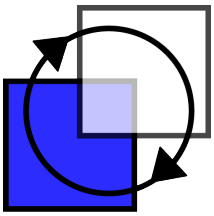
CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

Prof. Bernd Finkbeiner, Ph.D.
Jana Hofmann, M.Sc.
Reactive Systems Group



Programmierung 1 (WS 2020/21)
Zusatzerklärung zum Thema
Verstärkung

Im Folgenden möchten wir uns etwas genauer mit der Verstärkung von Korrektheitsaussagen beschäftigen. Betrachten wir dazu zunächst das folgende Beispiel:

In den ersten Kapiteln haben wir gelernt, wie man die Potenz x^n endrekursiv berechnet:

$$\begin{aligned} &\mathit{powi} : \mathbb{N} \times \mathbb{N} \times \mathbb{N} \to \mathbb{N} \\ &\mathit{powi}\,(x, 0, a) = a \\ &\mathit{powi}\,(x, n, a) = \mathit{powi}\,(x, n-1, a \cdot x) \qquad \text{für } n > 0 \end{aligned}$$

Nun sind wir in der Lage, die Korrektheit dieses Verfahrens zu beweisen. Die Aussage, die wir hierfür zeigen wollen, lautet $\forall x \in \mathbb{N} : \forall n \in \mathbb{N} : \mathit{powi}(x, n, 1) = x^n$.

Beweis. Sei $x \in \mathbb{N}$ beliebig. Wir zeigen

$$\forall n \in \mathbb{N} : \mathit{powi}\,(x, n, 1) = x^n$$

durch Induktion über $n \in \mathbb{N}$.

Wir unterscheiden zwei Fälle:

- Sei $n = 0$. Dann

  $$\begin{aligned} \mathit{powi}\,(x, 0, 1) &= 1 && \text{Definition } \mathit{powi} \\ &= x^0 && \text{Arithmetik} \end{aligned}$$

- Sei $n > 0$.

  Induktionsannahme: Für alle $m < n$ gilt, dass $\mathit{powi}\,(x, m, 1) = x^m$.

  Dann

  $$\begin{aligned} \mathit{powi}\,(x, n, 1) &= \mathit{powi}\,(x, n, 1 \cdot x) && \text{Definition } \mathit{powi} \\ &= \mathit{powi}\,(x, n, x) \\ &\lightning \end{aligned}$$

Hier stecken wir im Beweis leider fest. Unsere Induktionsannahme trifft nur eine Aussage über *powi*, wenn der Akku gerade den Wert 1 hat. Bei der Anwendung von *powi* ändert sich jedoch der Akku zu x. Wir dürfen unsere Induktionsannahme folglich nicht anwenden. Machen Sie sich klar, dass auch das Vertauschen der Quantoren von x und n hier nicht helfen würde.

Ein Lösungsansatz für dieses Problem ist, nach einer allgemeineren Aussage zu suchen, aus der dann die Aussage, die wir eigentlich zeigen wollten, folgt. Hierbei spricht man davon, die Aussage zu *verstärken*. Um eine passende Verstärkung zu finden, müssen wir uns überlegen, wie die Prozedur *powi* vorgeht. Aus den definierenden Gleichungen lässt sich ablesen, dass der Akku vor einem rekursiven Aufruf verändert wird. Das deutet darauf hin,

dass wir unsere Aussage nicht für einen fixen Wert (hier 1) im Akku beweisen wollen, sondern für einen beliebigen Wert. Wir überlegen uns also, was die Prozedur *powi* berechnet, wenn wir sie mit einer beliebigen Zahl im Akku aufrufen, sprich $powi\,(x, n, a)$. In diesem Fall liefert *powi* gerade x^n multipliziert mit dem initialen Wert a des Akkus. Entsprechend versuchen wir die allgemeinere Aussge $\forall x \in \mathbb{N} : \forall n \in \mathbb{N} : \forall a \in \mathbb{N} : powi\,(x, n, a) = x^n \cdot a$ zu beweisen. Durch Verwendung eines Allquantors weisen wir hier explizit darauf hin, dass alle möglichen natürlichen Zahlen für a berücksichtigt werden.

