Kapitel 4

Induktive Definitionen und Beweise

Bei der Definition der Semantik der Programmiersprache IMP haben wir an vielen verschiedenen Stellen induktive Definitionen benutzt: angefangen bei der Syntax von IMP, über die Semantik der Ausdrücke bis hin zur Semantik der Anweisungen. Teilweise waren die Definitionen explizit induktiv, wie beispielsweise bei der Definition der Semantik für arithmetische Ausdrücke. Teilweise waren die Definitionen „versteckt“ induktiv. Beispielsweise verbirgt sich hinter der Definition der Syntax durch eine Grammatik auch eine induktive Definition; ebenso verbirgt sich hinter der Definition der Semantik durch Regeln eine induktive Definition.

Wenn man genau hinsieht, gibt es in der Informatik fast nichts, was nicht induktiv definiert wäre. Davon werden wir uns im weiteren Verlauf der Vorlesung noch überzeugen können. Deshalb spielen induktive Definitionen und Beweise in der Informatik eine ganz zentrale Rolle – ob man sie nun explizit macht oder nicht.

Aus diesem Grunde beschäftigen wir uns in diesem Kapitel ausführlich mit diesem Thema. Wir beginnen damit, daß wir das Prinzip der *vollständigen Induktion* zur *Noetherschen Induktion* verallgemeinern. Danach werden wir das Prinzip der *induktiven Definition* mit Hilfe von *Regeln* und der durch sie definierten Menge präzisieren. Dann werden wir zeigen, wie man Eigenschaften von induktiv definierten Mengen beweisen kann: die *Regelinduktion*. Am Ende beschäftigen wir uns dann mit der *Herleitung* und der Definition *induktiv über die Struktur einer Menge*.

1 Noethersche Induktion

Ein grundlegendes und sehr einfaches Beweisprinzip, das teilweise schon im Schulunterricht in der Oberstufe vermittelt wird, ist das Prinzip der *vollständigen Induktion*. Dabei beweist man, daß eine Aussage für alle natürlichen Zahlen gilt, indem man die Aussage für $i = 0$ beweist und darüber hinaus zeigt, daß die Aussage für $i + 1$ gilt, falls sie für i gilt. Man „hangelt“ sich mit diesem Prinzip ausgehend von der Aussage für 0 zu jeder natürlichen Zahl durch. Die Aussage gilt damit für jede natürliche Zahl.
Dieses Prinzip können wir wie folgt formulieren, wobei wir die Aussage durch ein Prädikat $P \subseteq \mathbb{N}$ formalisieren. Wir sagen, daß das Prädikat bzw. die Aussage für eine Zahl n gilt, wenn $n \in P$ gilt; wir schreiben dafür auch $P(n)$.

Prinzip 4.1 (Vollständige Induktion)
Sei $P \subseteq \mathbb{N}$ ein Prädikat über den natürlichen Zahlen. Wenn

Induktionsanfang: $P(0)$ gilt und

Induktionsschritt: für jedes $i \in \mathbb{N}$ mit $P(i)$ auch $P(i + 1)$ gilt,

dann gilt $P(n)$ für jedes $n \in \mathbb{N}$ (d. h. $P = \mathbb{N}$).

> *Im Induktionsschritt nennt man die Voraussetzung $P(i)$ auch die* Induktionsvoraussetzung.
>
> *Man kann das Prinzip der vollständigen Induktion auch knapp wie folgt formulieren:*
>
> $$(P(0) \wedge \forall i \in \mathbb{N}.(P(i) \Rightarrow P(i + 1))) \Rightarrow \forall n \in \mathbb{N}.P(n)$$
>
> *Tatsächlich ist das Induktionsprinzip ein Axiom zur Formalisierung der natürlichen Zahlen. Deshalb beweisen wir das Induktionsprinzip auch nicht. Allerdings beschäftigen wir uns hier nicht mit der Axiomatisierung der natürlichen Zahlen. Wir wenden das Prinzip „nur“ an – zum Beweisen von Aussagen.*

Um zu sehen, wie man das Induktionsprinzip zum Beweisen einer Aussage einsetzen kann, betrachten wir ein einfaches Beispiel.

> *In der Vorlesung wird das Prinzip der vollständigen Induktion nur kurz wiederholt. Der folgende Beweis wird gar nicht besprochen. Er sollte aber ohne Probleme mit den Kenntnissen des Grundstudiums verständlich sein.*

Beispiel 4.1
Aus der Schule wissen wir, daß sich die Summe aller Zahlen von 1 bis zu einer Zahl n geschlossen durch den Ausdruck $\frac{n\cdot(n+1)}{2}$ darstellen läßt, d. h. für jede natürliche Zahl $n \in \mathbb{N}$ gilt:

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

Wir beweisen diese Aussage nun mit Hilfe der vollständigen Induktion. Dabei ist das Prädikat P wie folgt definiert:

$$P(n) \equiv \sum_{i=1}^{n} i = \frac{n \cdot (n+1)}{2}$$

Wir beweisen nun durch vollständige Induktion, daß $P(n)$ für jedes $n \in \mathbb{N}$ gilt:

Induktionsanfang: Wir müssen $P(n)$ für $n = 0$, d. h. $\sum_{i=1}^{0} i = \frac{0\cdot(0+1)}{2}$, zeigen. Offensichtlich gilt $\sum_{i=1}^{0} i = 0 = \frac{0\cdot(0+1)}{2}$.

Induktionsvoraussetzung: Wir gehen nun davon aus, daß für ein $n \in \mathbb{N}$ die Aussage $P(n)$ gilt, d. h. $\sum_{i=1}^{n} i = \frac{n\cdot(n+1)}{2}$.

