzschreibform: $\mathbf{A} = [a_{i,j}]$

12.2 Addition von Matrizen

Addition von Matrizen erfolgt jeweils durch die Addition der einzelnen Positionen

12.3 Multiplikation mit einer Zahl

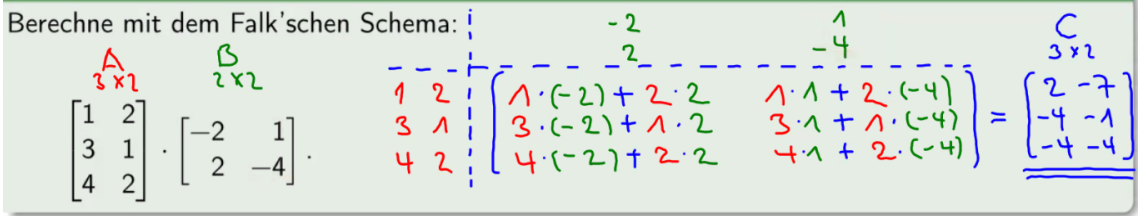
Einfach jede Zahl multiplizieren.

12.4 Matrixmultiplikation

$\mathbf{C} = \mathbf{AB}$, wobei die Anzahl Spalten in $\mathbf{A}$ gleich der Anzahl Reihen in $\mathbf{B}$ sein muss

Example (Falk'sches Schema)

Berechne mit dem Falk'schen Schema:



12.5 Transporierte Matrix

Eine transponierte Matrix ist eine, bei der die Spalten und Reihen vertauscht wurden.

Example (Transponierte Matrix)

Wie lauten die Transponierten der folgenden Matrizen:

$$\underset{2\times2}{\mathbf{A}} = \begin{bmatrix} 1 & 2 \\ 3 & 1 \end{bmatrix} \text{ und } \underset{2\times3}{\mathbf{B}} = \begin{bmatrix} -2 & 1 & 3 \\ 2 & -4 & -2 \end{bmatrix}.$$

$$\underset{2\times2}{A^T} = \begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix} \qquad \underset{3\times2}{B^T} = \begin{bmatrix} -2 & 2 \\ 1 & -4 \\ 3 & -2 \end{bmatrix}$$

12.6 Matrizen Eigenschaften

Keywords: symmetrisch, antisymmetrisch, Einheitsmatrix, k-te Potenz

Rechnen mit Matrizen — Eigenschaften

- Eine Matrix $\mathbf{A}$ heisst **symmetrisch**, falls $\mathbf{A}^\mathsf{T} = \mathbf{A}$.
- Eine Matrix $\mathbf{A}$ heisst **antisymmetrisch**, falls $\mathbf{A}^\mathsf{T} = -\mathbf{A}$.
- Eine symmetrische oder antisymmetrische Matrix ist quadratisch!
- Die n-dimensionale **Einheitsmatrix** $\mathbf{I}_n$ ist eine Matrix bei der alle Elemente auf der Diagonalen Eins und alle anderen Null sind.
- Ist $\mathbf{A}$ eine $(n \times n)$-Matrix, dann kann man deren **k-te Potenz** rekursiv definieren durch: $\mathbf{A}^0 = \mathbf{I}_n$ und $\mathbf{A}^n = \mathbf{A}\,\mathbf{A}^{n-1}$, $n = 1, 2, \ldots$.
- Matrizen werden in **MatLab** (steht für **Mat**rix **Lab**oratory) zur Darstellung von Bildern verwendet: dabei entspricht das (i, j)-Matrixelement dem Grauwert des entsprechenden Pixels (i, j). Der Nullpunkt befindet sich oben links, die erste Koordinate zeigt nach unten, die zweite nach rechts!

TODO: (SW03) Inverse Matrix und Matrizen Eigenschaften allgemein & Rechenregeln mit Matrizen.

12.7 Null-Eins Matrizen

Auch boolesche Matrizen genannt.

Boolesches Matrizen Produkt wird folgendermassen geschrieben: $\mathbf{A} \odot \mathbf{B}$.

Example (Boolsches Produkt (die Lösung))

$$\mathbf{A} \odot \mathbf{B} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{bmatrix} \odot \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} (1 \wedge 1) \vee (0 \wedge 0) & (1 \wedge 1) \vee (0 \wedge 1) & (1 \wedge 0) \vee (0 \wedge 1) \\ (0 \wedge 1) \vee (1 \wedge 0) & (0 \wedge 1) \vee (1 \wedge 1) & (0 \wedge 0) \vee (1 \wedge 1) \\ (1 \wedge 1) \vee (0 \wedge 0) & (1 \wedge 1) \vee (0 \wedge 1) & (1 \wedge 0) \vee (0 \wedge 1) \end{bmatrix}$$

$$= \begin{bmatrix} 1 \vee 0 & 1 \vee 0 & 0 \vee 0 \\ 0 \vee 0 & 0 \vee 1 & 0 \vee 1 \\ 1 \vee 0 & 1 \vee 0 & 0 \vee 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

Beachten Sie, dass hier die Klammern gesetzt werden müssen, da ja UND- und ODER-Verknüpfung die selbe Priorität haben, aber hier zuerst die UND-Verknüpfung ausgeweret werden muss!

