Diskrete Strukturen und Logik

WiSe 2006/07 in Trier

Henning Fernau
Universität Trier
fernau@informatik.uni-trier.de

Diskrete Strukturen und Logik Gesamtübersicht

- Organisatorisches
- Einführung
- Logik & Mengenlehre
- Beweisverfahren
- Kombinatorik: Die Kunst des Zählens
- algebraische Strukturen

Beweisverfahren — Eine Übersicht

Direkter Beweis
Beweis durch Umkehrschluss
Widerspruchsbeweis (Indirekter Beweis)
Fallunterscheidungen
Schubfachprinzip
Induktion

Peano-Axiome: ein klassisches Beispiel einer *rekursiven Definition*

axiomatische Definition der Menge der natürlichen Zahlen $\mathbb{N}$ durch Giuseppe Peano (1889)
eigentlich von Richard Dedekind in “Was sind und was sollen die Zahlen ?” (1888)
1. 0 ist eine natürliche Zahl.
2. Zu jeder natürlichen Zahl n gibt es genau einen Nachfolger n', der ebenfalls eine natürliche Zahl ist.
3. Es gibt keine natürliche Zahl, deren Nachfolger 0 ist.
4. Zwei verschiedene natürliche Zahlen n und m besitzen stets verschiedene Nachfolger n' und m'.
5. Enthält eine Menge X die Zahl 0 und mit jeder natürlichen Zahl n auch stets deren Nachfolger n', so enthält X bereits alle natürlichen Zahlen. *Induktionsaxiom*
(Ist X dabei selbst eine Teilmenge der natürlichen Zahlen, dann ist $X = \mathbb{N}$.)

Peano verwendet dabei die Begriffe 0, Zahl und *Nachfolger*.

Wie sehen natürliche Zahlen aus ? (nach Dedekind / Peano)

$0, 0', 0'', 0''', 0'''', \ldots$

Es ist jedoch bequemer, bei der gewohnten Schreibweise zu bleiben:

$0, 1, 2, 3, 4, \ldots$

Diese ist überdies deutlich kürzer als die rekursiv definierte.

Rekursion versus Induktion

Induktiv können wir "der Reihe nach" die definierten Objekte auflisten.

Den umgekehrten Weg geht die Rekursion: n' ist eine natürliche Zahl, wenn n eine ist, und das ist der Fall, wenn entweder $n = 0$ gilt oder aber n von der Form m' ist...

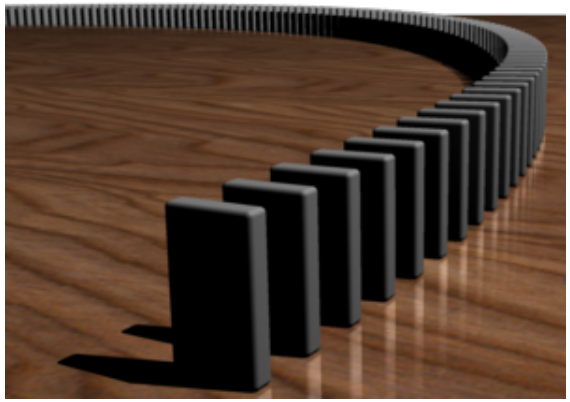
Grundgedanke der mathematischen Induktion

Es sei $p(n)$ eine Aussageform, die von $n \in \mathbb{N}$ abhängt.
Mathematische Induktion ist eine Beweistechnik, die auf dem Induktionsaxiom fußt und schematisch wie folgt arbeitet.

1. *Induktionsanfang* (IA) (auch *Anker* genannt): Zeige $p(0)$.
2. *Induktionsschritt* (IS) Es wird gezeigt, dass für alle $n \in \mathbb{N}$ gilt: $p(n) \Rightarrow p(n+1)$.
$p(n)$ heißt hier auch *Induktionsannahme* oder *Induktionsvoraussetzung* (IV).

Nach dem Prinzip der mathematischen Induktion folgt hieraus: $\forall n(p(n))$.