Induktionsschritt: Wir zeigen nun, daß dann auch die Aussage $P(n+1)$ gilt, d. h. $\sum_{i=1}^{n+1} i = \frac{n+1\cdot((n+1)+1)}{2}$:

$$\begin{array}{rcll}
\sum_{i=1}^{n+1} i & = & (\sum_{i=1}^{n} i) + (n+1) & \text{Aufteilung der Summe} \\
& = & \frac{n\cdot(n+1)}{2} + (n+1) & \text{Induktionsvoraussetzung} \\
& = & \frac{n\cdot(n+1)+2\cdot(n+1)}{2} & \text{Rechenregeln} \\
& = & \frac{(n+1)\cdot(n+2)}{2} & \text{Rechenregeln} \\
& = & \frac{(n+1)\cdot((n+1)+1)}{2} & \text{Rechenregeln}
\end{array}$$

Gemäß des Prinzips der vollständigen Induktion gilt damit $P(n)$ für jedes $n \in \mathbb{N}$. Die Aussage $\sum_{i=1}^{n} i = \frac{n\cdot(n+1)}{2}$ ist damit für jedes $n \in \mathbb{N}$ bewiesen.

Diese Aussage kann man auch ohne (explizite Benutzung der vollständigen Induktion) beweisen:

$$\begin{array}{ccccccccc}
1 & + & 2 & + & \ldots & + & (n-1) & + & n \\
n & + & (n-1) & + & \ldots & + & 2 & + & 1 \\
\hline
(n+1) & + & (n+1) & + & \ldots & + & (n+1) & + & (n+1)
\end{array}$$

Die doppelte Summe aller Zahlen von 1 bis n ist also $n \cdot (n+1)$. Allerdings verbirgt sich hinter den Pünktchen ... doch wieder eine heimliche Induktion.

Das Beweisprinzip der Induktion ist nicht auf die Struktur der natürlichen Zahlen beschränkt. Die einzige Voraussetzung ist, daß die zugrundeliegende Struktur einen oder mehrere „Anfänge“ besitzt und daß jedes Element ausgehend von diesen „Anfängen“ irgendwann erreicht wird. Solche Strukturen sind gerade die wohlgegründeten Ordnungen (siehe Kapitel 2 Abschnitt2). Das Prinzip der Noetherschen Induktion sagt, daß eine Aussage für alle Elemente einer wohlgegründeten Ordnung gilt, wenn man für jedes Element zeigen kann, daß die Aussage für das Element selbst gilt, wenn sie für alle Vorgänger des Elementes gilt.

Prinzip 4.2 (Noethersche Induktion)
Sei $(X, \prec)$ eine wohlgegründete (irreflexive) Ordnung und $P \subseteq X$ ein Prädikat über X. Wenn für jedes $x \in X$, für das für jedes $y \in Y$ mit $y \prec x$ die Aussage $P(y)$ gilt, auch $P(x)$ gilt, dann gilt für jedes $z \in X$ die Aussage $P(z)$ (d. h. $P = X$).

Wir können analog zum Prinzip der vollständigen Induktion das Prinzip der Noetherschen Induktion wie folgt formulieren:

$$(\forall x \in X.((\forall y \prec x.P(y)) \Rightarrow P(x))) \Rightarrow \forall z \in X.P(z)$$

Die Bedingung $\forall y \prec x.P(y)$ ist dann gerade die Induktionsvoraussetzung für $P(x)$ in der Noetherschen Induktion.

Die Noethersche Induktion hat ihren Namen von der Mathematikerin Emmy Noether erhalten.

Oft wird das Prinzip der Noetherschen Induktion noch allgemeiner für wohlgegründete Relationen formuliert (eine Relation ist wohlgegründet, wenn sie keine unendlich absteigende Ketten besitzt).

Die Prinzipien der Noetherschen Induktion und der vollständigen Induktion sind sich strukturell sehr ähnlich. Im Induktionsschritt zeigt man für jedes Element, daß die Aussage für dieses Element gilt, wenn sie für alle seine Vorgänger gilt. Was man bei der Noetherschen Induktion auf den ersten Blick vermißt, ist der Induktionsanfang. Haben wir den Induktionsanfang vergessen?
Die Antwort ist, daß der Induktionsanfang im Induktionsschritt enthalten ist. Das sieht man, wenn wir ein minimales Element $x \in X$ der Ordnung betrachten[1]. Per Annahme besitzt x keine Vorgänger. Dementsprechend ist

[1] Zur Erinnerung: In der ersten Übung haben wir gezeigt, daß jede nicht-leere Teilmenge von X einer wohlgegründeten Ordnung ein minimales Element enthält. Deshalb besitzt X ein minimales Element, wenn X wenigstens ein Element enthält.

die Induktionsvoraussetzung $\forall y \prec x.P(y)$ für jedes minimales Element eine triviale Aussage (eine über die leere Menge). Für ein minimales Element x ist dementsprechend die Bedingung der Noetherschen Induktion äquivalent zu $P(x)$. Wir müssen also für die minimalen Elemente x die Aussage $P(x)$ ohne weitere Voraussetzungen beweisen. Das entspricht gerade dem Induktionsanfang.

