CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

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

Programmierung 1 (WS 2020/21)
Zusatztutorium 4 (Lösungsvorschläge)
Induktion

Hinweis: Diese Aufgaben wurden von den Tutoren für das Zusatztutorium erstellt. Sie sind für die Klausur weder relevant noch irrelevant. 🤔 markiert potentiell schwerere Aufgaben.

Natürliche Induktion

Aufgabe Z4.1 *(Induktive Korrektheitsbeweise)*
Zeigen Sie für die folgenden Prozeduren jeweils mittels Induktion, dass p die Funktion f berechnet, also dass $\forall z \in \mathit{Dom}\ f : p\ z = f\ z$ gilt.

(a)
$$\begin{aligned}
&p : \mathbb{N}^2 \to \mathbb{N}\\
&p\ (0, y) = y\\
&p\ (x, y) = 1 + p\ (x-1, y) \quad \text{für } x > 0\\
&f = \lambda(x,y) \in \mathbb{N}^2.\ x + y
\end{aligned}$$

(b)
$$\begin{aligned}
&p : \mathbb{N} \times \mathbb{Z} \to \mathbb{Z}\\
&p\ (0, y) = 0\\
&p\ (x, y) = y + p\ (x-1, y) \quad \text{für } x > 0\\
&f = \lambda(x,y) \in \mathbb{N} \times \mathbb{Z}.\ x \cdot y
\end{aligned}$$

(c)
$$\begin{aligned}
&p : \mathbb{N}^2 \to \mathbb{N}\\
&p\ (0, y) = y\\
&p\ (x, y) = p\ (x-1, y+1) \quad \text{für } x > 0\\
&f = \lambda(x,y) \in \mathbb{N}^2.\ x + y
\end{aligned}$$

(d)
$$\begin{aligned}
&p : \mathbb{Z}^2 \to \mathbb{N}\\
&p\ (x, y) = \text{if } x = y \text{ then } x\\
&\qquad\qquad \text{else if } x = 0 \text{ then } p\ (x, y-1)\\
&\qquad\qquad \text{else if } y = 0 \text{ then } p\ (x-1, y)\\
&\qquad\qquad \text{else } p\ (x-1, y-1)\\
&f = \lambda(x,y) \in \mathbb{N}^2.\ \text{if } x = y \text{ then } x \text{ else } 0
\end{aligned}$$

Lösungsvorschlag Z4.1

(a) Sei $y \in \mathbb{N}$.

Behauptung: $\forall x \in \mathbb{N} :\ p\ (x, y) = x + y$
Beweis: Durch Induktion über $x \in \mathbb{N}$. Wir unterscheiden zwei Fälle.

- Sei $x = 0$. Dann gilt:

$$\begin{aligned}
p\ (x, y) &= p\ (0, y) && x = 0\\
&= y && \text{Definition } p\\
&= 0 + y && \text{Arithmetik}\\
&= x + y && x = 0
\end{aligned}$$

- Sei $x > 0$. Induktionsannahme : $\forall y \in \mathbb{N} : \forall m < x : p(m, y) = m + y$

Dann gilt:

$$\begin{aligned} p(x,y) &= 1 + p(x-1,y) && \text{Definition } p \\ &= 1 + ((x-1)+y) && \text{Induktion für } x-1 \\ &= x + y && \text{Assoziativität, Kommutativität} \end{aligned}$$

(b) Sei $y \in \mathbb{Z}$.

Behauptung: $\forall x \in \mathbb{N} : \ p\,(x,y) = x \cdot y$
Beweis: Durch Induktion über $x \in \mathbb{N}$. Wir unterscheiden zwei Fälle.