Induktion veranschaulicht: Der Dominoeffekt:



Die Aufstellung gewährleistet:
Wenn der k-te Dominostein in der Reihe fällt, so auch der $k+1$-te.

Jetzt fällt der erste Dominostein.

Folgerung: Schließlich werden alle Steine umgefallen sein.

Induktion aus logischer Sicht.

Stimmt das Induktionsprinzip ?

$\mathrm{p}(0)$ ist richtig wegen des Ankers.
$\mathrm{p}(1)$ ist wahr, denn $\mathrm{p}(0)$ ist wahr und $\mathrm{p}(0) \Rightarrow \mathrm{p}(1)$ ist Spezialfall des Induktionsschritts, also folgt $\mathrm{p}(1)$ mit modus ponens.
$\mathrm{p}(2)$ ist wahr, denn $\mathrm{p}(1)$ ist wahr und $\mathrm{p}(1) \Rightarrow \mathrm{p}(2)$ ist Spezialfall des Induktionsschritts, also folgt $\mathrm{p}(2)$ mit modus ponens.
...

Induktion aus logischer Sicht.

Angenommen, die Aussage $p(n)$ gölte nicht für alle natürlichen Zahlen n.
Dann gibt es eine kleinste Zahl n_0, für die sie falsch ist. Es gibt nun zwei Fälle:
1. $n_0 = 0$: Dies wird durch den Induktionsanfang ausgeschlossen.
2. $n_0 \neq 0$: Nach Voraussetzung ist n_0 die kleinste Zahl, für die $p(n)$ falsch ist, also ist $p(n_0 - 1)$ wahr.
Induktionsschritt $\rightsquigarrow p((n_0 - 1) + 1)$ ist wahr: Widerspruch.
Beide Fälle können also ausgeschlossen werden, damit ist die Aussage $p(n)$ für alle natürlichen Zahlen n wahr.

Bei diesem Argument wurde im magentafarbenen Teil implizit das harmlos erscheinende *Wohlordnungsaxiom* verwendet:
Jede nichtleere Teilmenge natürlicher Zahlen besitzt ein kleinstes Element.

Induktion am Beispiel.

Satz: $\forall n \in \mathbb{N}(n^2 = \sum_{i=1}^{n}(2i-1))$.

Beweis: IA: Die "leere Summe" ist gleich Null, d.h., die Behauptung gilt für $n = 0$.
IS: Angenommen, die Aussage gilt für n. Dann rechnen wir:

$$\begin{aligned}
(n+1)^2 &= n^2 + 2n + 1 && \text{binomischer Lehrsatz} \\
&= (\sum_{i=1}^{n}(2i-1)) + 2n + 1 && \text{IV} \\
&= \sum_{i=1}^{n+1}(2i-1)
\end{aligned}$$

Nach dem Prinzip der mathematischen Induktion folgt die Behauptung.

Induktion am Beispiel.

Satz: $\forall n \in \mathbb{N}(2^{n+1} - 1 = \sum_{i=0}^{n} 2^i)$.

Beweis: IA: Die Behauptung gilt für $n = 0$: $2^1 - 1 = 1 = 2^0$.
IS: Angenommen, die Aussage gilt für n. Dann rechnen wir:

$$\begin{aligned} 2^{n+2} - 1 &= 2^{n+1} + (2^{n+1} - 1) \\ &= 2^{n+1} + (\sum_{i=0}^{n} 2^i) \qquad \text{IV} \\ &= \sum_{i=0}^{n+1} 2^i \end{aligned}$$

Nach dem Prinzip der mathematischen Induktion folgt die Behauptung.

Induktion am Beispiel: $H_m = \sum_{i=1}^{m} \frac{1}{i}$ *m-te harmonische Zahl*

Möglicherweise bekannt aus Analysis: Die Folge H_m konvergiert nicht gegen eine konstante Zahl, sondern sie wächst über alle Maßen.
Frage: Wie "schnell" wächst H_m mit m ?
Antwort: "Etwa so wie der Logarithmus."