Eine quadratische Matrix kann auch eine Potenz haben:
$\mathbf{A}^{[r]} = \mathbf{A} \odot \mathbf{A} \cdots \odot \mathbf{A}$:

$$\mathbf{A} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix} \qquad \mathbf{A}^2 = \mathbf{A} \odot \mathbf{A} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix} \odot \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix}$$

13 Mathematisches Begründen

Bekannte Beweismethoden:

- **Direkter Beweis:** Man zeigt, dass $p \to q$ wahr ist.
- **Beweis durch Kontraposition:** Man verwendet, dass $p \to q$ äquivalent ist zur Kontraposition $\neg q \to \neg q$.
- **Beweis durch Widerspruch:** Wir möchten zeigen, dass p wahr ist indem...

13.1 Mathematische Induktion

1. **Induktionsverankerung:** Für die kleinste Zahl zeigen, dass die Formel wahr ist (1 bei $n \in \mathbb{N}$).
2. **Induktionsschritt:** Es wird gezeigt, dass die Implikation $P(k) \to P(k+1)$ wahr ist $\forall k \geq 1$.

Beispiel: Dominosteine $\to$ falls der erste fällt, muss der 2. auch fallen. Falls der 2. fällt muss der 3. auch fallen.

Hinweis: Immer zuerst überlegen was am Schluss herauskommen sollte, falls der Beweis mit Induktion bewiesen werden kann, dann fällt auch das Beweisen leichter.

13.2 Rekursiv definierte Funktionen

Wenn eine Funktion mit Definitionsbereich $D(f) = \mathbb{N}$ für die f(0) definiert ist und bei welcher f(k) durch f(k-1), f(k-2) ... f(1), f(0) berechnet wird. **Beispiel:** Fibonacci Folge.

Diese kann man auch mit Induktion beweisen.

13.3 Beispiel Türme von Hanoi

Vermutung: $f(n) = 2^n - 1$
Das heisst $f(n+1) = 2^{n+1} - 1$

$f(1) = 2 - 1 = 1$: stimmt
Es braucht 2^n Züge um einen Turm zu bewegen.
Dann brauch es +1 um die unterste Scheibe (n+1 Scheibe) zu verschieben.
Und schlussendlich noch einmal $2^n + 1$
Das ergibt: $2 * (2^n - 1) + 1 = 2^{n+1} - 2 + 1 = 2^{n+1} - 1$
Vermutung stimmt.

14 Grundlagen des Zählens

14.1 Zusammenfassung

Bei Permutationen spielt die Reihenfolge eine Rolle; bei Kombinationen dagegen spielt die Reihenfolge keine Rolle!

Art	Wiederholung erlaubt	Anzahl	Reihenfolge relevant
r-Permutationen von n Elementen	Nein	$\frac{n!}{(n-r)!}$	ja
r-Kombinationen von n Elementen	Nein	$\frac{n!}{r!(n-r)!} = \binom{n}{r} = \binom{n}{n-r}$	nein
r-Permutationen von n Objekten	Ja	n^r	ja
r-Kombinationen von n Objekten	Ja	$\frac{(n+r-1)!}{r!(n-1)!} = \binom{n+r-1}{r}$	nein

14.2 Schubfachprinzip

Es gibt wenigstens ein Fach in das mehr als 2 Objekte reingehen.

Beispiel: In jeder Menge von 5 Zahlen gibt es 2, welche bei einer Division durch 4 den gleichen Rest geben.
Bei einer Divison durch 4 gibt es Reste von 0, 1, 2 oder 3. Man hat 5 Zahlen, heisst 2 Zahlen müssen sich denselben Rest teilen.

14.3 Permutationen

Eine Permutation von n verschiedenen Elementen ist eine geordnete Anordnung dieser n Elemente.
Das heisst die Anordnung (3,1,2) der Menge S=1,2,3 ist eine Permutation von S.
3-Permutationen ((1,2,3), (1,3,2), (2,1,3), (2,3,1), (3,1,2), (3,2,1)): 3!
2-Permutationen ((1,2), (1,3), (2,1), (2,3), (3,1), (3,2)): $2 \cdot 3$

Allgemeine Formel für Anzahl r-Permutationen einer Menge von n Elementen:

$$P(n,r) = \frac{n!}{(n-r)!}, \quad 0 \leq r \leq n \in \mathbb{N}$$

n = die Anzahl Elemente
r = die Anzahl Elemente im Tuple

Die Reihenfolge **spielt** eine Rolle.