Beispiel 4.2 (Euklid)
In Beispiel 3.1 hatten wir bereits den Algorithmus von Euklid zum Berechnen des größten gemeinsamen Teilers zweier Zahlen in unsere Programmiersprache IMP formuliert:

```
while ¬(x = y) do
⌜ if x ≤ y then y:= y − x
             else x:= x − y   ⌟
```

Der Einfachheit halber bezeichnen wir dieses Programm mit E für Euklid. Wir werden nun mit Hilfe der Noetherschen Induktion beweisen, daß dieses Programm für jeden Zustand σ mit $\sigma(x) \geq 1$ und $\sigma(y) \geq 1$ terminiert, d. h. daß ein Zustand σ' mit $\langle E, \sigma\rangle \to \sigma'$ existiert.
Zunächst definieren wir die irreflexive Ordnung, über die wir die Induktion ausführen. Wir definieren $X = \{\sigma \in \Sigma \mid \sigma(x) \geq 1 \wedge \sigma(y) \geq 1\}$. Die Ordnung $\prec$ auf X definieren wie folgt: $\sigma' \prec \sigma$ gdw. $\sigma'(x) \leq \sigma(x)$ und $\sigma'(y) \leq \sigma(y)$ und $\sigma'(x) \neq \sigma(x)$ oder $\sigma'(y) \neq \sigma(y)$. Die Ordnung $(X, \prec)$ ist dann wohlgegründet.
Zunächst formalisieren wir das Prädikat, das wir dann mit Hilfe der Noetherschen Induktion beweisen werden:

$$P(\sigma) = \exists \sigma' \in \Sigma.\langle E, \sigma\rangle \to \sigma'$$

Sei nun $\sigma \in \Sigma$ beliebig:

Induktionsannahme: Wir nehmen an, daß für jedes $\sigma'' \prec \sigma$ ein σ''' mit $\langle E, \sigma''\rangle \to \sigma'''$ existiert.

Induktionsschritt: Wir beweisen nun, daß dann auch für σ ein σ' mit $\langle E, \sigma\rangle \to \sigma'$ existiert:

Dazu unterscheiden wir zwei Fälle:

1. **Fall** $\sigma(x) = \sigma(y)$**:** In diesem Falle gilt $\langle \neg(x = y), \sigma\rangle \to \mathit{false}$. Mit der 1. Regel für die Schleife ist damit $\langle E, \sigma\rangle \to \sigma$ herleitbar. Damit gilt die zu beweisende Aussage (mit $\sigma' = \sigma$).

2. Fall $\sigma(x) \neq \sigma(y)$**:** In diesem Falle gilt $\langle \neg(\mathrm{x} = \mathrm{y}), \sigma\rangle \rightarrow \mathit{true}$. Außerdem ist mit den Regeln für die Bedingte Anweisung und für die Zuweisung

$$\langle \textbf{if } (\mathrm{x} \leq \mathrm{y}) \textbf{ then } \mathrm{y} := \mathrm{y} - \mathrm{x} \textbf{ else } \mathrm{x} := \mathrm{x} - \mathrm{y}, \sigma\rangle \rightarrow \sigma''$$

mit

$$\sigma'' = \begin{cases} \sigma[\sigma(y) - \sigma(x)/y] & \text{für } \sigma(y) > \sigma(x) \\ \sigma[\sigma(x) - \sigma(y)/x] & \text{für } \sigma(x) > \sigma(y) \end{cases}$$

herleitbar. Insbesondere gilt $\sigma'' \in X$ und $\sigma'' \prec \sigma$. Wegen Induktionsvoraussetzung gilt also $P(\sigma'')$. Es gibt also ein σ''' mit $\langle E, \sigma''\rangle \rightarrow \sigma'''$. Mit der Regel für die Schleife können wir damit $\langle E, \sigma\rangle \rightarrow \sigma'''$ herleiten. Damit gilt die zu beweisende Aussage (mit $\sigma' = \sigma'''$).

Damit haben wir per Noetherscher Induktion die Aussage $P(\sigma)$ für jedes $\sigma \in X$ bewiesen.

In diesem Beispiel hätten wir den Beweis mit Hilfe der Vollständigen Induktion führen können. Mit Hilfe der Noetherschen Induktion wird der Beweis aber oft viel einfacher.

2 Induktive Definitionen

Wir haben im Kapitel 3 *induktive Definitionen* in verschiedenen Formen benutzt: Grammatiken (bzw. die BNF), Regeln und die explizite Form. Hinter allen diesen Definitionen steckt dasselbe Prinzip:

- Für bestimmte Elemente wird gesagt, daß sie unbedingt zu der definierten Menge gehören.
- Für andere Elemente wird gesagt, daß sie unter der Voraussetzung zu der definierten Menge gehören, daß andere Elemente Menge bereits zu der Menge gehören.

Der erste Fall entspricht gerade den Axiomen, der zweite Fall entspricht gerade den Regeln (mit mind. einer Voraussetzung).
Um den Begriff der induktiven Definition formal zu fassen, definieren wir dazu zunächst den Begriff der Regel bzw. der Regelinstanz. Dabei gehen wir immer

davon aus, daß die Regeln auf einer vorgegebenen Menge von „potentiellen Objekten“ operieren und die Regeln dann eine Teilmenge davon definieren. In der Praxis wird diese Menge von „potentiellen Objekten“ oft nicht explizit erwähnt. Für die Formalisierung des Begriffes müssen wir diese Menge X, auf der die Regeln arbeiten, explizit machen.

Definition 4.3 (Regel und Axiom)
Sei X eine Menge. Für eine endliche Teilmenge $Y \subseteq X$ und ein Element $x \in X$ nennen wir das Paar (Y, x) eine *Regelinstanz* über X. Die Elemente der Menge Y nennen wir die *Voraussetzungen* der Regel, das Element x nennen wir die *Folgerung* der Regel.

Manchmal reden wir auch von der linken und rechten Seite einer Regel.

Eine Regelinstanz $(\emptyset, x)$ nennen wir *Axiominstanz*.