Satz: $\forall n(1 + \frac{n}{2} \leq H_{2^n} \leq 1 + n)$.

Beweis: IA: klar für $n = 0$, denn $H_1 = 1$.

IS (für erste Ungleichung): Angenommen, die Aussage gilt für n. Dann rechnen wir:

$$
\begin{aligned}
H_{2^{n+1}} &= \sum_{i=1}^{2^{n+1}} \frac{1}{i} \\
&= \sum_{i=1}^{2^n} \frac{1}{i} + \sum_{i=2^n+1}^{2^{n+1}} \frac{1}{i} \\
&= H_{2^n} + \sum_{i=2^n+1}^{2^{n+1}} \frac{1}{i} \\
&\geq 1 + \frac{n}{2} + 2^n \cdot \frac{1}{2^{n+1}} \qquad \text{IV und einfache Absch.} \\
&= 1 + \frac{n}{2} + \frac{1}{2} \\
&= 1 + \frac{n+1}{2}
\end{aligned}
$$

Entsprechend sieht man für die zweite Ungleichung:

$$\begin{aligned} H_{2^{n+1}} &= \cdots = H_{2^n} + \sum_{i=2^n+1}^{2^{n+1}} \frac{1}{i} \\ &\leq 1 + n + 2^n \cdot \frac{1}{2^n} \qquad \text{IV und einfache Absch.} \\ &= 1 + n + 1 \\ &= 1 + n + 1 \end{aligned}$$

Nach dem Prinzip der mathematischen Induktion folgt die Behauptung.

Induktion in der Anwendung: *Schleifeninvariante* $P(i, q) := (q = (i-1)^2)$.

1. Lies die natürliche Zahl n ein.

2. Setze $q := 0$ und $i := 1$.
   $\{\ P(1,0) = (0 = (1-1)^2)$ ✓ Induktionsanfang $\}$

3. **Solange** $i \leq n$ **tue**:
   $\{$ IV: Es gilt $P(i, q)$, also $q = (i-1)^2$. $\}$
   $q := q + 2i - 1$;
   $i := i + 1$
   $\{$ IS: Zu zeigen ist $P(i+1, q+2i-1) = (q + 2i - 1 = i^2)$ mit
   $i^2 = ((i-1)+1)^2 = (i-1)^2 + 2(i-1) + 1 = (i-1)^2 + 2i - 1 =^{IV} q + 2i - 1$. $\}$

4. Gib q aus. $\{$ Bei Schleifenaustritt gilt: $i = n + 1. \rightsquigarrow q = n^2$ $\}$

Das Prinzip der **vollständigen mathematischen Induktion** verallgemeinert das bislang Gesagte.
Der Induktionsschritt besteht nun aus dem Schluss

$$\forall n([p(0) \wedge p(1) \wedge \cdots \wedge p(n)] \Rightarrow p(n+1)).$$

Manchmal ist es hilfreich, bei Induktionsbeweisen “tiefer zurück” gehen zu dürfen, um den Induktionsschritt zu beweisen.

Induktion am Beispiel.

Satz: Jede natürliche Zahl ungleich Null kann als Produkt von Primzahlen geschrieben werden.

Beweis: IA: $n = 0$ inhaltsleer wahr. $n = 1$ stimmt (leeres Produkt)

IS: Angenommen, die Aussage gilt für n.

1. Fall: $n + 1$ ist Primzahl. Dann ist die Aussage trivialerweise richtig.

2. Fall: $n + 1$ ist keine Primzahl. Wegen $n > 1$ ist $n + 1$ Produkt zweier Zahlen $(n + 1) = (k \cdot \ell)$ mit $2 \leq k, \ell < n$.

Nach IV lassen sich k, ℓ als Produkt von Primzahlen darstellen und mithin $n + 1$.

Nach dem Prinzip der vollständigen mathematischen Induktion folgt die Behauptung.

