Mathematik I

Vorlesung 3 - Beweistechniken, Vollständige Induktion, Rekursion

Prof. Dr. Sandra Eisenreich

30. Oktober 2023

Hochschule Landshut

3.1 Grundlagen und Beweistechniken

Motivation

Warum interessiert uns als Informatiker so etwas theoretisches wie Beweistechniken (= die Art und Weise, wie man Aussagen logisch nachweisen kann)?

- Schult Abstraktionsvermögen;
- Beweistechnik = logische Denkstruktur, mit der man ein Problem angehen kann. → man lernt auch Informatik-Probleme strukturiert anzugehen;
- Das Vorgehen in Beweisen ist sehr strukturiert → algorithmische Denkweise;

In diesem Einführungskapitel schauen wir uns erst grob verschiedene Beweismethoden an, bevor wir eine spezielle Beweismethode (Induktion) vertiefen.
Anwendung in der Informatik: überall, weil die Denkweise dieselbe ist wie bei Algorithmen.

Beweistechniken

Definition

Ein **Beweis** ist eine Folge von unmittelbar aufeinander aufbauenden logischen Schritten, mit der aus einer Menge von Axiomen und als wahr bekannten Aussagen die Korrektheit einer neuen Aussage hergeleitet wird.

Beweistechniken:

- **direkter Beweis:** hier wird die zu beweisende Aussage direkt aus den Voraussetzungen logisch gefolgert. (der Beweis von $A \Rightarrow B$ ist also von der Form $A \Rightarrow C_1 \Rightarrow C_2 \Rightarrow \ldots \Rightarrow B$)
- **indirekter Beweis:** Um zu zeigen, dass unter der Voraussetzung A die Aussage B folgt ($A \Rightarrow B$), zeigt man: $\neg B \Rightarrow \neg A$.
- **Widerspruchsbeweis:** Man nimmt das Gegenteil der zu beweisenden Aussage B an und leitet einen Widerspruch zur Voraussetzung A her. (man zeigt also: $A \wedge \neg B$ ist falsch).
- **Induktionsbeweis:** nächster Abschnitt.

Beispiel

Wir verwenden, dass man eine gerade (bzw. ungerade) Zahl n schreiben kann als $n = 2 \cdot k$ (bzw. $2 \cdot k + 1$) für eine ganze Zahl k.

- **direkter Beweis für "Sind a und b $\in \mathbb{Z}$ ungerade, so ist a+b gerade.":**
  a und b sind ungerade $\Rightarrow$ gibt es zwei ganze Zahlen k, l mit $a = 2k + 1, b = 2l + 1$ $\Rightarrow$ Dann ist $a + b = 2k + 1 + 2l + 1 = 2k + 2l + 2 = 2(k + l + 1) \Rightarrow a + b$ ist gerade.
- **indirekter Beweis für "Sei $n \in \mathbb{Z}$. Wenn n^2 gerade ist, so ist n auch gerade.":**
  zeige statt dessen: Wenn n keine gerade Zahl ist, ist auch n^2 keine gerade Zahl.
  Ist n ungerade, dann kann man n schreiben als $n = 2k + 1$ für ein $k \in \mathbb{Z}$. Dann gilt
  $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$ ist ungerade, da $4(k^2 + k)$ gerade ist.
- **Widerspruchsbeweis für die obige Behauptung:**
  Angenommen n wäre ungerade. Dann kann man n schreiben als $n = 2k + 1$ für ein $k \in \mathbb{Z}$.
  Dann gilt $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$ ist ungerade, da $4(k^2 + k)$ gerade ist. Dies ist ein Widerspruch zur Voraussetzung, dass n^2 gerade ist.