Lemma 1. $\forall x \in \mathbb{N} : \forall n \in \mathbb{N} : \forall a \in \mathbb{N} : \mathit{powi}\,(x, n, a) = x^n \cdot a$

Beweis. Sei $x \in \mathbb{N}$ beliebig. Wir zeigen

$$\forall n \in \mathbb{N} : \forall a \in \mathbb{N} : \mathit{powi}\,(x, n, a) = x^n \cdot a$$

durch Induktion über $n \in \mathbb{N}$.

Wir unterscheiden zwei Fälle:

- Sei $n = 0$. Sei $a \in \mathbb{N}$ beliebig. Dann

$$\begin{aligned} \mathit{powi}\,(x, 0, a) &= a && \text{Definition } \mathit{powi} \\ &= x^0 \cdot a && \text{Arithmetik} \end{aligned}$$

- Sei $n > 0$. Sei $a \in \mathbb{N}$ beliebig.

  Induktionsannahme: Für alle $m < n$ gilt, dass $\forall a' \in \mathbb{N} : \mathit{powi}\,(x, m, a') = x^m \cdot a'$.

  Dann

$$\begin{aligned} \mathit{powi}\,(x, n, a) &= \mathit{powi}\,(x, n-1, a \cdot x) && \text{Definition } \mathit{powi} \\ &= x^{n-1} \cdot (a \cdot x) && \text{Induktion für } m = n-1 \text{ und } a' = a \cdot x \\ &= x^n \cdot a && \text{Arithmetik} \end{aligned}$$

■

Betrachten wir den obigen Beweis noch einmal genauer: Im Fall $n > 0$ lautete unsere Induktionannahme vor der Verstärkung $\mathit{powi}(x, m, 1) = x^m$ für alle $m < n$. Da wir bei der verstärkten Aussage eine Aussage über alle initialen Werte a des Akkus treffen, lautet unsere neue Induktionsannahme $\forall a \in \mathbb{N} : \mathit{powi}\,(x, n, a) = x^n \cdot a$. Wir dürfen also eine beliebige Zahl für a wählen, wenn wir die Annahme verwenden wollen. Hierbei war es wichtig, dass wir das a nach dem n quantifiziert haben, da sonst das „$\forall a \in \mathbb{N}$" nicht Teil der Induktionsannahme wäre.

Die Aussage $\mathit{powi}\,(x, n, 1) = x^n$ folgt dann aus unserer bewiesenen verstärkten Aussage mittels elementarer Mathematik, wenn wir für a die Zahl 1 wählen.

Korollar 1. $\mathit{powi}\,(x, n, 1) = x^n$

Beweis.

$$\begin{aligned} \mathit{powi}\,(x, n, 1) &= x^n \cdot 1 && \text{Lemma 1} \\ &= x^n && \text{Arithmetik} \end{aligned}$$

■

Aufgabe 1
Deklarieren Sie *endrekursive* Prozeduren fac', length', rev', sodass fac' die Fakultät einer Zahl berechnet, length' die Länge einer Liste bestimmt, und rev' Listen reversiert. Beweisen Sie anschließend folgende Korrektheitsaussagen:

(a) $\forall n \in \mathbb{N} : \mathit{fac}'\,(n, 1) = n!$

(b) $\forall xs \in \mathscr{L}\,(X) : \mathit{length}'\,(xs, 0) = |xs|$

(c) $\forall xs \in \mathscr{L}\,(X) : \mathit{rev}'\,(xs, []) = \mathit{rev}\,xs$

Gehen Sie dazu wie folgt vor: Versuchen Sie zunächst einen Induktionsbeweis zu führen, ohne die Aussagen zu verstärken. Schreiben Sie explizit die Induktionsannahme auf und machen Sie sich bewusst, warum sich diese nicht anwenden lässt. Überlegen Sie sich anschließend eine geeignete Verstärkung der Aussage und führen Sie den Beweis erneut. Achten Sie auch hier darauf, die allquantifizierte Induktionsannahme aufzuschreiben.

Kompliziertere Verstärkungen

Verstärkungen erfordern im Allgemeinen Kreativität. Es gibt kein Schema, nach dem man immer die richtige Verstärkung findet. Viele Prozeduren lassen sich analog zu *powi* verstärken. Manchmal ist dieses Vorgehen jedoch nicht gut genug, wie das folgende Beispiel zeigt.