14.4 Permutation nicht unterscheidbarer Objekte

Die Anzahl verschiedener Permutationen von n Objekten, von denen n_1 Objekte der Art 1, n_2 Objekte der Art 2, ..., n_k Objekte der Art k sind, ist gegeben durch:

$$\frac{n!}{n_1!n_2!\dots n_k!}, \text{ wobei } n = \sum_{i=1}^{k} n_i$$

Beispiel:
wie viele Wörter kann man aus den Zeichen von SUCCESS machen?
$n = SUCCESS = 7$
$n_1 = S = 3$
$n_2 = U = 1$
$n_3 = C = 1$
$n_4 = E = 2$

Ergibt: $\frac{7!}{3!2!1!1!} = \frac{7!}{3 \cdot 2 \cdot 2} = 420$

14.5 Kombinationen

Für $S = \{1, 2, 3, 4\}$ ist {1, 3, 4} eine 3-Kombination von S. Beachte, dass {3, 1, 4} die selbe 3-Kombination von S ist.

Die Reihenfolge spielt **keine** Rolle.

Die Anzahl von r-Kombinationen einer Menge von $n \geq 0$ Elementen isst gegeben durch:

$$C(n, r) = \frac{n!}{r!(n-r)!} = \binom{n}{r} = C(n, n-r)$$

n = die Anzahl Elemente
r = die Anzahl Elemente im Set

14.6 Kombinationen mit Wiederholungen

Beispiel: Wie viele verschiedene Früchteschalen kann man mit Äpfeln, Orangen und Birnen machen, wenn immer 4 Früchte verwendet werden?
AAAA, AAAO, AAAB, AAOO, AAOB ...

$$C(n + r - 1, r) = \binom{n + r - 1}{r}$$

15 Diskrete Wahrscheinlichkeitsrechnung

Wahrscheinlichkeiten werden oft mit $p(A)$ angegeben. Wobei p die Wahrscheinlichkeit allgemein beschreibt und A der Output. Heisst $p(A)$ ist die Wahrscheinlichkeit mit der das Ereignis A eintrifft.

15.1 Bedingte Wahrscheinlichkeit

Definition: Die Wahrscheinlichkeit, dass ein Ereignis A eintritt, wenn ein Ereignis B eingetreten ist, ist gegeben durch
$p(A|B) = \frac{p(A \cap B)}{p(B)}$ (siehe Beispiel mit Münze in SW06).

15.2 Verteilungsfunktionen

Zusammenfassung der (diskreten) Verteilung

Die **Wahrscheinlichkeitsfunktion** $f(x)$ der hypergeometrischen Verteilung kann im Grenzfall grosser N und M und kleinem n durch die Binomialverteilung mit $p = M/N$ approximiert werden. Diese kann für kleine p und grosse n durch die Poissonverteilung mit $\mu = np$ approximiert werden.

Verteilung	Parameter	f(k)	Bedingung für Approximation
hypergeometrisch	N, M, n	$\frac{\binom{M}{k}\binom{N-M}{n-k}}{\binom{N}{n}}$	
Binomial	n, $p = M/N$	$\binom{n}{k} p^k (1-p)^{n-k}$	wobei $p = M/N$ $n \leqslant M/10$, $n \leqslant (N-M)/10$
Poisson	$\mu = np$	$\frac{\mu^k}{k!} e^{-\mu}$	wobei $\mu = np$ $p \leqslant 0.1$, $n \geqslant 100$

15.2.1 Bernoulli-Verteilung

Zufallsexperiment mit nur 2 möglichen Ergebnissen, wobei die Bernoulli-Verteilung der Wahrscheinlichkeitsverteilung entspricht. Wobei wahr p entspricht und falsch 1-p. Die Wahrscheinlichkeiten müssen dabei voneinander unabhänig sein.

Beispiel: Bitstring mit 3 Bits bei der n-Einsen vorkommen (und wenn man eine 1 Würfelt ist es ein Erfolg resp. p oder ein nicht-Erfolg resp. $1 - p$ oder q).

P(k=0) = P($\{000\}$) = $1p^0 \cdot (1-p)^3$
P(k=1) = P($\{001\}$,$\{010\}$,$\{010\}$) = $3p^1 \cdot (1-p)^2$
P(k=2) = P($\{011\}$,$\{110\}$,$\{101\}$) = $3p^2 \cdot (1-p)^1$
P(k=3) = P($\{111\}$) = $1p^3 \cdot (1-p)^0$

Definition durch Binomialverteilung:
$B(k|n,p) = B_{n,p}(k) = C(n,k)p^k(1-p)^{n-k} = \binom{n}{k}p^k(1-p)^{n-k}$
B: Bernoulli
k: Anzahl Erfolge
n: Anzahl Versuche
p: Wahrscheinlichkeit für Erfolg

Mit dieser Formel kann man die Wahrscheinlichkeit ausrechnen für k-Erfolge.

Beispiel für eine Ungleichverteilung:
Eine 0 wird zu 90% und eine 1 zu 10% gewürfelt. Wie wahrscheinlich ist es 8 Nullen bei 10 Würfen zu erzielen.

