Übungen zu Formale Methoden I – 5. Blatt

Christian Sternagel
christian.sternagel@uibk.ac.at

15. November 2005

1 Der Induktionsbeweis

1.1 Aussagenlogische Grundlagen

1.1.1 Modus Ponens

Beim *Modus Ponens* (manchmal auch *Implikations Elimination* genannt) handelt es sich um eine Form des logischen Schließens. Sei eine Implikation $A \Rightarrow B$ gegeben. Wenn man nun weiß, dass A gilt, dann kann man mit Hilfe des *Modus Ponens* sofort auf B schließen. Diese Situation kann wie folgt ausgedrückt werden:

$$\text{Aus } A = \texttt{true} \text{ und } A \Rightarrow B \text{ folgt } B.$$

Also in Worten: "Wenn A wahr ist und 'A impliziert B' gilt, dann folgt daraus, dass B wahr ist."

Das kann für $A = \texttt{true}$ symbolisch sehr einfach gezeigt werden:

$$\begin{aligned} A \Rightarrow B &\equiv \texttt{true} \Rightarrow B \\ &\equiv \neg\texttt{true} \vee B \\ &\equiv \texttt{false} \vee B \\ &\equiv B \end{aligned}$$

1.1.2 Induktion über die natürlichen Zahlen

Das Beweisprinzip des *Induktionsbeweises* kann aussagenlogisch begründet werden. Im einfachsten Fall (dem einzigen der hier betrachtet wird) wird ein Induktionsbeweis geführt um mathematische Eigenschaften zu zeigen, die von den natürlichen Zahlen abhängen.

Sei nun A_n eine Aussage der Form: "Die Eigenschaft A gilt für die natürliche Zahl $n \in \mathbb{N}$." (z.B. bedeutet A_5: "Die Eigenschaft A gilt für 5.").

Man nehme an die folgenden beiden Dinge über die Eigenschaft A seien bekannt:

1. **Induktionsanfang:** Die natürliche Zahl 1 hat die Eigenschaft A, d.h. es gibt einen Beweis für A_1.

2. **Induktionsschluss:** Wenn n eine natürliche Zahl ist, von der man annimmt, dass A_n gilt, dann kann man zeigen dass für $n+1$ die Eigenschaft A_{n+1} gilt; d.h. es gibt einen Beweis für $A_n \Rightarrow A_{n+1}$.

DEFINITION 1.1. Das Prinzip der mathematischen Induktion besagt, dass auf Grund dieser beiden Information, für *jede* natürliche Zahl n die Eigenschaf A_n gilt. Die Annahme von A_n beim Induktionsschluss (der selbst oft Induktionsschritt genannt wird) wird *Induktionshypothese* oder *Induktionsannahme* genannt.

1.1.3 Warum macht das Induktionsprinzip Sinn?

Man nehme eine *beliebige* natürliche Zahl k. Wenn k gleich 1 ist, dann gilt für k die Eigenschaft A_1 auf Grund des Induktionsanfangs.

Andernfalls kann man den Induktionsschluss mit $n = 1$ verwenden um zu zeigen, dass für $2 = 1+1$ die Eigenschaft A_2 gilt. In diesem Schritt verwenden wir den *Modus Ponens* mit der Implikation $A_1 \Rightarrow A_2$ und der Tatsache, dass A_1 gilt. Nun verwendet man den Induktionsschluss ein weiteres mal um zu zeigen, dass für 3 die Eigenschaft A_3 gilt usw. Man wiederholt diesen Schritt bis man $n = k$ erreicht.

Nachdem k beliebig gewählt wurde gilt A_k somit für alle $k \in \mathbb{N}$.

Damit wurde gezeigt, dass es ausreicht den Induktionsanfang und den Induktionsschluss für eine Eigenschaft A zu zeigen, um damit gleichzeitig einen Beweis dafür zu geben, dass A für alle natürlichen Zahlen n gilt, die größer sind als die beim Induktionsanfang gewählte Zahl (meist 0 oder 1).

2 Zu Aufgabe 24

DEFINITION 2.1. Der *Gray-Code* der Länge n ist eine Aufzählung von $\{0,1\}^n$, die induktiv durch

$$\begin{aligned} \alpha_0 : \{1\} &\to \{\epsilon\}, \\ 1 &\mapsto \epsilon, \end{aligned}$$

und, für $n \geq 1$, durch

$$\begin{aligned} \alpha_n : \{1, \ldots, 2^n\} &\to \{0,1\}^n, \\ i &\mapsto \begin{cases} 0\alpha_{n-1}(i) & \text{falls } i \leq 2^{n-1} \\ 1\alpha_{n-1}(2^n + 1 - i) & \text{falls } i > 2^{n-1}, \end{cases} \end{aligned}$$

definiert wird.