Im folgenden werden wir meist nur von Regeln und Axiomen reden, wenn wir Regelinstanzen und Axiominstanzen meinen. Der Grund für die Unterscheidung zwischen dem Begriff der Regel und der Regelinstanz ist, daß wir bei der syntaktischen Formulierung einer Regel meist unendlich viele Regelinstanzen bezeichnen. Beispielsweise steht die eine Regel bzw. das eine Axiom über $Aexp \times \Sigma \times \mathbb{Z}$ aus Abschnitt 2.2

$$\frac{}{\langle n, \sigma \rangle \to n}$$

für unendlich viele Regelinstanzen: Für jedes $n \in \mathbb{Z}$ und jeden Zustand $\sigma \in \Sigma$ ist $(\emptyset, (n, \sigma, n))$ eine Instanz dieser Regel. Um zwischen der syntaktischen Repräsentation einer Regel und ihren meist unendlich vielen Instanzen unterscheiden zu können, haben wir in der obigen Definition über Regelinstanzen geredet. Da wir uns aber über die syntaktische Repräsentation von Regeln keine weitere Gedanken machen, werden wir im folgenden nur noch von Regeln reden, wenn wir eigentlich Regelinstanzen meinen.
Wenn wir nun eine Menge von Regeln (die natürlich auch Axiome enthalten kann) angeben, ist nun die Frage, welche Menge durch diese Regeln definiert wird. Ganz klar sollte die definierte Menge die Regeln respektieren, d. h. wenn alle Voraussetzungen in der Menge liegen, dann auch ihre Folgerung. Eine Menge, die diese Eigenschaft besitzt, nennen wir *abgeschlossen* unter der Regelmenge, oder kurz R-abgeschlossen, wobei R die Menge der Regeln bezeichnet:

Definition 4.4 (Unter einer Regelmenge abgeschlossene Menge)
Sei R eine Menge von Regeln über X. Eine Menge $Q \subseteq X$ heißt *abgeschlossen* unter R (kurz R-abgeschlossen), wenn für jede Regel(instanz) $(Y, x) \in R$ mit $Y \subseteq Q$ auch $x \in Q$ gilt.

Offensichtlich enthält jede R-abgeschlossene Menge all die Elemente, die auf der rechten Seite eines Axioms auftreten. Denn für die linke Seite $\emptyset$ eines Axioms gilt immer $\emptyset \subseteq Q$ und damit muß die rechte Seite x in Q liegen. Die Frage ist nun, ob für eine gegebene Regelmenge R über X überhaupt eine R-abgeschlossene Menge existiert. Falls sie existiert, müssen wir uns überlegen, ob sie eindeutig ist. Die erste Frage ist einfach zu beantworten, denn die Menge X ist trivialerweise immer R-abgeschlossen. Und das beantwortet auch schon fast die zweite Frage: im allgemeinen gibt es mehrere verschiedene R-abgeschlossene Mengen.

Beispiel 4.3 (Abgeschlossene Mengen)
Wir betrachten die Menge $X = \{a, b\}$ und die Regeln $R = \{(\{a\}, b), (\{b\}, a)\}$. Dann sind die beiden Mengen $\emptyset$ und X abgeschlossen unter R. Die leere Menge ist für diese Regeln R auch R-abgeschlossen, da in ihr kein Axiom vorkommt. Es muß also kein Element unbedingt in die Menge aufgenommen werden.
Dagegen sind die beiden Mengen $\{a\}$ und $\{b\}$ nicht R-abgeschlossen, da die Regeln verlangen, daß das jeweils andere Element auch in die Menge gehört.

Man kann sich leicht Beispiele für Regelmengen überlegen, für die noch sehr viel mehr abgeschlossene Mengen existieren. Die Frage ist nun, welche der R-abgeschlossenen Mengen die durch die Regelmenge induktiv definierte Menge sein soll. Die Idee ist, daß wir nur das in die induktiv definierte Menge aufnehmen sollten, was unbedingt nötig ist – und nicht mehr. Wir sollten also die kleinste R-abgeschlossene Menge wählen. Zuvor müssen wir uns jedoch davon überzeugen, daß es diese kleinste R-abgeschlossene Menge überhaupt gibt.

Lemma 4.5 (Existenz der kleinsten R-abgeschlossenen Menge)
Sei R eine Menge von Regeln über X.

1. Sei nun $(Q_i)_{i \in I}$ eine Familie von R-abgeschlossenen Mengen, d. h. für jedes $i \in I$ ist Q_i abgeschlossen unter R. Dann ist auch die Menge $Q = \bigcap_{i \in I} Q_i$ unter R abgeschlossen.

2. Es gibt eine bzgl. Mengeninklusion $\subseteq$ kleinste R-abgeschlossene Menge.

Beweis: Der Beweis von 1. ist einfach. Der Beweis von 2. benutzt 1.

Den Beweis werden wir in der Übung besprechen.

□

Zur Erinnerung: Das kleinste Element einer Menge ist, wenn es existiert, eindeutig.

Da wir nun wissen, daß es für jede Regelmenge eine kleinste R-abgeschlossene Menge gibt, können wir diese als die *induktiv durch R definierte Menge* festlegen.

Definition 4.6 (Induktiv definierte Menge)
Sei R eine Regelmenge über X. Wir nennen die (bzgl. $\subseteq$) kleinste unter R abgeschlossene Menge die *durch R induktiv definierte Menge*. Wir bezeichnen diese Menge mit I_R.

Oft liest man bei induktiven Definitionen den Zusatz „nichts sonst ist in der Menge“. Das ist gemäß der obigen Definition – und dem in der Mathematik üblichen Verständnis von induktiven Definitionen – überflüssig (oder sogar unsinnig). Denn wenn man eine Menge induktive definiert, dann ist die kleinste R-abgeschlossene Menge gemeint; und die enthält keine „überflüssigen“ Elemente.

Beispiel 4.4 (Induktive Definitionen)

1. In Kapitel 3 haben wir bereits einige Beispiele für induktive Definitionen kennen gelernt. Allerdings haben wir dort die Menge X nicht explizit benannt und die Regeln mehr oder weniger explizit angegeben.

   Zur Übung können Sie sich ja mal überlegen, wie die Menge X und die zugehörigen Regelinstanzen aussehen.