Summen- und Produktnotation

Wenn eine Summe sehr viele Summanden hat, kann man manchmal abkürzen und es ist trotzdem klar was gemeint ist, z.B. bei

$$1 + 2 + 3 + 4 + \ldots + 100$$

Aber was, wenn nicht so offensichtlich ist, welcher "Regel" die Summanden folgen? → abgekürzte Schreibweise:

$$\sum_{i=1}^{100} i := 1 + 2 + 3 + 4 + \ldots + 100 = \text{“Summe von } i = 1 \text{ bis 100 über i”}$$

Solch eine Notation gibt es auch für Produkte über viele Zahlen:

$$\prod_{i=1}^{100} i := 1 \cdot 2 \cdot 3 \cdot 4 \cdot \ldots \cdot 100 = \text{“Produkt von } i = 1 \text{ bis 100 über i”}$$

Definition

Seien $a_1, \ldots, a_n$ Werte, die man aufsummieren bzw. aufmultiplizieren kann (z.B. reelle Zahlen, oder ganze Zahlen). Dann schreibt man

$$\sum_{i=1}^{n} a_i := a_1 + a_2 + \ldots + a_n = \text{“Summe über } a_i \text{ von } i = 1 \text{ bis } n\text{”}$$

$$\prod_{i=1}^{n} a_i := a_1 \cdot a_2 \cdot \ldots \cdot a_n = \text{“Produkt über } a_i \text{ von } i = 1 \text{ bis } n\text{”}$$

3.2 Vollständige Induktion

Motivation

Denkweise, die funktioniert wie eine Domino-Reihe:

- Wenn irgendein Stein fällt, wirft er den nächsten um.
- Der erste Stein wird umgeworfen.

Dann wissen wir, dass die ganze Reihe fällt.
Genauso funktioniert vollständige Induktion:

Wir wollen eine Aussage $A(n)$ zeigen für alle natürlichen Zahlen $n \in \mathbb{N}$. Aber wenn wir jedes n einzeln beweisen, werden wir nie fertig. Statt dessen beweist man folgendes:

- Wenn für irgendein n $A(n)$ richtig ist, muss auch $A(n+1)$ richtig sein. (Sicherstellen, dass jeder Dominostein auch den nächsten umwirft, wenn er fällt).
- Dann beweist man $A(1)$. (Umwerfen des ersten Steins)

Dann muss $A(n)$ für alle n richtig sein!

Vollständige Induktion

Satz

Sei $A(n)$ eine Aussage über die natürliche Zahl n.

Es gelte:

(a) **Induktionsanfang:** $A(1)$ *ist wahr.*

(b) *für alle $n \in \mathbb{N}$ gilt der* **Induktionsschritt:** *Falls $A(n)$ wahr ist (genannt* **Induktionsannahme/Induktionsvoraussetzung***), dann gilt auch $A(n+1)$.*

Dann ist $A(n)$ wahr für alle $n \in \mathbb{N}$.

Beispiel: Mit Hilfe von vollständiger Induktion kann man zum Beispiel den "kleinen Gauss" zeigen: $A(n) : 1 + 2 + 3 + 4 + \ldots + n = \sum_{i=1}^{n} i = \dfrac{n(n+1)}{2}$

Beweis. Wir zeigen, dass $A(n)$ die beiden Bedingungen c) und b) erfüllt:

(a) **Induktionsanfang:** $A(1) : 1 = \frac{1 \cdot (1+1)}{2} = 1$

(b) **Induktionsannahme:** Angenommen es gilt $A(n)$, also: $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$

Induktionsschluss: z.z.: $A(n+1)$, d.h.

$A(n+1):\ 1 + 2 + \ldots + n + (n+1) = \frac{(n+1) \cdot (n+1+1)}{2}$ Das rechnen wir einfach nach:

$$\begin{aligned} 1 + 2 + \ldots + n + (n+1) &= (1 + 2 + 3 + \ldots + n) + (n+1) \\ &= \frac{n(n+1)}{2} + (n+1) = (n+1) \cdot \left(\frac{n}{2} + 1\right) \\ &= (n+1) \cdot \frac{n+2}{2} = \frac{(n+1)(n+1+1)}{2} \end{aligned}$$

$\blacksquare$

Geometrische Reihe

Eine weitere Anwendung für das Prinzip der Induktion ist:

Satz

Sei $q \in \mathbb{R} \backslash \{1\}$, dann gilt für alle $n \in \mathbb{N}$

$$\underbrace{1 + q + q^2 + \ldots + q^n}_{\text{“geometr. Reihe”}} = \frac{1 - q^{n+1}}{1 - q}$$

Beweis. mit vollständiger Induktion:

Induktionsanfang ($A(1)$ ist wahr) $1 + q = \dfrac{1 - q^2}{1 - q}$ da $\dfrac{1 - q^2}{1 - q} = \dfrac{(1 - q)(1 + q)}{1 - q}$

Induktionsannahme ($A(n)$ ist wahr für ein n) $A(n) : 1 + q + \ldots + q^n = \dfrac{1 - q^{n+1}}{1 - q}$

Induktionsschluss (Zeige, dass $A(n + 1)$ wahr ist unter der Annahme, dass $A(n)$ wahr ist)

$$\underline{1 + q + q^2 + \ldots + q^n} + q^{n+1} = \frac{1 - q^{n+1}}{1 - q} + q^{n+1} = \frac{1 - q^{n+1} + (1 - q)q^{n+1}}{1 - q} = \frac{1 - q^{n+2}}{1 - q} = \frac{1 - q^{(n+1)+1}}{1 - q}$$

Das ist genau die Aussage $A(n + 1)$. Somit gilt $A(n)$ für alle $n \in \mathbb{N}$. ∎

3.3 Verallgemeinertes Induktionsprinzip, Rekursion

Motivation

Wir betrachten die rekursiv definierte Folge (**Fibonacci-Folge**)

$a_0 = 1,\ a_1 = 1,\ a_2 = a_0 + a_1 = 2,\ a_3 = a_1 + a_2 = 1 + 2 = 3,\ \ldots,$ also:

$$a_{n+2} := a_n + a_{n+1} \text{ für alle } n \geq 0.$$

Wir wollen etwas für alle Folgenglieder a_n zeigen. Geht das mit vollständiger Induktion?
Antwort: Nein!
Grund: Induktionsschritt für bei vollständiger Induktion hängt nur vom **jeweils vorangengangenen** Folgenglied ab. Aber hier hängt ein Folgenglied $a_{n+2} := a_n + a_{n+1}$ von den **letzten beiden** ab. Das heißt es reicht nicht, nur das erste "Dominosteinchen" umzuwerfen, sondern wir müssen die ersten beiden umwerfen, damit das dritte umfällt! etc.

Dann können wir vollständige Induktion nicht verwenden, oder doch?

Die Analogie von Domino-Reihen klappt auch hier: Nur dass die Domino-Reihe nicht “normal” aufgestellt ist, sondern die ersten beiden Dominosteinchen so stehen, dass Steinchen 2 erst umfällt wenn sie beide gleichzeitig umfallen, und Steinchen 3 nur fällt wenn 1 und 2 gefallen sind, etc. Der nächste Stein fällt also nur, wenn allgemein **alle Steine zuvor** bereits umgefallen sind!

Dieses Prinzip heißt **verallgemeinertes Induktionsprinzip**: beim Induktionsanfang muss man alle “separaten” Fälle einzeln betrachten, und beim Induktionsschritt dann annehmen, dass alle bisherigen Fälle bereits gezeigt wurden.

Verallgemeinertes Induktionsprinzip

Satz

Sei $A(n)$ eine Aussage über eine ganze Zahl und $n_0 \in \mathbb{Z}$ fest. Es gelte:

- *$A(n_0)$ ist wahr*
- *Aus der Gültigkeit von $A(i)$ für alle i mit $n_0 \leq i \leq n$ folgt auch die Gültigkeit von $A(n+1)$*

Dann gilt die Aussage für alle $n \geq n_0$

Beispiel: Wir betrachten die rekursiv definierte Folge (**Fibonacci-Folge**)

$a_1 = 1,\ a_2 = 1,\ a_3 = a_1 + a_2 = 1 + 1 = 2,\ a_4 = a_2 + a_3 = 1 + 2 = 3,\ \ldots,$ also:

$$a_{n+2} := a_n + a_{n+1} \text{ für alle } n \geq 0.$$

Behauptung: $a_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right)$

Für den Beweis benötigt man das allgemeine Induktionsprinzip.

