Klassische Induktion

Die allgemeine Struktur der klassischen vollständigen Induktion lautet wie folgt: Um eine Gültigkeit einer Aussage $A(n)$ für alle n ab einer gewissen unteren Schranke n_0 nachzuweisen (d.h. für alle $n \geq n_0$) genügt es zu zeigen, dass gilt:

$$\underbrace{A(n_0)}_{\text{IA}} \wedge \underbrace{\forall n \geq n_0 \big(\underbrace{A(n)}_{\text{IV}} \Rightarrow A(n+1) \big)}_{\text{Induktionsschritt (IS)}} \Longrightarrow \forall n \geq n_0 : A(n)$$

Die Abkürzungen stehen dabei für

- IA: Induktionsanfang. Hier ist die Gültigkeit der Aussage $A(n_0)$ zu zeigen.
- IV: Induktionsvoraussetzung. Nachdem der Induktionsanfang gezeigt wurde ist im Induktionsschritt die Annahme, die Aussage $A(n)$ sei korrekt.
- IS: Induktionsschritt. Basierend auf der Induktionsannahme $A(n)$ soll nun gezeigt werden, dass auch $A(n+1)$ gilt.

Dazu direkt zwei Beispiele:

Behauptung 1. *Es gilt* $2^n < n!$ *für alle* $n > 3$.

Beweis. **Induktionsanfang**. Zeige, dass gilt: $A(4) = \big(2^4 < 4!\big)$. Für $n_0 = 4$ erhalten wir $2^4 = 16 < 24 = 1 \cdot 2 \cdot 3 \cdot 4 = 4!$. Damit ist $A(4)$ wahr.

Induktionsschritt. Angenommen die Aussage $A(n) = \big(2^n < n!\big)$ ist wahr (**Induktionsvoraussetzung**), dann haben wir nun zu zeigen, dass gilt: $A(n+1) = \big(2^{n+1} < (n+1)!\big)$. Da $A(n)$ wahr ist folgt aber direkt

$$2 \cdot 2^n = 2^{n+1} < 2 \cdot n! < (n+1)! \quad (\text{da } 2 < n+1 \text{ mit } n > 3).$$

Damit ist $A(n+1)$ gezeigt. $\square$

Behauptung 2. *Für alle* $n \in \mathbb{N}$ *gilt:*

$$\sum_{k=0}^{n} q^k = \frac{1 - q^{n+1}}{1 - q}.$$

Beweis. **Induktionsanfang**. Zeige, dass gilt: $A(0) = \big(q^0 = \frac{1-q^{0+1}}{1-q}\big)$. Das jedoch ist aber klar, denn $q^0 = 1 - \frac{1-q}{1-q}$. Damit ist $A(0)$ wahr.

Induktionsschritt. Angenommen die Aussage $A(n) = \left(\sum_{k=0}^{n} q^k = \frac{1-q^{n+1}}{1-q}\right)$ ist wahr (**Induktionsvoraussetzung**), dann haben wir nun zu zeigen, dass $A(n+1)$ gilt. Wir bemerken zunächst die Identität

$$\sum_{k=0}^{n} q^k = \frac{1-q^{n+1}}{1-q} \iff \sum_{k=0}^{n} (q^k - q^{k+1}) = 1 - q^{n+1},$$

erhalten durch Multiplikation von $A(n)$ mit $(1-q)$. Dann folgt:

$$\begin{aligned}
&(1-q)\sum_{k=0}^{n+1} q^k = \sum_{k=0}^{n+1}(q^k - q^{k+1}) = \sum_{k=0}^{n}(q^k - q^{k+1}) + q^{n+1} - q^{n+2} \\
&\stackrel{\text{IV}}{=} (1-q^{n+1}) + q^{n+1} - q^{n+2} = 1 - q^{n+2} \\
\implies \quad &\sum_{k=0}^{n+1} q^k = \frac{1-q^{n+2}}{1-q}.
\end{aligned}$$

Damit ist $A(n+1)$ gezeigt. □

Aufgaben

(a) Zeige: $1^3 + \cdots + n^3 = (1 + \cdots + n)^2$.

(b) Zeige: 6 teilt die natürliche Zahl $n^3 - n$ für alle $n \in \mathbb{N}$.

(c) Für mehr, befrage Google. :)

Strukturelle Induktion

Beginnen wir mit einem Zitat:

> Bei der vollständigen Induktion werden Eigenschaften der natürlichen Zahlen bewiesen; bei der strukturellen Induktion werden Eigenschaften für **Mengen** bewiesen, deren Elemente aus Grundelementen durch eine **endliche Anzahl von Konstruktionsschritten** (unter Verwendung bereits konstruierter Elemente) beziehungsweise mittels eines Erzeugungssystems entstehen. [Wikipedia]