$B(8|10,0.9) = \binom{10}{8} \cdot 0.9^8 \cdot 0.1^2 = 19.37\%$

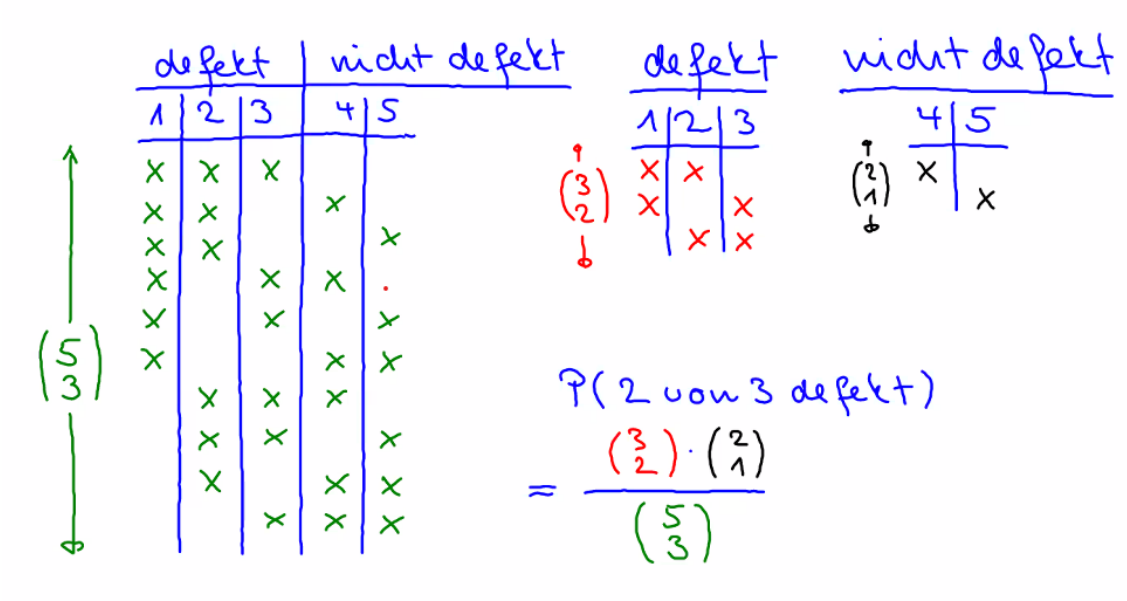
15.2.2 Hypergeometrische Verteilung

Binomialverteilung liegt vor, wenn bei einer Stichprobe die Objekte wieder zurückgelegt werden. Werden die Objekte nicht wieder zurückgelegt handelt es sich um die Hypergeometrische Verteilung.

Beispiel:
Wenn man insgesamt N Objekte hat und M davon sind defekt. Wie gross ist die Wahrscheinlichkeit, dass von n gezogenen Objekten k Objekte defekt sind?

$$p(k) = \frac{\binom{M}{k}\binom{N-M}{n-k}}{\binom{N}{n}}$$

Anschauliches Beispiel:



Grün: Anzahl der Objekte
Rot: Anzahl der Objekte die defekt sind
Schwarz: Anzahl der Objekte die nicht defekt sind

15.2.3 Poisson-Verteilung

Wenn bei einer Binomialverteilung sehr viele Versuche durchgeführt werden und die Wahrscheinlichkeit sehr klein ist, ist die Annäherung durch die Poisson-Verteilung viel einfacher.
$p \to 0$ und $n \to \infty$ dann $\mu = np$:

$$p(k) = \frac{\mu^k e^{-\mu}}{k!}$$

15.3 Zufallsvariablen

Wahrscheinlichkeitsverteilung einer Zufallsvariable X ist die Verteilungsfunktion $F_X(x)$,

16 Fortgeschrittene Zählmethoden

16.1 Rekursionsbeziehungen

Rekursionsbeziehungen liegen immer vor, wenn ein Wert a_n von einem anderen Wert a_{n-1} abhängt.
Beispiel für Rekursionsbeziehungen:

Wie viele Bitstrings der Länge n gibt es, die keine zwei aufeinanderfolgende Nullen enthalten?

$a_n = a_{n-1} + a_{n-2}$

Ein Bitstring endet mit einer 1 oder 0. Im ersten Fall kann irgendein Wert davor stehen, davon gibt es a_{n-1} Möglichkeiten. Im zweiten Fall muss ein 1 vor der 0 stehen, davon gibt es a_{n-2} Möglichkeiten.

Beispiel Computersystem Passwort:
Ein Passwort ist korrekt, wenn es eine gerade Anzahl von Nullen hat.

a_{n-1} Möglichkeiten bei einer Zahl, welche mit 1-9 endet.
Wenn eine Null steht, dann noch $10^{n-1} - a_{n-1}$ Möglichkeiten.

$a_n = 9 \cdot a_{n-1} + 10^{n-1} - a_{n-1}$
$a_n = 8 \cdot a_{n-1} + 10^{n-1}$

- Sie ist homogen, falls $r(n) = 0$
- Sie ist linear, falls die Variablen von F a_n, a_{n-1}, a_{n-2} sind. (meistens ist F von der Form $a_n - c_1 a_{n-1} - c_2 a_{n-2} - \cdots - c_k a_{n-k} = 0$)
- Sie ist von k-tem Grade, falls F höchstens von Gliedern ab a_{n-k} abhängt.