Beweis. Beachten wir zunächst den Fall $n_0 = n = 1$:

$$\begin{aligned} a_1 &= 1 = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^1 - \left(\frac{1-\sqrt{5}}{2}\right)^1\right) \\ &= \frac{1\cdot(1+\sqrt{5}-1+\sqrt{5})}{\sqrt{5}\cdot 2} = 1 \quad \checkmark \end{aligned}$$

Die Formel gilt also für a_1! Aber: wir können auf Basis von nur einem Wert a_1 noch keinen Induktionsschritt vornehmen, weil die Rekursionsformel $a_{n+2} = a_n + a_{n+1}$ auf **zwei** Werte zugreift! Also brauchen wir für unseren ersten Induktionsschritt noch den Wert für $n = 2$ und können die Aussage mit allgemeiner Induktion für $n \geq 2$ beweisen.

Also: Induktionsanfang für $n_0 = 2$: Wir zeigen, dass $A(2)$ gilt, d.h. Formel ist nichtig für $n = 1$ und $n = 2$ Fur $n = 1$ heben wir das schon gezeigt. für $n = 2$ kann man das auch durch leichtes Nachrechnen zeigen.

Wir rechnen auf der nächsten Seite nach, dass $A(n+1)$ richtig ist unter der Annahme, dass $A(n)$ nichtig ist.

$$
\begin{aligned}
a_{n+1} &= a_n + a_{n-1} \\
&\underset{\substack{\uparrow \\ \text{wegen Ind.} \\ \text{Voraussetzung}}}{=} \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right) + \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n-1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n-1}\right) \\
&= \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n-1}\left(\left(\frac{1+\sqrt{5}}{2}\right)+1\right) - \left(\frac{1-\sqrt{5}}{2}\right)^{n-1}\left(\left(\frac{1-\sqrt{5}}{2}\right)+1\right)\right) \\
&= \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n-1}\left(\frac{3+\sqrt{5}}{2}\right) - \left(\frac{1-\sqrt{5}}{2}\right)^{n-1}\left(\frac{3-\sqrt{5}}{2}\right)\right)
\end{aligned}
$$

$$
\left[\begin{array}{ll} \text{NR:} & (1+\sqrt{5})^2 = 1+5+2\sqrt{5} = 6+2\cdot\sqrt{5} \\ & (1-\sqrt{5})^2 = 6-2\sqrt{5} \end{array}\right]
$$

$$
\begin{aligned}
&= \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n-1}\frac{(1+\sqrt{5})^2}{4} - \left(\frac{1-\sqrt{5}}{2}\right)^{n-1}\cdot\frac{(1-\sqrt{5})^2}{4}\right) \\
&= \frac{1}{\sqrt{5}}\cdot\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right)
\end{aligned}
$$

$\Rightarrow A(n+1)$ ist wahr. ∎

Beispiel: Weitere **wichtige rekursiv definierte Folgen**:

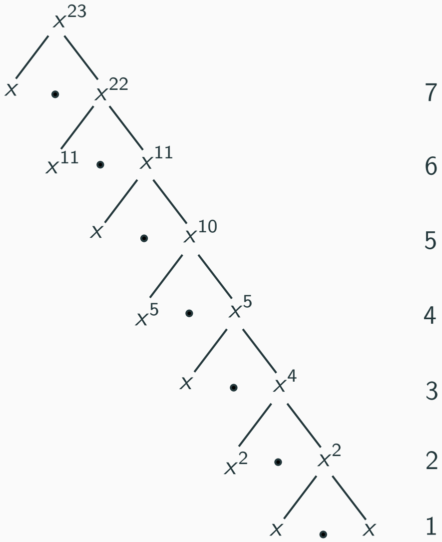
- $n! = n \cdot (n-1)!, \;\; 0! = 1$
  z.B. $7! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7$ (wächst sehr schnell)
- Sei $x \in \mathbb{R}$