- Sei $x = 0$. Dann gilt:

$$\begin{aligned} p\,(x,y) &= p\,(0,y) && x = 0 \\ &= 0 && \text{Definition } p \\ &= 0 \cdot y && \text{Arithmetik} \\ &= x \cdot y && x = 0 \end{aligned}$$

- Sei $x > 0$. Induktionsannahme : $\forall y \in \mathbb{N} : \forall m < n : p(m,y) = m \cdot y$
  Dann gilt:

$$\begin{aligned} p\,(x,y) &= y + p\,(x-1,y) && \text{Definition } p \\ &= y + ((x-1) \cdot y) && \text{Induktion für } x-1 \\ &= y + (x \cdot y - y) && \text{Distributivität} \\ &= x \cdot y && \text{Assoziativität, Kommutativität} \end{aligned}$$

(c) An dieser Stelle ist es wichtig, in der Behauptung über y zu quantifizieren, da die Induktionshypothese für beliebige $y \in \mathbb{N}$ anwendbar sein muss.

Behauptung: $\forall x \in \mathbb{N} : \forall y \in \mathbb{N} : \ p\,(x,y) = x + y$
Beweis: Durch Induktion über $x \in \mathbb{N}$. Wir unterscheiden zwei Fälle.

- Sei $x = 0$. Dann gilt:

$$\begin{aligned} p\,(x,y) &= p\,(0,y) && x = 0 \\ &= y && \text{Definition } p \\ &= 0 + y && \text{Arithmetik} \\ &= x + y && x = 0 \end{aligned}$$

- Sei $x > 0$. Induktionsannahme : $\forall y \in \mathbb{N} : \forall m < x : p(m,y) = m + y$
  Dann gilt:

$$\begin{aligned} p\,(x,y) &= p\,(x-1,y+1) && \text{Definition } p \\ &= (x-1) + (y+1) && \text{Induktion für } x-1 \\ &= x + y && \text{Assoziativität, Kommutativität} \end{aligned}$$

(d) Es gilt $Dom\,p = \mathbb{N}^2$.

Behauptung: $\forall (x,y) \in \mathbb{N}^2 : \ p\,(x,y) = \text{if } x = y \text{ then } x \text{ else } 0$
Beweis: Durch Induktion über $x + y \in \mathbb{N}$. Wir unterscheiden zwei Fälle.

- Sei $x + y = 0$, also $x = 0$ und $y = 0$. Dann gilt:

$$\begin{aligned}
p\ (x, y) = {} & p\ (0, 0) && x = 0 \land y = 0 \\
= {} & \text{if } 0 = 0 \text{ then } 0 \\
& \quad \text{else if } 0 = 0 \text{ then } p\ (0, 0 - 1) \\
& \quad \text{else if } 0 = 0 \text{ then } p\ (0 - 1, 0) \\
& \quad \text{else } p\ (0 - 1, 0 - 1) && \text{Definition } p \\
= {} & 0 && \text{Vereinfachen} \\
= {} & \text{if } 0 = 0 \text{ then } 0 \text{ else } 0 && \text{Semantik von } \textit{if} \\
= {} & \text{if } x = y \text{ then } x \text{ else } 0 && x = 0 \land y = 0
\end{aligned}$$

- Sei $x + y > 0$. Man unterscheide drei weitere Fälle:
  - Sei $x = 0$ und $y > 0$.

$$\begin{aligned}
p\ (x, y) = {} & p\ (0, y) && x = 0 \\
= {} & \text{if } 0 = y \text{ then } 0 \\
& \quad \text{else if } 0 = 0 \text{ then } p\ (0, y - 1) \\
& \quad \text{else if } y = 0 \text{ then } p\ (0 - 1, y) \\
& \quad \text{else } p\ (0 - 1, y - 1) && \text{Definition } p \\
= {} & p\ (0, y - 1) && \text{Vereinfachen (wegen } y \neq 0) \\
= {} & \text{if } 0 = y - 1 \text{ then } 0 \text{ else } 0 && \text{Induktion für } (x + y) - 1 \\
= {} & 0 && \text{Vereinfachen: Da Konsequenz und Alternative } 0 \\
= {} & \text{if } 0 = y \text{ then } 0 \text{ else } 0 && \text{Da Konsequenz und Alternative } 0 \\
= {} & \text{if } x = y \text{ then } 0 \text{ else } 0 && x = 0
\end{aligned}$$