16.2 Lösen von Rekursionsbeziehungen

Eigenschaften von Rekursionsbeziehungen:
$F(a_n, a_{n-1} \dots a_2, a_1) = r(n)$

Allgemeines Lösen einer linearen RB in drei Schritten:

1. Bestimme die allgemeine Lösung $\left\{a_n^{(h)}\right\}$ der zugehörigen, homogenen Rekursionsbeziehung (RHS gleich null setzen).

2. Bestimme eine (einzige) partikuläre Lösung $\left\{a_n^{(p)}\right\}$ der zugehörigen, inhomogenen Rekursionsbeziehung

3. Dann ist die allgemeine Lösung der inhomogenen RB die Summe der beiden Lösungen:
$$\{a_n\} = \left\{a_n^{(h)}\right\} + \left\{a_n^{(p)}\right\}$$

1. Schritt:
Die homogene RB
$(a_n - c_1 a_{n-1} - c_2 a_{n-2} - \dots - c_k a_{n-k} = 0)$
wird durch den folgenden Ansatz gelöst:
$a_k = r^k$, $k = n - k, n - k + 1, \dots, n$.

Beispiel:
Setzt man in die lineare, homogene Rekursionsbeziehung $a_n - a_{n-1} - a_{n-2} = 0$ den Ansatz $a_n = r^n$ ein, erhält man

$r^n - r^{n-1} - r^{n-2} = 0$
$r^{n-2}(r^2 - r - 1) = 0$
$r^2 - r - 1 = 0$

$$r_1 = \frac{1}{2}\left(1 + \sqrt{5}\right) \qquad r_2 = \frac{1}{2}\left(1 - \sqrt{5}\right)$$

Bei Auflösung der quadratischen Gleichung:
Wenn $D > 0$, dann $a_n^{(h)} = \alpha_1 r_1^n + \alpha_2 r_2^n$ wobei die Alphas beliebige Konstanten sind.

Wenn $D = 0$, dann $a_n^{(h)} = (\alpha_1 + \alpha_2 n) r^n$

17 Zahlentheorie

17.1 Lösung Diophantischer Gleichungen

$n_1 \cdot x + n_2 \cdot y = n$
Hat immer dann ganzzahligen Lösungen, wenn ggT(n_1, n_2) — n ist. Das heisst, falls ggT(n_1, n_2) ein Teiler von n ist.

Sind n_1 und n_2 teilerfremd, dann hat die Gleichung immer eine Lösung.

17.2 Modulare Inverse

x mal was gibt 1: $3^{-1} \cdot \frac{1}{3} = 1$

$ggT(345, 124) = 1$

$345 \cdot \underbrace{(-23)}_{=x} + 124 \cdot \underbrace{64}_{=y} = 1$

$345 \cdot (-23) = 1 - 124 \cdot 64$

$\equiv 1 \pmod{124}$

$97 \cdot 101 \equiv 1 \pmod{124}$

Also: $97^{-1} \equiv 101 \pmod{124}$

$101^{-1} \equiv 97 \pmod{124}$

$124 \cdot 64 = 1 - 345 \cdot (-23)$

$\equiv 1 \pmod{345}$

Das heisst, dass wo immer eine 1 in der Grafik ist, existiert ein modulo inverse. Ist die Modulo Zahl eine Primzahl existiert immer ein modulo inverse, andererseits nicht unbedingt.

Grundsätzlich mit erweitertem euklidischem Algorithmus lösen.

Beispiel: Finden Sie ein modulares Inverses von 963 modulo 218.

$ggT(345,124) = 1$

$345 \cdot \underbrace{(-23)}_{=x} + 124 \cdot \underbrace{64}_{=y} = 1$

$345 \cdot (-23) = 1 - 124 \cdot 64$

$\equiv 1 \pmod{124}$

$97 \cdot 101 \equiv 1 \pmod{124}$

also: $97^{-1} \equiv 101 \pmod{124}$

$101^{-1} \equiv 97 \pmod{124}$

$124 \cdot 64 = 1 - 345 \cdot (-23)$

$\equiv 1 \pmod{345}$

17.3 Der chinesische Restsatz

Seien $m_1, m_2, \ldots, m_k$ paarweise teilerfremde Zahlen. Dann hat das System k simultane Kongruenzen

$$\begin{aligned} x &\equiv r_1 \mod m_1 \\ x &\equiv r_2 \mod m_2 \\ &\vdots \\ x &\equiv r_k \mod m_k \end{aligned}$$

Konstruktionskonzept:
$m = m_1 \cdot m_2 \cdots m_k$

1. Dann definieren wir für alle $i = 1, 2, \ldots, k$:

   $$M_i = \frac{m}{m_i}$$

   Sicher gilt dann ggT(m_i, M_i) = 1. Denn die Voraussetzung ist, dass alle m_i teilerfremd sind.