$$x^n := \begin{cases} x & \text{falls} \quad n = 1 \\ x \cdot x^{n-1} & \text{sonst} \end{cases}$$

  z.B. $x^3 = x \cdot x^2 = x \cdot x \cdot x$ Eignet sich nicht so gut für die Berechnung von x^n da man $n-1$ Multiplikationen benötigt. **Alternativ:**

$$x^n = \begin{cases} 1 & \text{falls } n = 0 \\ x \cdot x^{n-1} & \text{falls } n \text{ ungerade} \\ x^{\frac{n}{2}} \cdot x^{\frac{n}{2}} & \text{falls } n \text{ gerade} \end{cases}$$

Beispiel: $n = 23$



Es sind nur 7 Multiplikationen notwendig. (vs. 22 Multiplikationen in der andern Rekursion). Allgemein benötigt man mit dieser Methode höchstens $2 \cdot \log_2 n$ Multiplikationen. Das ist für großes n *viel kleiner* als $n - 1$.

Binomialkoeffizient

Es gibt eine weitere wichtige Anwendung von (verallgemeinerter) vollständiger Induktion und Rekursion: die Binomialkoeffizienten. Bisher kennen Sie diese vermutlich aus der Wahrscheinlichkeitsrechnung, wenn man z.B. n verschiedene Kugeln in einer Urne hat und k davon zieht, ohne sie zurückzulegen.

Definition

für $k, n \in \mathbb{N}_0, k \leq n$, definieren wir

$\binom{n}{k}$:= Anzahl der Teilmengen der Mächtigkeit k einer Menge mit n Elementen

Beispiel:

- $n = 6,\ k = 1$. Dann ist $\binom{6}{1} = 6$
- $n = 3,\ k = 2$. Dann ist $\binom{3}{2} = 3$, da die zweielementigen Teilmengen von $\{1, 2, 3\}$ gegeben sind durch $\{1, 2\}, \{1, 3\}, \{2, 3\}$.
- $n,\ k = n - 1$. Dann ist $\binom{n}{n-1} = n$.
- Was ist $\left(\begin{array}{c} 49 \\ 6 \end{array} \right)$ =? Hierfür brauchen wir eine Rechenregel!

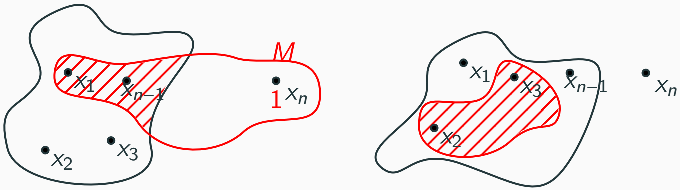
Anwendungen in der Informatik

- wichtig in der Statistik und damit auch in Machine Learning
- Bildverarbeitung: bei Gaußfiltern zur Berechnung
- uvm.

Satz

Sei $k, n \in \mathbb{N}_0$ und $k \leq n$. Dann gilt:

$$\binom{n}{k} = \begin{cases} 1 & \text{falls } k = 0 \text{ oder } k = n \\ \binom{n-1}{k} + \binom{n-1}{k-1} & \text{sonst} \end{cases}$$

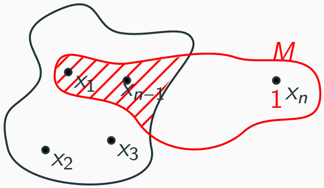


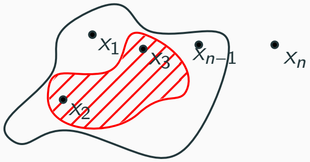
Beweis.