Wir definieren die Folge der Fibonacci-Zahlen und eine Prozedur, die diese endrekursiv berechnet:

$$\begin{aligned} F_0 &= 0 \\ F_1 &= 1 \\ F_{n+2} &= F_{n+1} + F_n \end{aligned} \qquad \begin{aligned} \mathit{fib}' &: \mathbb{N} \times \mathbb{N} \times \mathbb{N} \to \mathbb{N} \\ \mathit{fib}'\,(0, a, b) &= a \\ \mathit{fib}'\,(n+1, a, b) &= \mathit{fib}'\,(n, b, a+b) \end{aligned}$$

Die Korrektheitsaussage, an der wir nun interessiert sind, lautet $\forall n \in \mathbb{N} : F_n = \mathit{fib}'\,(n, 0, 1)$.

Versuchen wir hier eine einfache Induktion über $n \in \mathbb{N}$, so werden wir analog zum Beispiel der endrekursiven Potenz scheitern, da sich der Akku unserer Prozedur fib' im Rekursionsfall ändert. Ein erster Ansatz könnte sein, die Argumente von fib' analog zu obigem Beweis zu $\mathit{fib}'\,(n, a, b)$ zu verallgemeinern. Allerdings scheint es mit dieser Generalisierung fast unmöglich, vorherzusagen, was die Prozedur nun berechnet. Wählt man beispielsweise $a = 3$ und $b = 7$, so sind die ersten Werte $3, 7, 10, 17, 27, \ldots$ Die Ergebnisse scheinen kaum noch mit den entsprechenden Fibonacci-Zahlen $0, 1, 1, 2, 3, \ldots$ zusammenzuhängen. Bei genauerer Betrachtung der Prozedur stellen wir jedoch fest, dass immer, wenn die Prozedur mit aufeinanderfolgenden Fibonacci-Zahlen aufgerufen wird, sie für $n > 0$ wieder mit aufeinander folgenden Fibonacci-Zahlen aufgerufen wird. Wir können uns deshalb überlegen, was das Ergebnis ist, wenn die Prozedur mit zwei aufeinander folgenden Fibonacci-Zahlen F_k, F_{k+1} aufgerufen wird. Da die Prozedur in diesem Fall genau n-mal das jeweils nächste Paar aus Fibonacci-Zahlen generiert, kommen wir zu folgender Verstärkung: $\forall k \in \mathbb{N} : F_{n+k} = \mathit{fib}'\,(n, F_k, F_{k+1})$. Für den Beweis ist es wieder essentiell für das Anwenden der Induktionsannahme, dass k in dieser Aussage allquantifiziert wird.

Lemma 2. $\forall n \in \mathbb{N} : \forall k \in \mathbb{N} : F_{n+k} = \mathit{fib}'(n, F_k, F_{k+1})$

Beweis. Wir zeigen

$$\forall n \in \mathbb{N} : \forall k \in \mathbb{N} : F_{n+k} = \mathit{fib}'(n, F_k, F_{k+1})$$

durch Induktion über $n \in \mathbb{N}$.

Wir unterscheiden zwei Fälle:

- Sei $n = 0$. Sei $k \in \mathbb{N}$ beliebig. Dann

  $$\begin{aligned} \mathit{fib}'\,(0, F_k, F_{k+1}) &= F_k && \text{Definition } \mathit{fib}' \\ &= F_{0+k} && \text{Arithmetik} \end{aligned}$$

- Sei $n > 0$. Sei $k \in \mathbb{N}$ beliebig.

  Induktionannahme: Für alle $m < n$ gilt, dass $\forall k' \in \mathbb{N} : F_{m+k'} = \mathit{fib}'\,(m, F_{k'}, F_{k'+1})$.

  Dann

  $$\begin{aligned} \mathit{fib}'\,(n, F_k, F_{k+1}) &= \mathit{fib}'\,(n-1, F_{k+1}, F_k + F_{k+1}) && \text{Definition } \mathit{fib}' \\ &= \mathit{fib}'\,(n-1, F_{k+1}, F_{k+2}) && \text{Definition } F \\ &= F_{(n-1)+(k+1)} && \text{Induktion für } n-1 \text{ und } k' = k+1 \\ &= F_{n+k} && \text{Arithmetik} \end{aligned}$$

■

Korollar 2. $F_n = \mathit{fib}'\,(n, 0, 1)$

Beweis.

$$\begin{aligned} F_n &= F_{n+0} \\ &= \mathit{fib}'\,(n, F_0, F_{0+1}) && \text{Lemma 2} \\ &= \mathit{fib}'\,(n, 0, 1) && \text{Definition } F \end{aligned}$$

■