2. Für $i = 1, 2, \ldots k$ hat M_i ein modulares Inverses (erweiterter euklidischer Algorithmus) y_i modulo m_i, d.h.

$M_i \cdot y_i \equiv 1 \pmod{m_i}$

3. Die simultane Lösung der Kongruenzen ist dann:

$$x = \sum_{i=0}^{k} r_i \cdot M_i \cdot y_i$$

17.4 Eulersche ϕ-Funktion

In der Zahlentheorie und Kryptologie sind folgende Mengen wichtig:
$\mathbb{Z}_n := \{0, 1, 2, 3, \ldots, n-1\}$, wobei $|\mathbb{Z}_n| = n$, das heisst: $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ und $|\mathbb{Z}_4| = 4$
$\mathbb{Z}_n^* := \{x \in \mathbb{Z}_n | x > 0 \text{ und } ggT(x, n) = 1\}$ mit $|\mathbb{Z}_n^*| :=$ Anzahl Elemente in $\mathbb{Z}_n^*$

Die Eulersche ϕ-Funktion ist definiert als:

$\phi : \mathbb{N} \to \mathbb{N}, n \mapsto |\mathbb{Z}_n^*| =: \phi(n)$

Sie ordnet jeder natürlichen Zahl n die Anzahl der zu ihr teilerfremden natürlichen Zahlen zu, die kleiner als n sind.

17.5 Eigenschaften der Eulerschen ϕ-Funktion

Seien p und q zwei verschiedene Primzahlen, $m = p_1^{r_1} \cdot p_2^{r_2} \cdots p_n^{r_n}$, die Primfaktorzerlegung $m \in \mathbb{N}$ und weiter $n \in \mathbb{N}$ teilerfremd zu m, dann gilt:

$$\begin{aligned}
\phi(p) &= p - 1 \\
\phi(p \cdot q) &= (p-1) \cdot (q-1) \\
\phi(m) &= (p_1 - 1) \cdot p_1^{r1-1} \cdot (p_2 - 1) \cdot p_2^{r_2-1} \cdots (p_n - 1) \cdot p_n^{r_n-1} \\
\phi(m \cdot n) &= \phi(m) \cdot \phi(n)
\end{aligned}$$

Example

Ein Beispiel zum letzten Teil des Satzes. Bekanntlich sind $m = 150 = 2 \cdot 3 \cdot 5^2$ und $n = 77 = 7 \cdot 11$ teilerfremd, d.h. $ggT(150, 77) = 1$. Dann gilt

$$\begin{aligned}
\phi(11550) &= \phi(150 \cdot 77) = \phi(150) \cdot \phi(77) \\
&= (2-1) \cdot 2^0 \cdot (3-1)3^0 \cdot (5-1) \cdot 5^1 \cdot (7-1) \cdot (11-1) = 1 \cdot 2 \cdot 4 \cdot 5 \cdot 6 \cdot 10 = 2400.
\end{aligned}$$

$\phi(150) = \phi(2 \cdot 3 \cdot 5^2) = (2-1)2^0(3-1)3^0(5-1)5^1$

17.6 Der kleine Satz von Fermat

Sei p eine Primzahl und m eine nicht negative Zahl, dann gilt:

$m^p \mod p = m \mod p$

17.7 Der Satz von Wilson

Eine natürliche Zahl $n > 1$ ist genau dann eine Primzahl, wenn
$(n-1)! + 1 = (n-1)(n-2) \cdots 2 \cdot 1 + 1$ durch n teilbar ist.

17.8 Relationen

Eine Relation R auf einer Menge A ist eine Teilmenge von $A \times A$.

$\{1,2,3\}^2 =$

$$\{(1,1),(1,2),(1,3)$$
$$(2,1),(2,2),(2,3)$$
$$(3,1),(3,2),(3,3)\}$$

R ist zum Beispiel $= \{(1,2),(1,3),(2,3)\}$

Wenn A die Menge aller Landpunkte auf einem Planet ist, dann ist
$R = \{(x,y) \in A \times A | y$ lässt sich von x aus trockenen Fusses erreichen$\}$
$R = \{(x,y) \in \mathbb{Z} \times \mathbb{Z} | y \equiv x \mod n\}$

17.8.1 Symmetrische Relationen

Eine symmetrische Relation ist, wenn man in der obigen Definitionsformel x und y vertauschen kann.

$\forall x, y \in A((x,y) \in R \longrightarrow (y,x) \in R)$.

Auf dem Planet, lässt sich von jedem Punkt zu einem Anderen auf der Landmasse der Weg umkehren (rückwärts gehen).

17.8.2 Transitive Relationen

Wenn für jedes Element folgendes gilt: Wenn sich von x aus y erreichen lässt und von y aus lässt sich z erreichen, dann lässt sich von z aus auch x erreichen (ist wahr auf dem Planet, mit der Landmasse), dann ist die Relation transitiv.

$x, y, z \in \mathbb{Z}$ mit $y \equiv x \mod n$ **und** $z \equiv y \mod n$ **und** $z \equiv x \mod n$

17.8.3 Äquivalenzrelationen

Definition: Falls die Relation auf der Menge A reflexiv, symmetrisch und transitiv ist, dann ist sie eine Äquivalenzrelation.