Gegeben sei also eine Menge M; definiere nun eine Ordnungsrelation $<_M$ auf M. Dann lässt sich die klassiche Induktion über den natürlichen Zahlen wie folgt verallgemeinern (dabei sei $m_0 \in M$):

$$\underbrace{A(m_0)}_{\text{IA}} \wedge \underbrace{\forall m, m', m_0 \leq_M m <_M m' \left(\underbrace{A(m)}_{\text{IV}} \Rightarrow A(m')\right)}_{\text{Induktionsschritt (IS)}} \Longrightarrow \forall m, m_0 \leq_M m : A(m).$$

(Zur Vereinfachung notieren wir hier $\leq_M$ als $m \leq_M m' :\Longleftrightarrow (m <_M m' \vee m = m')$.) Dass dies tatsächlich eine Verallgemeinerung des Induktionsprinzips über $\mathbb{N}$ ist sehen wir mit $M = \mathbb{N}$ und der Ordnung $<_{\mathbb{N}}$, definiert als $n <_{\mathbb{N}} n' :\Longleftrightarrow n' = n+1$ für alle $n \in \mathbb{N}$. Insbesondere haben wir bei der strukturellen Induktion nicht notwendigerweise eine **sichtbare** Induktionsvariable n, wie die folgenden drei Beispiele zeigen werden.

Behauptung 3. *Sei Σ ein beliebiges Alphabet. Dann ist die Menge der regulären Ausdrücke $REG(\Sigma)$ abgeschlossen unter der Operation rev (Umkehrung regulärer Ausdrücke), d.h. für jedes $\alpha \in REG(\Sigma)$ gilt $rev(\alpha) \in REG(\Sigma)$.*

Beweis. Setze $M = \mathrm{REG}(\Sigma)$ und definiere

$$\alpha <_M \beta :\Longleftrightarrow \left(\alpha \text{ ist Teilausdruck von } \beta,\ \alpha \in \mathrm{REG}(\Sigma)\right).$$

Konstruiere rev wie folgt rekursiv:

$$\mathrm{rev}(\emptyset) := \emptyset, \tag{R0}$$
$$\mathrm{rev}(a) := a \text{ für alle } a \in \Sigma, \tag{R1}$$
$$\mathrm{rev}(\alpha + \beta) := \mathrm{rev}(\alpha) + \mathrm{rev}(\beta) \text{ für alle } \alpha, \beta \in \mathrm{REG}(\Sigma), \tag{R2}$$
$$\mathrm{rev}(\alpha\beta) := \mathrm{rev}(\beta)\mathrm{rev}(\alpha), \tag{R3}$$
$$\mathrm{rev}(\alpha^*) := (\mathrm{rev}(\alpha))^*. \tag{R4}$$

Induktionsanfang:

- Zeige: Ist $\emptyset \in \mathrm{REG}(\Sigma)$, so ist auch $\mathrm{rev}(\emptyset) \in \mathrm{REG}(\Sigma)$. Das aber folgt direkt nach (R0) in der Konstruktion von rev.
- Zeige: Ist $a \in \Sigma$, so ist auch $\mathrm{rev}(a) \in \mathrm{REG}(\Sigma)$. Das folgt direkt nach (R1) in der Konstruktion von rev, also $\mathrm{rev}(a) = a$ für alle $a \in \Sigma \subset \mathrm{REG}(\Sigma)$.

Induktionsschritt: Sei $\gamma = \alpha \bullet \beta$ (für eine Operation $\bullet \in \{+, \cdot\}$) mit $\alpha, \beta <_M \gamma$ und α, β zwei von $\emptyset$ verschiedene reguläre Ausdrücke. Angenommen auch $\mathrm{rev}(\alpha)$ und $\mathrm{rev}(\beta)$ sind reguläre Ausdrücke (**Induktionsvoraussetzung**). Dann gilt:

$$\mathrm{rev}(\gamma) = \mathrm{rev}(\alpha + \beta) \overset{(R2)}{=} \mathrm{rev}(\alpha) + \mathrm{rev}(\beta) \overset{\text{IV}}{\Longrightarrow} \mathrm{rev}(\alpha) + \mathrm{rev}(\beta) \in \mathrm{REG}(\Sigma)$$
$$\mathrm{rev}(\gamma) = \mathrm{rev}(\alpha\beta) \overset{(R3)}{=} \mathrm{rev}(\beta)\mathrm{rev}(\alpha) \overset{\text{IV}}{\Longrightarrow} \mathrm{rev}(\beta)\mathrm{rev}(\alpha) \in \mathrm{REG}(\Sigma)$$

Analog zeigt man die Aussage für (R4) mit $\gamma = (\alpha)^*$. Damit ist die Abgeschlossenheit unter rev bewiesen. □

Behauptung 4. *Gegeben sei eine kontextfreie Grammatik $G = (\Sigma, V, P, X)$, definiert durch*

$$\begin{aligned}
&\Sigma = \{a, b\},\\
&V = \{X\},\\
&P = \{X \to \varepsilon,\ X \to aXbX,\ X \to bXaX\}
\end{aligned}$$

Dann gilt für die durch G erzeugte Sprache $L(G)$, dass $L(G) = L := \{w \in \{a,b\}^* \mid |w|_a = |w|_b\}$.

