Induktion

- **Vollständige Induktion**

  Gelten die beiden Aussagen:

  - $p(0)$ und
  - $\forall n \in \mathbb{N} : p(n) \rightarrow p(n+1)$,

  dann gilt auch $\forall n \in \mathbb{N} : p(n)$.

- **Verallgemeinerte vollständige Induktion**

  Gelten die beiden Aussagen:

  $p(0)$ und

  $\forall n \in \mathbb{N} : p(0) \wedge p(1) \wedge \cdots \wedge p(n) \rightarrow p(n+1)$

  dann gilt die Aussage $\forall n \in \mathbb{N} : p(n)$.

Struktur von Induktionsbeweise

- **Vollständige Induktion**

  Induktionsbasis: Beweise $p(0)$

  Induktionsvoraussetzung: Für $a \in \mathbb{N}$ beliebig gewählt gilt $p(a)$

  Induktionsschluss: Folgere $p(a+1)$ aus der Induktionsvoraussetzung $p(a)$

- **Verallgemeinerte vollständige Induktion**

  Induktionsbasis: Beweise $p(0)$

  Induktionsvoraussetzung: Für $a \in \mathbb{N}$ beliebig gewählt gilt $p(0) \wedge \cdots \wedge p(a)$

  Induktionsschluss: Folgere $p(a+1)$ aus der Induktionsvoraussetzung $p(0) \wedge \cdots \wedge p(a)$

Induktion

- **Wohlfundierte Induktion**

  Sei $\succ$ eine wohlfundierte strikte Halbordnung auf X
  (i.e. $\succ$ transitiv, irreflexiv, wohlfundiert).

  Falls $\forall x \in X : (\forall y \in X : (x \succ y \to p(y)) \to p(x))$

  dann gilt $\forall x \in X : p(x)$

Induktionsbasis: Beweise $p(m)$ für m minimal in X

Induktionsvoraussetzung: Für $a \in X$ beliebig gewählt gilt
$p(b)$ für jedes $b \in X$ mit $a \succ b$

Induktionsschluss: Folgere $p(a)$ aus der Induktionsvoraussetzung

Induktion

- **Wohlfundierte Induktion**

  Sei $\succ$ eine wohlfundierte strikte Halbordnung auf X
  (i.e. $\succ$ transitiv, irreflexiv, wohlfundiert).

Falls	$\forall x \in X : (\forall y \in X : (x \succ y \rightarrow p(y)) \rightarrow p(x))$
dann gilt	$\forall x \in X : p(x)$

Induktionsvoraussetzung: Für $a \in X$ beliebig gewählt gilt
$p(b)$ für jedes $b \in X$ mit $a \succ b$

Induktionsschluss: Folgere $p(a)$ aus der Induktionsvoraussetzung

Induktive Definitionen

Induktive Definition von Folgen:

a_0

$a_n = f_n(a_0, \ldots, a_{n-1})$

Induktive Definitionen

Induktive Definition von Mengen:

Beispiel

(1) Menge Σ^* aller Wörter über ein Alphabet Σ

Basismenge:	Das leere Wort $\epsilon \in \Sigma^*$
Erzeugungsregel:	Wenn $w \in \Sigma^*$ und $a \in \Sigma$,
	dann gilt $wa \in \Sigma^*$

Induktive Definitionen

Induktive Definition von Mengen:

Beispiel

(2) Menge aller aussagenlogischer Formeln

Basismenge: $w, f, x_0, x_1, x_2, \dots$ sind aussagenlogische Formeln (atomare Formeln)

Erzeugungsregel: Wenn F_1, F_2 aussagenlogische Formeln sind, dann sind auch $\neg F_1$, $F_1 \wedge F_2$, $F_1 \vee F_2$, $F_1 \rightarrow F_2$, $F_1 \leftrightarrow F_2$ aussagenlogische Formeln

Form(X)

Strukturelle Induktion

Form(X) kleinste Menge, die

- w, f und X enthält
- zusammen mit F auch $\neg F$ enthält
- zusammen mit F_1, F_2 auch $F_1 \mathrm{op} F_2$ enthält ($\mathrm{op} \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$)

Gelten die beiden Aussagen:

- $p(B)$ für alle atomaren Formeln $B \in \{w, f\} \cup X$
- $\forall F \in \mathrm{Form}(X)$:

$$((F = \neg F_1 \ \wedge p(F_1)) \rightarrow p(F)) \quad \wedge$$
$$((F = F_1 \mathrm{op} F_2 \ \wedge \ p(F_1) \ \wedge \ p(F_2)) \rightarrow p(F))$$

dann gilt auch $\forall F \in \mathrm{Form}(X) : p(F)$.