Die Restklassen sind immer die Zahlen, welche in Relation zueinander stehen (kongruent sind).

Alle ganzen Zahlen ergeben sich aus den Restklassen $\mathbb{Z} = [0] \cup [1] \cup \cdots \cup [n-1]$ dargestellt.

17.9 Modulares Rechnen

17.9.1 Modulare Rechenoperationen

Modulare Rechenoperationen

Definition

Sei $n \geqslant 2$. Wir führen auf der Menge $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ eine Addition $\oplus_n$ (Addition modulo n) und eine Multiplikation $\odot_n$ (Multiplikation modulo n) ein. Für $a, b \in \mathbb{Z}_n$ sei:

$$a \oplus_n b = a + b \bmod n = R_n(a+b)$$
$$a \odot_n b = a \cdot b \bmod n = R_n(a \cdot b)$$

Beim: $R_n(x)$ ist $x \% n$

Wir könnten auch noch weitere Operationen auf $\mathbb{Z}_n$ einführen, z.B.

$$a \ominus_n b = a - b \bmod n = R_n(a-b)$$

Example

$n = 6$ und $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$

$\mathbb{Z} = \underbrace{[0]}_{R_6=0} \cup \underbrace{[1]}_{R_6=1} \cup \underbrace{[2]}_{R_6=2} \cup \underbrace{[3]}_{R_6=3} \cup \underbrace{[4]}_{R_6=4} \cup \underbrace{[5]}_{R_6=5}$

$3 \oplus_6 4 = R_6(3+4) = 1$ problemlos

$3 \ominus_6 4 = R_6(3-4) = 5$ problemlos

$3 \odot_6 4 = R_6(3 \cdot 4) = 0$ problemlos aber ungewöhnlich

$3 \ominus_6 4 = R_6(3-4) = R_6(-1) = 5$

17.9.2 Modulare Rechenregeln

Rechenregeln beim modularen Rechnen

Theorem (Rechenregeln)

Sei $n \geqslant 2$ *und* $a, b, c \in \mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$. *Dann gilt*

$a \oplus_n b = b \oplus_n a$	*Kommutativgesetz bei der Addition*
$a \oplus_n 0 = a$	*Neutralelement der Addition*
$a \odot_n b = b \odot_n a$	*Kommutativgesetz bei der Multiplikation*
$a \odot_n 1 = a$	*Neutralelement der Multiplikation*
$a \odot_n (b \oplus_n c) = (a \odot_n b) \oplus_n (a \odot_n c)$	*Distributivgesetz*

Example

Berechnen Sie

$3 \odot_5 (2 \oplus_5 4) = 3 \odot_5 R_5(6) = 3 \odot_5 1 = R_5(3) = 3$

$3 \odot_7 (2 \oplus_7 4) = 3 \odot_7 R_7(6) = 3 \odot_7 6 = R_7(18) = 4$

$(3 \odot_5 2) \oplus_5 (3 \odot_5 4) = R_5(6) \oplus_5 R_5(12) = 1 \oplus_5 2 = R_5(3) = 3$

$(3 \odot_7 2) \oplus_7 (3 \odot_7 4) = R_7(6) \oplus_7 R_7(12) = 6 \oplus_7 5 = R_7(11) = 4$

Rechenregeln beim modularen Rechnen (Fort.)

Example ($\mathbb{Z}_5$ — Additions- und Multiplikationstabelle)

Ergänzen Sie alle fehlenden Einträge:

$\oplus_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\odot_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$\mathbb{Z}_5 = \{0,1,2,3,4\}$

$\mathbb{Z} = [0] \cup [1] \cup [2] \cup [3] \cup [4]$

$x \oplus_5 -x = 0$

$-0 = 0$
$-1 = 4$
$-2 = 3$
$-3 = 2$
$-4 = 1$

$x \odot_5 x^{-1} = 1$

0^{-1} = ex. nicht!
$1^{-1} = 1$
$2^{-1} = 3$
$3^{-1} = 2$
$4^{-1} = 4$

in $\mathbb{Q}$:
$2x + 4 = 1 \quad | + (-4)$
$2x = -3 \quad | \cdot 2^{-1}$
$x = -1.5$

in $\mathbb{Z}_3$:
$2x + 3 = 1 \quad | \oplus_5 2$
$2x = 3 \quad | \odot_5 3$
$x = 4$

17.10 Square-and-Multiply-Algorithmus

Effizientes potenzieren modulo n.