2. Sei A eine beliebige Menge und $\rightarrow$ eine binäre Relation über A. Wir definieren nun die folgende Regelmenge über $A \times A$:

$$\begin{aligned} R = \quad & \{(\emptyset, (a,a)) \mid a \in A\} \cup \\ & \{(\emptyset, (a,b)) \mid a \rightarrow b\} \cup \\ & \{(\{(a,b),(b,c)\}, (a,c)) \mid a,b,c \in A\} \end{aligned}$$

   Dann bezeichnet die durch diese Regeln induktiv definierte Menge gerade die reflexiv-transitive Hülle von $\rightarrow$, d. h. $I_R = \rightarrow^*$.

Die Regelinstanzen der ersten Zeile drücken die Reflexivität aus. Die Regelinstanzen der zweiten Zeile drücken aus, daß jeder Übergang von $\rightarrow$ auch zu I_R gehört. Die Regelinstanzen der dritten Zeile drücken die Transitivität aus.

Da I_R die kleinste R-abgeschlossene Menge ist, werden zu I_R gerade die für die reflexiv-transitive Hülle nötigen Übergänge hinzugenommen.

Die Definition 4.6 definiert uns zwar eindeutig die Menge I_R. Sie liefert uns aber kein Verfahren, um an die Elemente dieser Menge heranzukommen. Wir werden nun eine weitere Charakterisierung von I_R angeben, die es uns erlaubt, die Elemente von I_R systematisch zu generieren. Die Idee ist recht einfach: Wir beginnen mit der leeren Menge und nehmen schrittweise die Elemente dazu, die man mit Hilfe der Regeln aus den bisher abgeleiteten Elemente ableiten kann. Im ersten Schritt sind das nur die Folgerungen der Axiome, da die ja keine Voraussetzungen benötigen. Im zweiten Schritt können wir dann schon mehr ableiten. Natürlich kann es sein, daß dieser Iterationsprozeß nie endet. Aber im Laufe des Interationsprozesses kommen nach und nach alle Elemente von I_R dazu.
Für eine Regelmenge R über X sieht diese Iteration wie folgt aus:

$$\begin{array}{lcll} Q_0 & = & \emptyset & \\ Q_1 & = & \{x \in X \mid (\emptyset, x) \in R\} & = \widehat{R}(Q_0) \\ Q_2 & = & \{x \in X \mid (Y, x) \in R, Y \subseteq Q_1\} & = \widehat{R}(Q_1) \\ Q_3 & = & \{x \in X \mid (Y, x) \in R, Y \subseteq Q_2\} & = \widehat{R}(Q_2) \\ \vdots & & & \end{array}$$

Die Menge I_R ergibt sich dann als Vereinigung aller Q_i, d. h. $I_R = \bigcup_{i \in \mathbb{N}} Q_i$. Dabei definiert die Operation $\widehat{R}$ genau einen Ableitungsschritt: $\widehat{R}(Q)$ ist diejenige Menge von Elementen, die man in einem Schritt aus Q ableiten kann.

Definition 4.7 (Ableitungsschritt $\widehat{R}$)
Sei R eine Menge von Regeln über X. Die Abbildung $\widehat{R} : 2^X \rightarrow 2^X$ ist wie folgt definiert:

$$\widehat{R}(Q) = \{x \in X \mid \exists Y \subseteq Q.(Y, x) \in R\}$$

Die Elemente von $\widehat{R}(Q)$ heißen *die in einem Schritt mit R aus Q ableitbaren Elemente*.

Mit Hilfe des $\widehat{R}$-Operators können wir jetzt noch einfacher formulieren, wann eine Menge Q unter R abgeschlossen ist, nämlich genau dann, wenn $\widehat{R}(Q) \subseteq Q$ gilt.

Wir können nun unsere obigen Überlegungen als Satz formulieren:

Satz 4.8
Sei R eine Regelmenge über X und sei die Folge von Teilmengen $Q_0, Q_1, Q_2, \ldots$ wie folgt definiert:

- $Q_0 = \emptyset$
- $Q_{i+1} = \widehat{R}(Q_i)$ für $i \in \mathbb{N}$

Dann gilt $I_R = \bigcup_{i \in \mathbb{N}} Q_i$ und I_R ist ein Fixpunkt von $\widehat{R}$, d. h. $\widehat{R}(I_R) = I_R$.

Beweis: Ausführlich werden wir diesen Satz in den Übungen beweisen. Hier sind die wesentlichen Schritte des Beweises:

1. Der Operator $\widehat{R}$ ist monoton (steigend), d. h. für alle Mengen Q und Q' mit $Q \subseteq Q'$ gilt $\widehat{R}(Q) \subseteq \widehat{R}(Q')$.
2. Die Folge $Q_0, Q_1, Q_2, \ldots$ bildet eine aufsteigende Kette bezüglich $\subseteq$, d. h. für jedes $i \in \mathbb{N}$ gilt $Q_i \subseteq Q_{i+1}$.
3. Die Menge $Q = \bigcup_{i \in \mathbb{N}} Q_i$ ist $\widehat{R}$-abgeschlossen.
4. Für jedes Q_i und jede R-abgeschlossene Menge Q' gilt $Q_i \subseteq Q'$.
5. Q ist die kleinste unter R abgeschlossene Menge.
6. I_R ist Fixpunkt von $\widehat{R}$.

□

Aus der Definition von I_R wissen wir, daß I_R bezüglich Mengeninklusion kleiner ist als jede R-abgeschlossene Menge Q (d. h. als jede Menge mit $\widehat{R}(Q) \subseteq Q$. Insbesondere ist I_R kleiner als jeder Fixpunkt Q von $\widehat{R}$ (d. h. als jede Menge Q mit $\widehat{R}(Q) = Q$). Das heißt, daß I_R der (bezüglich Mengeninklusion) kleinste Fixpunkt von $\widehat{R}$ ist. Wir haben damit also ganz nebenbei gezeigt, daß $\widehat{R}$ immer einen kleinsten Fixpunkt besitzt.