Beweis. Setze $M = L(G)$ und definiere $<_M$ als

$$w <_M w' :\Longleftrightarrow \big(w \text{ ist Präfix von } w' \text{ und } \exists k \in \mathbb{N} \colon X \to_G^k w\big).$$

Wir haben zwei Inklusionen zu zeigen: $L(G) \subseteq L$ und $L \subseteq L(G)$. Die erste Inklusion ist sofort ersichtlich, denn durch jede Produktion werden einem Wort identisch viele a's und b's hinzugefügt.

Widmen wir uns daher der zweiten Inklusion, also $L \subseteq L(G)$. Wir zeigen diese durch strukturelle Induktion über die Produktionen der Grammatik G.

Induktionsanfang:

$(n = 0)$ Das Wort $w = \varepsilon$ kann erzeugt werden, nämlich durch $X \to_G \varepsilon$.

$(n = 1)$ Sei $w \in L$ ein Wort bestehend aus jeweils einem a und b, d.h. $|w|_a = |w|_b = n$. Beide Worte können in der Grammatik G aus dem Startsymbol X abgeleitet werden:

$$\begin{aligned}
X &\to_G aXbX \to_G a\varepsilon b\varepsilon = ab\\
X &\to_G bXaX \to_G b\varepsilon a\varepsilon = ba
\end{aligned}$$

Induktionsschritt: Angenommen alle Wörter $v \in L$ mit $|v| \leq 2n$ können in G abgeleitet werden (**Induktionsvoraussetzung**). Sei nun $w \in L$ ein Wort der Länge $2(n+1)$. Ohne Einschränkung beginne w mit a, d.h. $w = aw_2 \ldots w_{2(n+1)}$. Sei u der kürzeste von w verschiedene Präfix von w, der in L liegt. Da u der kürzeste Präfix von w in L ist, folgt zum einen $|u| \leq 2n$, und zum anderen $u = avb$ für ein v in L nach Induktionsvoraussetzung.[1] Damit ist nun w von der Form

$$w = u\underbrace{w_{|u|+1}\cdots w_{2(n+1)}}_{:=w'} = \underbrace{avb}_{u}w'.$$

[1] Salopp gesagt garantieren wir durch die Forderung an u der kürzeste Präfix von w zu sein, dass v nicht unnötig mit Ableitungen der zweiten Variable X abgeleitet wird; sprich v ist nicht von der Form $a \ldots bb \ldots a \ldots b \ldots a \ldots$.

Da $|v|, |w'| \leq 2n$ wenden wir die Induktionsvoraussetzung, v und w' seien ableitbar in G da der Länge $\leq 2n$, an und erhalten:

$$X \to_G aXbX \to_G^* avbw' = w.$$

Damit ist $w \in L(G)$. □

Behauptung 5. *Sei T ein Binärbaum mit n_T Knoten und Höhe h_T. Dann gilt: $n_T \leq 2^{h_T+1} - 1$.*

Beweis. Sei M die Menge aller Binärbäume, und definiere $<_M$ als

$$T <_M T' :\Longleftrightarrow \big(T \text{ ist Teilbaum von } T'\big).$$

Ein Teilbaum von T' zu sein bedeutet, es gibt einen Knoten v in T', so dass der durch v induzierte Teilbaum[2] dem Binärbaum T entspricht.

Induktionsanfang: T bestehe aus $n_T = 1$ Knoten. Damit hat T insbesondere die Höhe 0 und es gilt: $2^{0+1} - 1 = 1 = n_T$.

Induktionsschritt: Definiere einen Binärbaum T der Höhe h_T mit Wurzel v, dessen linkes und rechtes Kind Binärbäume T_1 und T_2 seien. Für T_1 und T_2 gelte zudem $T_1, T_2 <_M T$ (das ist klar durch unsere Konstruktion; daraus folgt insbesondere $h_1, h_2 < h_T$). Desweiteren gilt $n_T = 1 + n_1 + n_2$. Es folgt abschliessend:

$$1 + n_1 + n_2 \leq 1 + 2^{h_1+1} + 2^{h_2+1} - 2 \leq 2^{\max\{h_1,h_2\}+2} - 1 = 2^{h_T+1} - 1.$$

□

Abschliessende Bemerkungen

In der Regel spart man es sich bei struktureller Induktion eine Ordnungsrelation $<_M$ explizit anzugeben. Da diese jedoch essentiell für diese Beweistechnik ist muss die Relation zumindest implizit durch den Beweis definiert sein. Beispielsweise ist es im letzten Beweis über die Höhe von Binärbäumen damit getan zu bemerken, dass T aus zwei Binärbäumen zusammengesetzt wird. Damit ist dann klar, dass es sich bei der Ordnungsrelation um eine (salopp gesagt) "'ist Teilbaum"'-Relation handelt.

[2] D.h., der durch v induzierte Teilbaum von T' besteht aus v und allen Knoten w in T', für die ein Pfad von w nach v in T' existiert.