  - Sei $y = 0$ und $x > 0$.

$$\begin{aligned}
p\ (x, y) = {} & p\ (x, 0) && x = 0 \\
= {} & \text{if } x = 0 \text{ then } x \\
& \quad \text{else if } x = 0 \text{ then } p\ (x, 0 - 1) \\
& \quad \text{else if } 0 = 0 \text{ then } p\ (x - 1, 0) \\
& \quad \text{else } p\ (x - 1, 0 - 1) && \text{Definition } p \\
= {} & p\ (x - 1, 0) && \text{Vereinfachen (wegen } x \neq 0) \\
= {} & \text{if } x - 1 = 0 \text{ then } x - 1 \text{ else } 0 && \text{Induktion für } (x - 1 + y) = (x + y) - 1 \\
= {} & 0 && \text{Vereinfachen: Semantik von } \textit{if} \\
= {} & \text{if } x = 0 \text{ then } x \text{ else } 0 && \text{Semantik von } \textit{if} \\
= {} & \text{if } x = y \text{ then } 0 \text{ else } 0 && y = 0
\end{aligned}$$

  - Sei $x > 0$ und $y > 0$. Man unterscheide zwei weitere Fälle:
    * Sei $x = y$.

$$\begin{aligned}
p\ (x, y) = {} & \text{if } x = y \text{ then } x \\
& \quad \text{else if } x = 0 \text{ then } p\ (x, y - 1) \\
& \quad \text{else if } y = 0 \text{ then } p\ (x - 1, y) \\
& \quad \text{else } p\ (x - 1, y - 1) && \text{Definition } p \\
= {} & x && \text{Vereinfachen} \\
= {} & \text{if } x = y \text{ then } x \text{ else } 0 && \text{Wegen } x = y + \text{Semantik von } \textit{if}
\end{aligned}$$

* Sei $x \neq y$.

$$\begin{aligned}
p\ (x,y) &= \text{if } x = y \text{ then } x \\
&\quad\ \text{else if } x = 0 \text{ then } p\ (x, y-1) \\
&\quad\ \text{else if } y = 0 \text{ then } p\ (x-1, y) \\
&\quad\ \text{else } p\ (x-1, y-1) && \text{Definition } p \\
&= p\ (x-1, y-1) && \text{Vereinfachen (wegen } y \neq 0,\ x \neq 0 \text{ und } x \neq y) \\
&= \text{if } x-1 = y-1 \text{ then } x-1 \text{ else } 0 && \text{Induktion für } (x-1)+(y-1) = (x+y)-2 \\
&= 0 && \text{Aus } x \neq y \text{ folgt } x-1 \neq y-1 \text{ und Semantik von } \mathit{if} \\
&= \text{if } x = y \text{ then } x \text{ else } 0 && \text{Wegen } x \neq y \text{ und Semantik von } \mathit{if}
\end{aligned}$$

Aufgabe Z4.2 *(faciter)*
Beweisen Sie, dass für die Schrittfunktion $f = \lambda(k,x).\ (k+1, k \cdot x)$ gilt:

(a) $\forall n \in \mathbb{N} : f\ (n+1, n!) = (n+2, (n+1)!)$

(b) $\forall n \in \mathbb{N} : (n+1, n!) = f^n(1,1)$

Lösungsvorschlag Z4.2

(a) *Beweis.* Sei $n \in \mathbb{N}$, dann gilt

$$\begin{aligned}
f(n+1, n!) &= ((n+1)+1, (n+1) \cdot n!) && \text{Definition } f \\
&= (n+2, (n+1)!) && \text{Definition } !
\end{aligned}$$

■

(b) *Beweis.* Beweis durch Induktion über $n \in \mathbb{N}$.