Rekursion versus Induktion

In der Informatik finden Sie oft *rekursive Definitionen* allgemeinerer Bauart für *Syntax* und *Semantik* formaler Strukturen.

Beispiel: Was ist ein *wohlgeformter aussagenlogischer Ausdruck* (w.a.A.) ?

1. Die Wahrheitswerte w und f sind w.a.A.
2. Ist x eine aussagenlogische Variable, so ist x ein w.a.A.
3. Ist p ein w.a.A., so auch $\neg \mathrm{p}$.
4. Sind p, q w.a.A., so auch $(\mathrm{p} \wedge \mathrm{q})$, $(\mathrm{p} \vee \mathrm{q})$, $(\mathrm{p} \implies \mathrm{q})$, $(\mathrm{p} \iff \mathrm{q})$.
5. Nichts anderes sind w.a.A.

Beachte: 1. und 2. sind der *Rekursionsanker* .

Rekursion versus Induktion—Fortsetzung des Beispiels

$\alpha = ((x \vee f) \wedge \neg y)$ ist ein w.a.A., denn:

- x ist ein w.a.A. gemäß 2.
- f ist ein w.a.A. gemäß 1.
- $(x \vee f)$ ist ein w.a.A. gemäß 4. (und der voranstehenden Punkte)
- y ist ein w.a.A. gemäß 2.
- $\neg y$ ist ein w.a.A. gemäß 3. (und dem vorigen Punkt)
- α ist ein w.a.A. gemäß 4. (und dem zuvor Hergeleiteten)

Rekursion versus Induktion—Fortsetzung des Beispiels

Eine *Belegung* β eines w.a.A. α ist eine Vorschrift, die jeder in α vorkommenden Variablen einen Wahrheitswert zuordnet. Der Wahrheitswert $\beta(\alpha)$ ergibt sich entlang der rekursiven Definition der w.a.A. wie folgt:

1. $\beta(w)$ ist stets wahr und $\beta(f)$ ist stets falsch.
2. Ist x eine aussagenlogische Variable, so ist $\beta(x)$ der durch die Belegung β angegebene Wahrheitswert.
3. Ist p ein w.a.A., so ist $\beta(\neg p) := \neg(\beta(p))$.
4. Sind p, q w.a.A., so ist $\beta((p \wedge q)) := \beta(p) \wedge \beta(q)$, $\beta((p \vee q)) := \beta(p) \vee \beta(q)$, $\beta((p \implies q)) := \beta(p) \implies \beta(q)$, $\beta((p \iff q)) := \beta(p) \iff \beta(q)$.

Beachte: Unterschied zwischen w.a.A. als “reiner Zeichenfolgenvorschrift” (Syntax) und der ihnen durch Belegungen beigegebenen Bedeutung (Semantik).

Rekursion versus Induktion—Fortsetzung des Beispiels

Zwei w.a.A. α, α' heißen *äquivalent*, i.Z. $\alpha \equiv \alpha'$, gdw. sie dieselben Variablen enthalten und wenn für alle Belegungen β dieser Variablen $\beta(\alpha) = \beta(\alpha')$ gilt.

Ein w.a.A. heiße *vereinfacht*, wenn er weder $\Longrightarrow$ noch $\Longleftrightarrow$ als Symbole enthält.

Satz: Zu jedem w.a.A. gibt es einen äquivalenten vereinfachten.

Beweis: Auf der nächsten Folie definieren wir eine rekursive Prozedur `vereinfache`, welche eine eingegebenen w.a.A. α in einen äquivalenten vereinfachten w.a.A. α' umformt.

Die Prozedur $\texttt{vereinfache}(\alpha)$:

1. Ist $\alpha = w$ oder $\alpha = \mathrm{f}$, so liefere α.
2. Ist $\alpha = x$ für eine Variable x, so liefere α.
3. Ist $\alpha = \neg p$ für einen w.a.A. p, so liefere $\alpha' := \neg\texttt{vereinfache}(p)$.