Wir wollen die obige rekursive Formel herleiten. Linke Seit e= Anzahl der k-elementigen Teilmengen $M = \{x_{i_1}, \ldots, x_{i_k}\}$ von einer n-elementigen Menge $M = \{x_1, \ldots x_n\}$. Wir teilen nun diese Mengen M in zwei verschiedene Typen: solche, die das Element x_n enthalten (Typ 1), und solche, die das nicht tun (Typ 2). Wir können also schreiben:

linke Seite = (Anzahl der Mengen vom Typ 1) + (Anzahl der Mengen vom Typ 2)

Wir müssen also nur noch berechnen, wie viele Mengen es vom Typ 1 und Typ 2 gibt:





Typ 1: $x_n \in M$, die anderen $k-1$ Elemente von M sind irgendwelche anderen Elemente in M, also ist $M\backslash\{x_n\}$ eine $(k-1)$-elementige Teilmenge von $M\backslash\{x_n\}$. Somit gibt es von Typ 1 $\binom{n-1}{k-1}$ verschiedene Mengen.

Typ 2: $x_n \notin M$ In diesem Fall ist M eine k-elementige Teilmenge von $M\backslash\{x_n\}$, davon gibt es $\binom{n-1}{k}$ viele.

$$\Rightarrow \binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k} \qquad \blacksquare$$

Es ergibt sich somit das **Pascalsche Dreieck**:

$\sum$	
1	$\binom{0}{0} = 1$
2	$\binom{1}{0} = 1 \quad \binom{1}{1} = 1$
4	$\binom{2}{0} = 1 \quad \binom{2}{1} = 2 \quad \binom{2}{2} = 1$
8	$\binom{3}{0} = 1 \quad \binom{3}{1} = 3 \quad \binom{3}{2} = 3 \quad \binom{3}{3} = 1$
16	$\binom{4}{0} = 1 \quad \binom{4}{1} = 4 \quad \binom{4}{2} = 6 \quad \binom{4}{3} = 4 \quad \binom{4}{4} = 1$

Satz

Es gilt: $\binom{n}{k} = \dfrac{n!}{k!(n-k)!}$

Beweis. (mit Vollständiger Induktion)

Induktionsanfang $n = 0$: Es gibt nur dem Fall $\binom{0}{0} = 1 = \dfrac{0!}{0! \cdot (0-0)!}$

Induktionsschritt $n \to n+1$: Wir müssen zeigen, dass $\binom{n+1}{k} = \dfrac{(n+1)!}{k!(n+1-k)!}$ für alle k. Es gilt (s.oben):

$$\begin{aligned}
\binom{n+1}{k} &= \binom{n}{k-1} + \binom{n}{k} \overset{IV}{=} \frac{n!}{(k-1)!(n-(k-1))!} + \frac{n!}{k!(n-k)!} \\
&= \frac{n! \cdot k + n! \cdot (n-k+1)}{k! \cdot (n-k+1)!} = \frac{n!(k+n-k+1)}{k!(n+1-k)!} \\
&= \frac{n! \cdot (n+1)}{k!(n+1-k)!} = \frac{(n+1)!}{k! \cdot (n+1-k)!} \qquad \blacksquare
\end{aligned}$$

Beispiel: Verwendet man die Formel für $\binom{n}{k}$ für das "Ziehen der Lottozahlen", so ergibt sich

$$\binom{49}{6} = \frac{49!}{6! \cdot 43!} = \frac{49 \cdot 48 \cdot 47 \cdot 46 \cdot 45 \cdot 44}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6} = 13983816$$

Das bedeutet, dass die Wahrscheinlichkeit, 6 Richtige im Lotto zu haben, bei 1/13983816 ist. Berücksichtigt man auch die Reihenfolge der k Elemente, die aus n Elemente ausgewählt werden, dann gibt es sogar

$$\frac{n!}{(n-k)!} = n \cdot (n-1), \ldots, (n-k+1)$$

Möglichkeiten. Warum? $\underbrace{\boxed{n \mid n-1 \mid n-2 \mid n-3 \mid \ldots \mid n-k+1}}_{k}$