- Sei $n = 0$. Dann

$$\begin{aligned}
f^n(1,1) &= f^0(1,1) && n = 0 \\
&= (1,1) && \text{Definition Iteration} \\
&= (0+1, 0!) && \text{Arithmetik}
\end{aligned}$$

- Sei $n > 0$. Induktionsannahme : $\forall m < n : (m+1, m!) = f^m(1,1)$
Dann ist

$$\begin{aligned}
f^n(1,1) &= f(f^{n-1}(1,1)) && \text{Definition Iteration} \\
&= f((n-1)+1, (n-1)!) && \text{Induktion für } n-1 \\
&= f(n, (n-1)!) && \text{Arithmetik} \\
&= (n+1, n \cdot (n-1)!) && \text{Definition } f \\
&= (n+1, n!) && \text{Arithmetik}
\end{aligned}$$

■

Strukturelle Induktion

Aufgabe Z4.3 *(foldl auf zwei Listen)*
Seien X, Y Mengen und f eine Funktion $X \times Y \to Y$. Beweisen Sie durch strukturelle Induktion über xs, dass gilt:

$$\forall xs \in \mathscr{L}\ (X) : \forall ys \in \mathscr{L}\ (X) : \forall y \in Y : \mathit{foldl}\ (f, y, xs\ @\ ys) = \mathit{foldl}\ (f, \mathit{foldl}\ (f, y, xs), ys)$$

Lösungsvorschlag Z4.3

Beweis. durch Induktion über $xs \in \mathscr{L}(X)$. Fallunterscheidung.

- Fall $xs = nil$:

$$\begin{aligned} foldl\ (f, y, nil \mathbin{@} ys) &= foldl\ (f, y, ys) && \text{Definition von } @ \\ &= foldl\ (f, foldl\ (f, y, nil), ys) && \text{Definition von } foldl \end{aligned}$$

- Fall $xs = x :: xr$:
  Induktionsannahme: $\forall ys \in \mathscr{L}(X) : \forall xr : foldl\ (f, y, xr \mathbin{@} ys) = foldl\ (f, foldl\ (f, y, xr), ys)$

$$\begin{aligned} foldl\ (f, y, xs \mathbin{@} ys) &= foldl\ (f, y, (x :: xr) \mathbin{@} ys) && xs = x :: xr \\ &= foldl\ (f, f\ (x, y), xr \mathbin{@} ys) && \text{Definition von } foldl \\ &= foldl\ (f, foldl\ (f, f\ (x, y), xr), ys) && \text{Induktion für } xr \\ &= foldl\ (f, foldl\ (f, y, x :: xr), ys) && \text{Definition von } foldl \\ &= foldl\ (f, foldl\ (f, y, xs), ys) && xs = x :: xr \end{aligned}$$

■

Aufgabe Z4.4 *(Beträge)*
Beweisen Sie die Aussage $|xs \mathbin{@} [z]| = |xs| + 1$.

Lösungsvorschlag Z4.4
Beweis durch Induktion über $xs \in \mathscr{L}(X)$. Fallunterscheidung.

(a) Sei $xs = nil$:

$$\begin{aligned} |nil \mathbin{@} [z]| &= |z :: nil| && \text{Definition } :: \\ &= |[z]| && \text{Definition } @ \\ &= 1 + |nil| && \text{Definition } length \\ &= |nil| + 1 && \text{Kommutativität } + \end{aligned}$$

(b) Sei $xs = x :: xr$:

$$\begin{aligned} |(x :: xr) \mathbin{@} [z]| &= |x :: (xr) \mathbin{@} [z]| && \text{Definition } @ \\ &= 1 + |(xr) \mathbin{@} [z]| && \text{Definition } length \\ &= 1 + |(xr)| + 1 && \text{Induktion für } xr \\ &= |x :: xr| + 1 && \text{Definition } length \end{aligned}$$