$21 = (10101)_2$

$$
\begin{aligned}
5^{21} \mod 11 &= 5^{(2\cdot 2+1)\cdot 2\cdot 2+1} && \mod 11 \\
&= (((5^2)^2 \cdot 5)^2)^2 \cdot 5 && \mod 11 \\
&= ((25^2 \cdot 5)^2)^2 \cdot 5 && \mod 11 \\
&= (((25)^2 \cdot 5)^2)^2 \cdot 5 && \mod 11 \\
&= ((3^2 \cdot 5)^2)^2 \cdot 5 && \mod 11 \\
&= (1^2)^2 \cdot 5 && \mod 11 \\
&= 5
\end{aligned}
$$

Formal:

- Q bedeutet quadrieren und M multiplizieren
- Ersetze in der binären Darstellung des Exponenten jede 1 durch QM und jede 0 durch Q $(10101)_2 \rightarrow QMQQMQQM$
- Streiche das erste (links vorkommende) QM
  $QMQQMQQM \rightarrow QQMQQM$
- Das Symbol QQMQQM gibt die Reihenfolge von Quadrieren und Multiplizieren an, um um die Potenz zu berechnen. Nach jeder Operation wird das Ergebnis modulo 11 reduziert.

Beispiel:
$5^{21} \mod 11$
$5 \xrightarrow{Q} 25 \equiv 3 \xrightarrow{Q} 9 \xrightarrow{M} \equiv 1 \xrightarrow{Q} 1 \xrightarrow{Q} 1 \xrightarrow{M} 5$

17.11 Symmetrische Verschlüsselung

Besteht immer aus folgenden Elementen:

- **Schlüssel** $k \in K$ (Schlüsselraum)
- **Klartext** $m \in M$ (Klartextraum)
- **Geheimtext** $c \in C$ (Geheimtextraum) welcher sich folgendermassen ergibt: $c = f(k, m)$

Dabei muss immer gelten, dass f eine Umkehrfunktion hat, mit welcher sich der Geheimtext entschlüsseln lässt.

$m = f^*(k, c) = f^*(k, f(k, m))$

Auch muss gelten, dass mit unterschiedlichen Schlüsseln niemals der gleiche Geheimtext entsteht.

17.12 Asymmetrische Verschlüsselung

RSA Algorithmus-Formel:

$$\begin{aligned} c &= m^e \mod n \\ m &= c^d \mod n \end{aligned}$$

Wobei gelten muss, dass $e \cdot d \equiv 1 \mod \phi(n)$ resp. e muss zu $\phi(n)$ teilerfremd sein.

18 Graphentheorie

Graphen bestehen aus Knoten und Kanten.
Wobei Konten Orte im Netz sind und Kanten Verbindungen zwischen Knoten.

Ein ungerichteter Graph G besteht aus einer Knotenmenge V und einer Kantenmenge E.

wobei jeder Kante $e \in E$ zwei (nicht notwendigerweise verschiedene) Knoten aus V zugeordnet sind.

Schreibweise: $e = \{u, v\} = \{v, u\}$
Die Knoten u und v heissen dann **Endknoten** von e.

Eine Schlinge ist eine Kante, welche einen Knoten mit sich selbst verbindet.

Ein Graph, der weder Schlingen noch parallele Kanten enthält, heisst **einfacher Graph**.

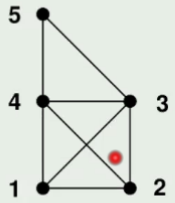
Beispiel:

Example

Die beiden Listen

$$V = \{1, 2, 3, 4, 5\}$$
$$E = \{\{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}, \{3, 5\}, \{4, 5\}\}$$
$$= \{e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8\}$$

entsprechen dem (gezeichneten) Graphen, wobei



$e_1 = \{1, 2\}$, $e_2 = \{1, 3\}$,
$e_3 = \{1, 4\}$, $e_4 = \{2, 3\}$,
$e_5 = \{2, 4\}$, $e_6 = \{3, 4\}$,
$e_7 = \{3, 5\}$, $e_8 = \{4, 5\}$.

Beachte: jede Kante ist eine Menge von (zwei) Knoten und alle Kanten vereint bilden die Menge der Kanten.

18.1 Knoten- oder Eckengrad

Der Grad eines Knotens ist die Anzahl der Kanten, die in diesem Knoten enden. Schlingen werden doppelt gezählt
Die **Gesamtsumme** aller Grade ist $2 \cdot |E|$

Spezialfälle:
$deg(v) = 0 \rightarrow v$ heiss **isolierte Ecke**
$deg(v) = 1 \rightarrow v$ heisst **Endecke**

Eine Gradliste $|V|$ ist eine Liste der Knotengrade eines Graphen.

Der **maximale Grad** eines Graphen wird mit $\Delta(G)$ bezeichnet.
Der **minimale Grad** eines Graphen wird mit $\delta(G)$ bezeichnet.

18.2 Isomorphe Graphen

Definition:
Zwei Graphen G_1 und G_2 heissen **isomorph**, wenn es eine Bijektion $f : V_1 \rightarrow V_2$ gibt, so dass für alle $u, v \in V_1$ gilt:
$\{u, v\} \in E \Longleftrightarrow \{f(u), f(v)\} \in E'$
Das heisst, dass für jede Kante und jeden Knoten in G_1 ein entsprechendes Äquivalent in G_2 existiert.

Isomorphe Graden haben also gleich viele Knoten und Kanten und deren Gradlisten sind identisch, die Umkehrung gilt jedoch nicht.