Tatsächlich ist der obige Satz bereits der Fixpunktsatz von Kleene (oder eine speziellen Ausprägung davon). Wir werden diesen Satz später beweisen. Der Beweis des Fixpunktsatzes von Kleene folgt exakt dem gleichen Muster.

Auch wenn der Beweis des Satzes insgesamt recht elementar ist, ist der Satz nicht ganz trivial. Denn wenn wir Regelinstanzen mit unendlich vielen Voraussetzungen zulassen würden, dann würde der Satz in dieser Form nicht gelten. Wer findet ein Gegenbeispiel?

3 Regelinduktion

Im vorangegangen Abschnitt haben wir gesehen, wie man Mengen induktiv definieren kann. Die Frage ist nun, wie man Eigenschaften der Elemente einer induktiv definierten Menge beweisen kann. Dies geht ganz analog zur Vollständigen Induktion. Wir müssen die Eigenschaft für jedes Element beweisen, das aufgrund eines Axioms in die Menge aufgenommen wird. Außerdem müssen wir beweisen, daß für jede Regel die Eigenschaft für die Folgerung (d. h. die rechte Seite der Regel) gilt, wenn die Eigenschaft für alle Voraussetzungen (d. h. alle Elemente auf der linken Seite der Regel) gilt. Dieses Prinzip wird *Induktion über die Regeln* oder kurz *Regelinduktion* genannt.

Wie bei der Noetherschen Induktion können wir den Induktionsanfang im Induktionsschritt „verstecken“, da die Axiome spezielle Regeln ohne Voraussetzung sind.

Prinzip 4.9 (Regelinduktion)
Sei R eine Menge von Regeln über X und P ein Prädikat über X. Wenn für jede Regel $(Y, x) \in R$, für die für jedes $y \in Y$ das Prädikat $P(y)$ gilt, auch das Prädikat $P(x)$ gilt, dann gilt das Prädikat $P(z)$ für jedes $z \in I_R$, d. h. für jedes Element der durch R induktiv definieren Menge.

Wir können das Prinzip der Regelinduktion auch kurz wie folgt formulieren:

$$(\forall (Y, x) \in R.((\forall y \in Y.P(y)) \Rightarrow P(x))) \Rightarrow \forall z \in I_R.P(z)$$

Eine weitere Formulierung ist die folgende:

$$(\forall (Y, x) \in R.(Y \subseteq P \Rightarrow x \in P)) \Rightarrow I_R \subseteq P$$

Beweis: Das Prinzip der Regelinduktion können wir mit Hilfe von Satz 4.8 auf das Prinzip der vollständigen Induktion zurückführen: Sei also R eine Regelmenge, für die für jede Regel $(Y, x) \in R$ mit $Y \subseteq P$ auch $x \in P$ gilt.

1. Aus der Definition des $\widehat{R}$-Operators folgt unmittelbar, daß dann für jede Teilmenge $Q \subseteq P$ auch gilt $\widehat{R}(Q) \subseteq P$.

2. Gemäß Satz 4.8 läßt sich die Menge I_R wie folgt durch die Folge von Mengen $Q_0, Q_1, \ldots$ mit

   - $Q_0 = \emptyset$
   - $Q_{i+1} = \widehat{R}(Q_i)$ für $i \in \mathbb{N}$

   charakterisieren: $I_R = \bigcup_{i \in \mathbb{N}} Q_i$.

3. Offensichtlich gilt $Q_0 = \emptyset \subseteq P$. Durch vollständige Induktion können wir nun unter Anwendung von 1. zeigen, daß für jedes $i \in \mathbb{N}$ gilt $Q_i \subseteq P$. Da jedes einzelne Q_i in P enthalten ist gilt dann auch $(\bigcup_{i \in \mathbb{N}} Q_i) \subseteq P$; also gilt $I_R \subseteq P$.

□

Das Prinzip der Regelinduktion können wir nun anwenden, um Eigenschaften der Elemente einer induktiv definierten Menge zu beweisen. Indirekt zeigen wir auf diese Weise auch, daß bestimmte Elemente nicht in der induktiv definierten Menge vorkommen: nämlich genau die Elemente, die die bewiesene Eigenschaft nicht besitzen. Dazu betrachten wir ein Beispiel.

Beispiel 4.5
Im Beispiel 3.5 in Kapitel 3 auf Seite 36 haben wir bereits informell argumentiert, daß es für die Anweisung $w \equiv$ **while** true **do skip** keine Zustände $\sigma, \sigma' \in \Sigma$ gibt, für die sich $\langle w, \sigma \rangle \to \sigma'$ ableiten läßt. Wir werden dies nun mit Hilfe der Regelinduktion beweisen. Dazu müssen wir uns zunächst ein Prädikat überlegen, das wir mit Hilfe der Regelinduktion beweisen können:

$$P(\langle c, \sigma \rangle \to \sigma') = c \not\equiv w$$

d. h. wir zeigen, daß für jeden Tripel $\langle c, \sigma \rangle \to \sigma'$, den wir aus den Regeln herleiten können, die Anweisung c definitiv nicht unsere Endlosschleife w ist. Wir beweisen die Gültigkeit des Prädikats nun für alle gemäß der Regeln herleitbare Tripel $\langle c, \sigma \rangle \to \sigma'$ durch Induktion über die Regeln:

$$\frac{}{\langle \textbf{skip}, \sigma \rangle \to \sigma}$$

Offensichtlich gilt **skip** $\not\equiv w$.

$$\frac{\langle a, \sigma \rangle \to n}{\langle v{:=}a, \sigma \rangle \to \sigma[n/v]}$$

Offensichtlich gilt v:= a $\not\equiv w$.