Aufgabe Z4.5 *(Alles über Listen)*
Beweisen Sie mit struktureller Induktion, dass für alle Listen $xs, ys \in \mathscr{L}(X)$ gilt:

(a) $xs \mathbin{@} nil = xs$

(b) $rev\ (xs \mathbin{@} ys) = rev\ ys \mathbin{@} rev\ xs$

(c) $rev\ (rev\ xs) = xs$

Hinweis : Die Verwendung von Aussagen aus vorherigen Aufgabenteilen kann nützlich sein, außerdem kann Proposition 10.5 an einer Stelle weiter helfen.

Lösungsvorschlag Z4.5

(a) *Beweis.* Wir zeigen

$$\forall xs \in \mathscr{L}(X) : xs \mathbin{@} nil = xs$$

durch strukturelle Induktion über $xs \in \mathscr{L}(X)$. Wir unterscheiden zwei Fälle:

- Fall $xs = nil$:

$$\begin{aligned} xs \mathbin{@} nil &= nil \mathbin{@} nil && xs = nil \\ &= nil && \text{Definition } @ \\ &= xs && xs = nil \end{aligned}$$

- Fall $xs = x :: xr$:

  Induktionsannahme: $xr \mathbin{@} nil = xr$

$$\begin{aligned} xs \mathbin{@} nil &= (x :: xr) \mathbin{@} nil && xs = x :: xr \\ &= x :: (xr \mathbin{@} nil) && \text{Definition } @ \\ &= x :: xr && \text{Induktion für } xr \\ &= xs && xs = x :: xr \end{aligned}$$

■

(b) *Beweis.* Wir zeigen

$$\forall xs \in \mathscr{L}(X) : \forall ys \in \mathscr{L}(X) : rev\ (xs \mathbin{@} ys) = rev\ ys \mathbin{@} rev\ xs$$

durch strukturelle Induktion über $xs \in \mathscr{L}(X)$. Wir unterscheiden zwei Fälle:

- Fall $xs = nil$. Sei $ys \in \mathscr{L}(X)$:

$$\begin{aligned} rev\ (xs \mathbin{@} ys) &= rev\ (nil \mathbin{@} ys) && xs = nil \\ &= rev\ ys && \text{Definition } @ \\ &= rev\ ys \mathbin{@} nil && \text{Aufgabe (a)} \\ &= rev\ ys \mathbin{@} rev\ nil && \text{Definition } rev \\ &= rev\ ys \mathbin{@} rev\ xs && xs = nil \end{aligned}$$

- Fall $xs = x :: xr$, sei $ys \in \mathscr{L}(X)$:

  Induktionsannahme: $\forall ys' \in \mathscr{L}(X) : rev\ (xr \mathbin{@} ys') = rev\ ys' \mathbin{@} rev\ xr$

$$\begin{aligned} rev\ (xs \mathbin{@} ys) &= rev\ ((x :: xr) \mathbin{@} ys) && xs = x :: xr \\ &= rev\ (x :: (xr \mathbin{@} ys)) && \text{Definition } @ \\ &= rev\ (xr \mathbin{@} ys) \mathbin{@} [x] && \text{Definition } rev \\ &= (rev\ ys \mathbin{@} rev\ xr) \mathbin{@} [x] && \text{Induktion für } ys' = ys \\ &= rev\ ys \mathbin{@} (rev\ xr \mathbin{@} [x]) && \text{Proposition 10.5} \\ &= rev\ ys \mathbin{@} rev\ (x :: xr) && \text{Definition } rev \\ &= rev\ ys \mathbin{@} rev\ xs && xs = x :: xr \end{aligned}$$

■

(c) *Beweis.* Wir zeigen

$$\forall xs \in \mathscr{L}(X) : rev\ (rev\ xs) = xs$$

durch strukturelle Induktion über $xs \in \mathscr{L}(X)$. Wir unterscheiden zwei Fälle:

- Fall $xs = nil$:

$$\begin{aligned} rev\ (rev\ xs) &= rev\ (rev\ nil) && xs = nil \\ &= rev\ nil && \text{Definition } rev \\ &= nil && \text{Definition } rev \\ &= xs && xs = nil \end{aligned}$$

- Fall $xs = x :: xr$:

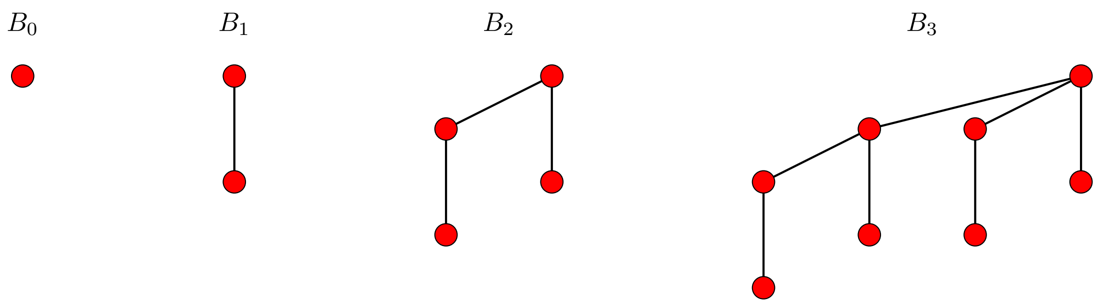
  Induktionsannahme: $rev\ (rev\ xr) = xr$

$$\begin{aligned} rev\ (rev\ xs) &= rev\ (rev\ (x :: xr)) && xs = x :: xr \\ &= rev\ (rev\ xr\ @\ [x]) && \text{Definition } rev \\ &= rev\ [x]\ @\ rev\ (rev\ xr) && \text{Aufgabe (b)} \\ &= rev\ [x]\ @\ xr && \text{Induktion für } xr \\ &= rev\ (x :: nil)\ @\ xr && \text{Definition } [\cdot] \\ &= (rev\ nil\ @\ [x])\ @\ xr && \text{Definition } rev \\ &= (nil\ @\ [x])\ @\ xr && \text{Definition } rev \\ &= [x]\ @\ xr && \text{Definition } @ \\ &= (x :: nil)\ @\ xr && \text{Definition } [\cdot] \\ &= x :: (nil\ @\ xr) && \text{Definition } @ \\ &= x :: xr && \text{Definition } @ \\ &= xs && xs = x :: xr \end{aligned}$$

■

Aufgabe Z4.6 *(Binomialbäume)*
Ein Binomialbaum $B_k \in \mathcal{B}$ der Ordnung k ist ein geordneter Baum und rekursiv wie folgt definiert:

- B_0 ist der Baum mit einem Knoten: $B_0 = [\,]$.
- B_k besteht aus zwei Kopien von B_{k-1}. Die Wurzel der einen Kopie wird das linkeste Kind der Wurzel der anderen Kopie: $B_k = [B_{k-1}, B'_1, \ldots, B'_n]$ wenn $B_{k-1} = [B'_1, \ldots, B'_n]$.



Graphische Darstellung der Binomialbäume B_0, B_1, B_2 und B_3

Seien die Prozeduren s, b, d wie in Kapitel 10.5 des Buches gegeben. Es sei außerdem die Prozedur $a : \mathcal{B} \to \mathbb{N}$ mit $a\ [t_1, \ldots, t_n] = n$ gegeben.

Beweisen Sie:

(a) $s\ (B_k) = 2^k$.

(b) $d\ (B_k) = k$.

(c) $a\ (B_k) = k$.

Lösungsvorschlag Z4.6

(a) Beweis von $\forall k \in \mathbb{N} : s\ (B_k) = 2^k$ durch Induktion über $k \in \mathbb{N}$. Fallunterscheidung.