LEMMA 2.2 $(*)$. *Aufeinanderfolgende Codewörter sowie letztes und erstes Codewort des* Gray-Codes *unterscheiden sich an* genau einer *Stelle.*

Beweis. Nun beweist man die Eigenschaft $(*)$ durch Induktion:

1. **Induktionsanfang:** $(n = 1)$. α_1 ist wie folgt definiert:

$$\begin{aligned}\alpha_1 : \{1,2\} &\to \{0,1\},\\ 1 &\mapsto 0\alpha_0(1) = 0\epsilon = 0\\ 2 &\mapsto 1\alpha_0(1) = 1\epsilon = 1\end{aligned}$$

   Die einzigen beiden Codewörter sind also 0 und 1. Man sieht sofort, dass diese Codewörter sich an *genau* einer Stelle unterscheiden (da es nur eine Stelle gibt und diese bei beiden aus einem anderen Zeichen besteht) und dass letztes (1) und erstes (0) Codewort sich an *genau* einer Stelle unterscheiden. Also gilt $(*)_1$.

2. **Induktionsschluss:** $(n \to n+1)$. Man nehme nun an, dass $(*)_n$ gelte (also, dass für α_n aufeinanderfolgende Codewörter sowie letztes und erstes Codewort sich an genau einer Stelle unterscheiden).

   α_{n+1} ist wie folgt definiert:

$$\begin{aligned}\alpha_{n+1} : \{1,2,\ldots,2^{n+1}\} &\to \{0,1\}^{n+1},\\ 1 &\mapsto 0\alpha_n(1)\\ &\vdots\\ 2^n &\mapsto 0\alpha_n(2^n)\\ 2^n+1 &\mapsto 1\alpha_n(2^{n+1}+1-(2^n+1)) = 1\alpha_n(2^n)\\ &\vdots\\ 2^{n+1} &\mapsto 1\alpha_n(2^{n+1}+1-2^{n+1}) = 1\alpha_n(1)\end{aligned}$$

   Man betrachte nun vier getrennte Fälle um $(*)_n \Rightarrow (*)_{n+1}$ zu zeigen:

   (a) Sei $i \leq 2^n$. Man sieht das *alle* Codewörter von α_{n+1} in diesem Bereich, nämlich

$$0\alpha_n(1), 0\alpha_n(2), \ldots, 0\alpha_n(2^n-1), 0\alpha_n(2^n),$$

   aus dem Zeichen 0 gefolgt von den Codewörtern von α_n bestehen. Da laut Annahme alle Codewörter von α_n die Eigenschaft $(*)$ haben, d.h. $(*)_n$ gilt, folgt dass alle Codewörter von α_{n+1} in diesem Bereich auch $(*)$ erfüllen. Es gilt also $(*)_{n+1}$ für alle Codewörter $\alpha_{n+1}(i)$ mit $i \leq 2^n$.

(b) Sei $i > 2^n$. In diesem Bereich liegen folgende Codewörter

$$1\alpha_n(2^n), 1\alpha_n(2^n - 1), \ldots, 1\alpha_n(2), 1\alpha_n(1).$$

Analog zu 2a folgt dann dass $(*)_{n+1}$ für alle Codewörter $\alpha_{n+1}(i)$ mit $i > 2^n$ gilt.

(c) Es muss noch gezeigt werden, dass $(*)$ auch im Übergangsbereich $i = 2^n$ und $i = 2^n + 1$ gilt. Wegen

$$\begin{aligned}\alpha_n(2^{n+1} + 1 - (2^n + 1)) &= \alpha_n(2 \cdot 2^n + 1 - 2^n - 1) \\ &= \alpha_n(2^n)\end{aligned}$$

folgt:

$$\begin{aligned}\alpha_{n+1}(2^n) &= 0\alpha_n(2^n) \\ \alpha_{n+1}(2^n + 1) &= 1\alpha_n(2^{n+1} + 1 - (2^n + 1)) \\ &= 1\alpha_n(2^n)\end{aligned}$$

Man sieht sofort, dass sich diese beiden Codewörter nur im ersten Zeichen unterscheiden (und damit an genau einer Stelle).

(d) Es bleibt zu zeigen, dass letztes und erstes Codewort von α_{n+1} sich an genau einer Stelle unterscheiden, d.h. dass $\alpha_{n+1}(1)$ und $\alpha_{n+1}(2^{n+1})$ sich an genau einer Stelle unterscheiden. Dann folgt:

$$\begin{aligned}\alpha_{n+1}(1) &= 0\alpha_n(1) \\ \alpha_{n+1}(2^{n+1}) &= 1\alpha_n(2^{n+1} + 1 - 2^{n+1}) \\ &= 1\alpha_n(1)\end{aligned}$$

Was zu beweisen war.

Aus 2a bis 2d folgt dass unter der Vorraussetzung dass $(*)$ für α_n gilt, $(*)$ auch für α_{n+1} gilt. d.h.:

$$(*)_n \Rightarrow (*)_{n+1}$$

□