4a. Ist $\alpha = (p \wedge q)$ für w.a.A. p und q, so liefere $\alpha' := (\texttt{vereinfache}(p) \wedge \texttt{vereinfache}(q))$.

4b. Ist $\alpha = (p \vee q)$ für w.a.A. p und q, so liefere $\alpha' := (\texttt{vereinfache}(p) \vee \texttt{vereinfache}(q))$.

4c. Ist $\alpha = (p \implies q)$ für w.a.A. p und q, so liefere $\alpha' := (\neg\texttt{vereinfache}(p) \vee \texttt{vereinfache}(q))$.

4d. Ist $\alpha = (p \iff q)$ für w.a.A. p und q, so liefere $\alpha' := ((\texttt{vereinfache}(p) \wedge \texttt{vereinfache}(q)) \vee (\neg\texttt{vereinfache}(p) \wedge \neg\texttt{vereinfache}(q)))$.

Satz: Zu jedem w.a.A. gibt es einen äquivalenten vereinfachten.

Beweis: Was müssen wir zeigen ?
1. `vereinfache` liefert stets einen vereinfachten w.a.A.
2. `vereinfache` liefert einen äquivalenten w.a.A.
(3. `vereinfache` *terminiert* stets (hält stets an).)

Alle Beweise arbeiten mit *Induktion über den rekursiven Aufbau* von w.a.A.; diese Abart der Induktion heißt auch *strukturelle Induktion*, da sie entlang der (rekursiven) Struktur arbeitet.

ad 1. IA: Für die Terminierungsbedingung in Schritt 1. und 2. von `vereinfache` ist die Behauptung klar gemäß dem Rekursionsanker in der Definition von w.a.A., außerdem sind die so gelieferten w.a.A. vereinfacht.
IS: Als Induktionsannahme wählen wir: Seien p (und evtl. q) w.a.A., wobei wir voraussetzen, dass `vereinfache`(p) und `vereinfache`(q) tatsächlich vereinfachte w.a.A. liefern.
Damit sind aber nach Definition von w.a.A. auch die durch
`vereinfache`$(\neg p)$,
`vereinfache`$((p \wedge q))$,
`vereinfache`$((p \vee q))$,
`vereinfache`$((p \implies q))$ und
`vereinfache`$((p \iff q))$
gelieferten Ergebnisse vereinfachte w.a.A.
Beispielsweise wird im letzteren Fall ein Ausdruck der Form
$v = ((r \wedge s) \vee (\neg r \wedge \neg s))$ für w.a.A. r, s geliefert.
Mit r und s sind auch $\neg r$ und $\neg s$ und mithin $t = (r \wedge s)$ und $u = (\neg r \wedge \neg s)$ w.a.A. Daher ist auch $v = (t \vee u)$ ein w.a.A.

ad 2. Was müssen wir genauer zeigen ? Ist α ein w.a.A. mit Variablen $x_1, \ldots, x_n$ und ist β eine beliebige Belegung dieser Variablen, so gilt:
$\texttt{vereinfache}(\alpha)$ liefert einen w.a.A. mit Variablen $x_1, \ldots, x_n$ und $\beta(\alpha) = \beta(\texttt{vereinfache}(\alpha))$.
IA klar ...
IS: Als Induktionsannahme wählen wir: Seien p (und evtl. q) w.a.A., wobei wir voraussetzen, dass $\texttt{vereinfache}(p)$ und $\texttt{vereinfache}(q)$ tatsächlich äquivalente w.a.A. liefern. Sei ferner β eine beliebige Belegung für die in p und q (und damit nach IV für die in $\texttt{vereinfache}(p)$ und $\texttt{vereinfache}(q)$) vorkommenden Variablen.
Betrachte Schritt 3.: Mit $\beta(p) = \beta(\texttt{vereinfache}(p))$ (IV) gilt:
$\beta(\alpha) = \beta(\neg p) = \neg\beta(p) =^{IV} \neg\beta(\texttt{vereinfache}(p)) = \texttt{vereinfache}(\neg p) = \texttt{vereinfache}(\alpha)$.
Entsprechend sieht man 4a. und 4b. Betrachte nun 4c.: $\alpha = (p \implies q)$.
(a) $\beta(\alpha) = \beta((p \implies q)) = \beta(p) \implies \beta(q)$.
(b) $\beta(\texttt{vereinfache}(\alpha)) = \beta(\texttt{vereinfache}((p \implies q))) =^{\text{Proz.}}$
$\beta((\neg\texttt{vereinfache}(p) \vee \texttt{vereinfache}(q))) =^{IV} \beta((\neg p \vee q)) = \neg\beta(p) \vee \beta(q)$