...

für alle Regeln bis auf die Regeln für die Schleife gilt die Aussage analog. Wir müssen also nur noch die Regeln für die Schleife w betrachten.

$$\frac{\langle \text{true}, \sigma\rangle \to \mathit{false}}{\langle \textbf{while } \text{true } \textbf{do skip } c, \sigma\rangle \to \sigma}$$

Für diese Regel ist die Voraussetzung $\langle \text{true}, \sigma\rangle \to \mathit{false}$ verletzt. Es ist also nichts zu zeigen.

$$\frac{\langle b, \sigma\rangle \to \mathit{true} \quad \langle \textbf{skip}, \sigma\rangle \to \sigma'' \quad \langle \textbf{while } \text{true } \textbf{do skip}, \sigma''\rangle \to \sigma'}{\langle \textbf{while } \text{true } \textbf{do skip}, \sigma\rangle \to \sigma'}$$

Da für die Voraussetzung $\langle \textbf{while } \text{true } \textbf{do skip}, \sigma''\rangle \to \sigma'$ das Prädikat nicht erfüllt ist, müssen wir für diese Regel nichts zeigen.

> *Hier stellen wir das informelle Argument, daß die Konstruktion einer Herleitung für $\langle \textbf{\textit{while}}\ \textit{true}\ \textbf{\textit{do skip}}, \sigma''\rangle \to \sigma'$ niemals terminieren würde, vom Kopf auf die Füsse: Wir beweisen den Induktionsschritt für diese Regel, indem wir die Ungültigkeit der Induktionsvoraussetzung für diese Regel zeigen. Das ist sicher etwas ungewöhnlich, aber es ist korrekt.*

4 Herleitungen

Bei der Definition des Begriffs der induktiv durch eine Regelmenge definierten Menge haben wir zur Motivation informell den Begriff der Ableitbarkeit und den Begriff der*Herleitung* benutzt. Insbesondere ist die alternative Charakterisierung der induktiven Mengen in Satz 4.8 durch die schrittweise Ableitbarkeit der Element motiviert.
Jetzt sind wir dazu in der Lage, diesen Begriff formal zu definieren – und zwar durch eine induktive Definition. Wir ziehen uns also fast an den eigenen Haaren aus dem Sumpf. Da wir den Begriff der Herleitung bei der formalen Definition der induktiv definierten Menge nicht benutzt haben, ist unser Vorgehen aber formal sauber.
Formal ist eine Herleitung ein Baum, an dessen Wurzel das hergeleitete Element steht. Die Verzweigungen im Baum entsprechen dabei den Regeln. Um eine aufwendige graphische Notation zu vermeiden, definieren wir eine Herleitung technisch als ein Paar $(\{d_1, \ldots, d_n\}, x)$, wobei $d_1, \ldots, d_n$ Teilherleitungen sind und x das hergeleitete Element. Um den Aspekt der Regelanwendung besser zum Ausdruck zu bringen benutzen wir anstelle des Kommas

den Schrägstrich: $(\{d_1, \ldots d_n\}/x)$. Wenn d eine Herleitung[2] für x ist, schreiben wir $d \vdash_R x$ (gesprochen „d leitet x her“). Dabei lassen wir den Index R meist weg, wenn R aus dem Kontext hervor geht.

Definition 4.10 (Herleitung)
Sei R eine Regelmenge über X. Wir definieren die Relation $\vdash_R$ induktiv durch die folgenden Regeln R':

- Für jedes Axiom $(\emptyset, x) \in R$ ist

$$\frac{}{(\emptyset/x) \vdash_R x}$$

  eine Regel aus R'.

- Für jede Regel $(\{x_1, \ldots, x_n\}, x) \in R$ ist

$$\frac{d_1 \vdash_R x_1 \quad \ldots \quad d_n \vdash_R x_n}{(\{d_1, \ldots, d_n\}/x) \vdash_R x}$$

  eine Regel aus R'.

Wenn $d \vdash_R x$ in der durch R' induktiv definierten Menge liegt, sagen wir, daß d eine *Herleitung* für x ist.

Durch diese Regeln werden die Herleitungsbäume in Form von „Klammergebirgen“ codiert. Für die Definition der Herleitung ist dies praktisch. Wenn wir aber über Herleitungen reden wollen, ist dies eher unpraktisch. Dann benutzen wir die Notation wie wir sie in Kapitel 3 in Abschnitt 3 benutzt haben (z. B. in Beispiel 3.4).
Wenn unsere Definition der induktiven Mengen und der Herleitung vernünftig sind, sollte nun gelten, daß die Elemente der durch die Regeln induktiv definierten Menge genau die Elemente sind, für die eine Herleitung existiert. Formal formulieren wir das wie folgt:

Lemma 4.11 (Induktive definierte Menge und Herleitung)
Sei R eine Regelmenge. Dann gilt $x \in I_R$ genau dann, wenn ein d mit $d \vdash_R x$ existiert.

[2]Im Englischen heißt Herleitung *derivation*. Deshalb bezeichnen wir Herleitungen im folgenden mit dem Zeichen d.

Beweis: Regelinduktion. Ein genauer Beweis wird in der Übung besprochen.

Fragen: Über welche Regeln geht die Regelinduktion? Wie genau ist das Prädikat formuliert, für das wir die Regelinduktion anwenden?