- Sei $k = 0$.

$$
\begin{aligned}
s\ (B_0) &= s\ [\,] && \text{Definition } B_0 \\
&= \text{if } n = 0 \text{ then } 1 \text{ else } 1 && \text{Definition s} \\
&= 1 && \text{Definition if, } n = 0 \\
&= 2^0 && \text{Arithmetik}
\end{aligned}
$$

- Sei $k = 1$.

$$
\begin{aligned}
s\ (B_1) &= s\ [B_0] && \text{Definition } B_1 \\
&= \text{if } n = 0 \text{ then } 1 \text{ else } 1 + s\ (B_0) && \text{Definition s} \\
&= 1 + s\ (B_0) && \text{Definition if, } n = 1 \\
&= 1 + 2^0 && s\ (B_0) = 2^0, \text{ s. o.} \\
&= 2^1 && \text{Arithmetik}
\end{aligned}
$$

- Sei $k > 1$.

  Induktionsannahme: $s\ (B_\ell) = 2^\ell$ gelte für alle $\ell < k$.

$$
\begin{aligned}
s\ (B_k) &= s\ [B_{k-1}, B'_1, \ldots, B'_n] && \text{Definition } B_k \\
&= \text{if } n+1 = 0 \text{ then } 1 \text{ else } 1 + s\ (B_{k-1}) + s\ (B'_1) + \ldots + s\ (B'_n) && \text{Definition s} \\
&= 1 + s\ (B_{k-1}) + s\ (B'_1) + \ldots + s\ (B'_n) && \text{Definition if, } n + 1 \neq 0 \\
&= s\ (B_{k-1}) + 1 + s\ (B'_1) + \ldots + s\ (B'_n) && \text{Assoziativität Addition} \\
&= s\ (B_{k-1}) + \text{if } n = 0 \text{ then } 1 \text{ else } 1 + s\ (B'_1) + \ldots + s\ (B'_n) && \text{Definition if, } n \geq 1 \\
&= s\ (B_{k-1}) + s\ (B_{k-1}) && \text{Definition } s \\
&= 2^{k-1} + 2^{k-1} && \text{Induktion für } k-1 \\
&= 2^k && \text{Arithmetik}
\end{aligned}
$$

(b) Beweis von $\forall k \in \mathbb{N} : d\ (B_k) = k$ durch Induktion über $k \in \mathbb{N}$. Fallunterscheidung.

- Sei $k = 0$.

$$
\begin{aligned}
d\ (B_0) &= d\ [\,] && \text{Definition } B_1 \\
&= \text{if } n = 0 \text{ then } 0 \text{ else } 1 + \max\{\,\} && \text{Definition } d \\
&= 0 && \text{Definition if, } n = 0
\end{aligned}
$$

- Sei $k = 1$.

$$
\begin{aligned}
d\ (B_1) &= d\ [B_0] && \text{Definition } B_1 \\
&= \text{if } n = 0 \text{ then } 0 \text{ else } 1 + \max\{d(B_0)\} && \text{Definition } d \\
&= 1 + \max\{d(B_0)\} && \text{Definition if, } n = 1 \\
&= 1 + \max\{0\} && d\ (B_0) = 0, \text{ s. o.} \\
&= 1 + 0 && \text{Definition max} \\
&= 0 && \text{Arithmetik}
\end{aligned}
$$

- Sei $k > 1$.