(a) und (b) liefern dasselbe wegen der bekannten Tautologie $u \Rightarrow v \equiv \neg u \vee v$.

4d. kann man ebenso nachrechnen. (Welche Tautologie verwenden wir hier ?)

ad. 3. Hier “hilft” wieder ein Induktionsbeweis.

Rekursion versus Induktion—Logischer Anschluss

Was haben rekursive Definitionen und die damit einhergehende *strukturelle Induktion* zu tun mit der anfänglich eingeführten (vollständigen) mathematischen Induktion ?

Beobachte (im Beispiel): Rekursionsanker entspricht w.a.A. ohne Vorkommen von Operatoren. Diese Maßzahl hätten wir explizit bei der rekursiven Definition von w.a.A. angeben können, z.B.: “Ist p ein w.a.A. mit n Vorkommen von Operatoren und q ein w.a.A. mit m Vorkommen von Operatoren, so ist $(\mathrm{p} \wedge \mathrm{q})$ ein w.a.A. mit $\mathrm{n} + \mathrm{m} + 1$ Vorkommen von Operatoren.”

Alle voranstehenden strukturellen Induktionsbeweise lassen sich dann als Beweise lesen, die mit dem Prinzip der vollständigen mathematischen Induktion arbeiten, nämlich über die Zahl der Vorkommen von Operatoren.

Nochmals Peano-Axiome

Wir könnten den axiomatischen Aufbau der natürlichen Zahlen in ähnlicher Weise (vielleicht moderner) wie folgt formulieren:

1. 0 ist eine natürliche Zahl.
2. Ist $\mathfrak{n}$ eine natürliche Zahl, so auch ihr sog. *Nachfolger* $\sigma(\mathfrak{n})$.
3. Nichts weiter sind natürliche Zahlen.

Vergleichen Sie diese mit der klassischen Definition !

Ein abschließendes Beispiel: Money, Money, Money, . . . 

Satz: Jeder Cent-Betrag ≥ 4 Cent kann unter ausschließlicher Verwendung von 2- und 5-Cent-Münzen bezahlt werden.

Beweis: Klar für 4 Cent.

Angenommen, wir wissen, wie $n > 4$ Cent bezahlt werden können, nämlich mit n_2 2-Cent-Münzen und mit n_5 5-Cent-Münzen. $\rightsquigarrow n = 2n_2 + 5n_5$.

Da $n > 4$, gilt $n_2 \geq 2$ oder $n_5 \geq 1$ (leicht einsehbar durch Umkehrschluss).

Wir geben jetzt zwei Regeln an, mit denen wir $n + 1$ Cent mit n_2' 2-Cent-Münzen und mit n_5' 5-Cent-Münzen bezahlen können:

Gilt $n_2 \geq 2$, so setze $n_2' := n_2 - 2$ und $n_5' := n_5 + 1$.

Andernfalls gilt $n_5 \geq 1$. $\rightsquigarrow$ Setze $n_2' = n_2 + 3$, $n_5' := n_5 - 1$.

Probe: $n + 1 = 2n_2 + 5n_5 + 1 = 2(n_2 - 2) + 5(n_5 + 1) = 2(n_2 + 3) + 5(n_5 - 1)$.

Die Behauptung folgt (wie genau ?) mit mathematischer Induktion.