□

Wenn es eine Herleitung d für ein Element x gibt, schreiben wir auch $\vdash_R x$, bzw. wenn R aus dem Kontext hervorgeht auch $\vdash x$. Die Aussagen $x \in I_R$ und $\vdash_R x$ sind dann gleichbedeutend. In der Literatur wird meist $\vdash_R x$ bzw. $\vdash x$ verwendet.
Das vorangegangene Lemma besagt nur, daß es für jedes Element einer induktiv definierten Menge mind. eine Herleitung gibt. Es kann jedoch sein, daß es für manche Elemente mehrere verschiedenen Herleitungen gibt. In der Praxis versucht man aber meist, induktive Definitionen so zu formulieren, daß es eine eindeutige Herleitung für jedes Element gibt. Um das zu formalisieren, formulieren wir nun den Begriff der *eindeutigen induktiven Definition.*

Definition 4.12 (Eindeutige induktive Definition)
Die durch eine Regelmenge R induktive definierte Menge heißt eindeutig induktiv definiert, wenn für jedes $x \in I_R$ genau eine Herleitung d mit $d \vdash_R x$ existiert.

Zur Übung sollte Sie sich einmal überlegen, welche der Regelmengen aus Kapitel 3 eindeutige induktive Definitionen sind und welche nicht. Besonders interessant sind die Regeln für das Auswerten der booleschen Ausdrücke.

Oft werden induktive Definitionen nur dann induktiv genannt, wenn sie eindeutig sind. Insbesondere bei der Definition von syntaktischen Mengen legt man Wert auf die Eindeutigkeit der Definition (vgl. Diskussion zur abstrakten Syntax in Kapitel 3 in Abschnitt 1.2). Um den Begriff der eindeutigen induktiven Definition zu bilden, ist es aber zweckmäßig zunächst den Begriff der induktiven Definition zu bilden, und dann die eindeutigen als Spezialfall zu charakterisieren.
Wenn eine induktive Definition eindeutig ist, kann man (totale) Abbildungen von I_R in irgendeine Menge Y *induktiv über den Aufbau der Menge* I_R definieren. Dazu betrachten wir einige Beispiele von Abbildungen, die wir später noch mehrfach benutzen werden.

Beispiel 4.6 (Definitionen induktiv über den Aufbau einer Menge)

1. Für die Menge der arithmetischen Ausdrücke *Aexp* definieren wir die Länge induktiv über den Aufbau: $\mathit{length} : \mathit{Aexp} \to \mathbb{N}$ ist definiert durch:

- $length(n) = 1$
- $length(v) = 1$
- $length(a_0 + a_1) = length(a_0) + length(a_0) + 1$
- $length(a_0 - a_1) = length(a_0) + length(a_0) + 1$
- $length(a_0 * a_1) = length(a_0) + length(a_0) + 1$

Formal könnte man die Abbildung durch die folgenden Regeln definieren:

$$\frac{}{(n,1)} \qquad \frac{}{(v,1)}$$

$$\frac{(a_0,n_0) \quad (a_1,n_1)}{(a_0{+}a_1, n_0+n_1+1)} \qquad \frac{(a_0,n_0) \quad (a_1,n_1)}{(a_0{-}a_1, n_0+n_1+1)}$$

$$\frac{(a_0,n_0) \quad (a_1,n_1)}{(a_0{*}a_1, n_0+n_1+1)}$$

Die dadurch definierte Relation $length \subseteq Aexp \times \mathbb{N}$ ist eine totale Abbildung, da die Definition der arithmetischen eindeutig ist (dies müßte man aber eigentlich beweisen).

2. Die Abbildung $assign : Com \to 2^{\mathbb{V}}$, die jeder Anweisung die Menge derjenigen Variablen zuordnet, an die ein Wert zugewiesen wird, ist induktiv definiert durch:

   - $assign(\textbf{skip}) = \emptyset$
   - $assign(v{:=}\ a) = \{v\}$
   - $assign(c_0;\ c_1) = assign(c_0) \cup assign(c_1)$
   - $assign(\textbf{if}\ b\ \textbf{then}\ c_0\ \textbf{else}\ c_1) = assign(c_0) \cup assign(c_1)$
   - $assign(\textbf{while}\ b\ \textbf{do}\ c) = assign(c)$

   Wir verzichten hier darauf, das Prinzip der Definition einer totalen Abbildung induktiv über den Aufbau der Menge zu formalisieren. Das erste Beispiel sollte einen guten Eindruck davon geben, wie das geht. Die Formalisierung und der Beweis, daß die so definierte Relation für jede eindeutig induktiv definierte Menge eine totale Abbildung ist, ist eine einfache Übungsaufgabe.

Weitere Beispiele für Definitionen induktiv über den Aufbau ist die Auswertung der arithmetischen Ausdrücke und der booleschen Ausdrücke. Die Semantik der Anweisungen dagegen ist *keine* Definition induktiv über den Aufbau! Warum wohl?

5 Zusammenfassung

In diesem Kapitel haben wir die Konzepte der induktiven Definition und des induktiven Beweisens formalisiert, die wir in Kapitel 3 benutzt haben, um die operationale Semantik der Programmiersprache IMP zu definieren. Methodisch hätten wir diese Definitionen vor der Definition der operationalen Semantik einführen müssen.
Aus didaktischen Gründen haben wir die Konzepte erst nach Ihrer Anwendung eingeführt. Generell stellt sich die Frage, ob wir (im Rahmen der Vorlesung Semantik) diese Konzepte formalisieren sollten, oder ob wir diese Konzepte als gemeinsame Pragmatik voraussetzen. Der Hauptgrund, diese Konzepte hier zu formalisieren, ist, daß auf dieser Ebene später deutlich wird, daß die mathematische und die operationale Ebene weit weniger unterschiedlich sind, als man zunächst erwarten würde. Ein weiterer Grund ist, ein Bewußtsein dafür zu schaffen, daß in der Informatik fast überall nur mit Wasser gekocht wird, wobei das Wasser die Konzepte des induktiven Definierens und Beweisens sind.