Kombinatorische Beweise

- Abzählargumente

Wichtig in allen Gebieten der Mathematik und Informatik

- Komplexität von Algorithmen
- Wahrscheinlichkeit eines Ereignisses
- Sicherheit von Computercodes

Zählen

Grundlegende Zählprinzipien

Produktregel

Sei $k \in \mathbb{N}$, $k > 0$, und seien $A_1, \ldots, A_k$ endliche Mengen.

Dann gilt $|A_1 \times \cdots \times A_n| = \prod_{i=1}^{n} |A_i|$

Summenregel

Sei $k \in \mathbb{N}$, $k > 0$, und seien $A_1, \ldots, A_k$ paarweise disjunkte endliche Mengen. Dann gilt $|\bigcup_{i=1}^{k} A_i| = \sum_{i=1}^{n} |A_i|$

Zählen

Grundlegende Zählprinzipien

Abbildungsanzahl

Seien A und B endliche Mengen.

Dann gilt $|\{f \mid f : A \to B\}| = |B|^{|A|}$

Anzahl eineindeutiger Abbildungen

Sei A eine endliche Menge.

Dann gilt $|\{f \mid f : A \to A \text{ eineindeutig }\}| = |A|!$

Zählen

Grundlegende Zählprinzipien

Anzahl der Untermengen einer endlichen Menge

Sei A eine endliche Menge.

Dann gilt $|\{S \mid S \subseteq A\}| = |2|^{|A|}$

Zählen

Grundlegende Zählprinzipien

Inklusions-Exklusionsprinzip

Seien A_1, A_2 endliche Mengen.

Dann gilt: $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$

Seien A_1, A_2, A_3 endliche Mengen.

Dann gilt:
$$\begin{aligned} |A_1 \cup A_2 \cup A_3| = \quad & |A_1| + |A_2| + |A_3| \\ & -|A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| \\ & +|A_1 \cap A_2 \cap A_3| \end{aligned}$$

Zählen

Grundlegende Zählprinzipien

Inklusions-Exklusionsprinzip

Seien $A_1, A_2, \ldots, A_n$ endliche Mengen. Dann gilt:

$$|\bigcup_{i=1}^{n} A_i| = \sum_{k=1}^{n} ((-1)^{k+1} \cdot \sum_{\substack{i_1,\ldots,i_k=1 \\ \text{paarweise verschieden}}}^{n} |A_{i_1} \cap \ldots A_{i_k}|)$$

Zählen

Grundlegende Zählprinzipien

Dirichlets Taubenschlagprinzip:

Halten sich $k+1$ Tauben in k Taubenschlägen auf, so gibt es mindestens einen Taubenschlag, in dem sich wenigstens zwei Tauben befinden.

Verallgemeinertes Taubenschlagprinzip:

Halten sich n Objekte auf k Fächer verteilt, dann gibt es mindestens ein Fach, das wenigstens $\frac{n}{k}$ Objekte enthält.

Zählen

Grundlegende Zählprinzipien

Verallgemeinertes Taubenschlagprinzip:

Halten sich n Objekte auf k Fächer verteilt, dann gibt es mindestens ein Fach, das wenigstens $\frac{n}{k}$ Objekte enthält.

Satz: Seien A, B zwei endlichen Mengen, und sei $f : A \longrightarrow B$ eine Funktion. Dann gibt es ein Element $b_0 \in B$ mit $|f^{-1}(b_0)| \geq \frac{|A|}{|B|}$.

Zählen

Grundlegende Zählprinzipien

Dirichlets & Verallgemeinertes Taubenschlagprinzip:

Beispiele

Satz: In einer Gruppe von acht Leuten haben mindestens zwei am gleichen Wochentag Geburtstag.

Satz: In jeder Menge A, die aus drei natürlichen Zahlen gebildet werden kann, sind stets zwei Zahlen, deren Summe gerade ist.

Satz: Sei A eine Gruppe von 6 Leuten, von denen jede beliebig ausgewählte Zweiergruppe entweder befreundet oder verfeindet ist. Dann gibt es in dieser Gruppe 3 Leute, die paarweise befreundet oder die paarweise verfeindet sind.