  Induktionsannahme: $s\ (B_\ell) = \ell$ gelte für alle $\ell < k$.

$$\begin{aligned}
d\ (B_k) &= d\ \ [B_{k-1}, B'_1, \ldots, B'_n] && \text{Definition } B_k \\
&= \text{if } n+1 = 0 \text{ then } 0 \text{ else } 1 + \max\left\{d\ (B_{k-1}), d\ (B'_1), \ldots, d\ (B'_n)\right\} && \text{Definition } d \\
&= 1 + \max\left\{d\ (B_{k-1}), d\ (B'_1), \ldots, d\ (B'_n)\right\} && \text{Definition if, } n+1 \neq 0 \\
&= 1 + \max\left\{d\ (B_{k-1}), \max\left\{d\ (B'_1), \ldots, d\ (B'_n)\right\}\right\} && \text{Definition max} \\
&= \max\left\{1 + d\ (B_{k-1}), 1 + \max\left\{d\ (B'_1), \ldots, d\ (B'_n)\right\}\right\} && \text{Definition max} \\
&= \max\left\{1 + d\ (B_{k-1}), \text{if } n = 0 \text{ then } 0 \text{ else } 1 + \max\left\{d\ (B'_1), \ldots, d\ (B'_n)\right\}\right\} && \text{Definition if, } n \geq 1 \\
&= \max\left\{1 + d\ (B_{k-1}), d\ (B_{k-1})\right\} && \text{Definition } d \\
&= 1 + d\ (B_{k-1}) && \text{Definition max} \\
&= 1 + (k-1) && \text{Induktion für } k-1 \\
&= k && \text{Arithmetik}
\end{aligned}$$

(c) Beweis von $\forall k \in \mathbb{N} : a\ (B_k) = k$ durch Induktion über $k \in \mathbb{N}$. Fallunterscheidung.

- Sei $k = 0$.

$$\begin{aligned}
a\ (B_0) &= a\ \ [\,] && \text{Definition } B_0 \\
&= 0 && \text{Definition } a
\end{aligned}$$

- Sei $k > 0$.

  Induktionsannahme: $a\ (B_\ell) = \ell$ gelte für alle $\ell < k$.

$$\begin{aligned}
a\ (B_k) &= a\ \ [B_{k-1}, B'_1, \ldots, B'_n] && \text{Definition } B_k \\
&= |[B_{k-1}, B'_1, \ldots, B'_n]| && \text{Definition } a \\
&= 1 + |[B'_1, \ldots, B'_n]| && \text{Definition } |\cdot| \\
&= 1 + a\ \ [B'_1, \ldots, B'_n] && \text{Definition } a \\
&= 1 + a\ (B_{k-1}) && \text{Definition } B_k \\
&= 1 + (k-1) && \text{Induktion für } k-1 \\
&= k && \text{Arithmetik}
\end{aligned}$$

Aufgabe Z4.7 *(Binäre Bäume)*
Ein binärer Baum ist ein Baum, bei dem jeder innere Knoten genau zwei Nachfolger hat. Wir definieren dafür die Menge $\mathcal{M} \subseteq \mathscr{T}$ der binären Bäume über zwei Regeln: 🤔

1. $[] \in \mathcal{M}$
2. $[t_1, t_2] \in \mathcal{M}$ falls $t_1, t_2 \in \mathcal{M}$

(a) Beweisen Sie: $\forall t \in \mathcal{M} : b\ t \leq 2^{d\ t}$.

(b) Beweisen Sie: $\forall t \in \mathcal{M} : s\ t \leq 2^{d\ t + 1} - 1$.

Lösungsvorschlag Z4.7

(a) *Beweis.* Wir zeigen nun die Aussage

$$\forall t \in \mathcal{M} : b\ t \leq 2^{d\ t}$$

durch strukturelle Induktion über $t \in \mathcal{M}$. Wir unterscheiden zwei Fälle:

- Fall $t = []$.

Dann gilt:

$$\begin{aligned} b\ [] &= 1 && \text{Definition von } b \\ &= 2^0 && \text{Definition Potenz} \\ &= 2^{d\ []} && \text{Definition von } d \end{aligned}$$

- Fall $t = [t_1, t_2]$ mit $t_1, t_2 \in \mathcal{M}$.

  Induktionsannahme: $\forall t' \in \{t_1, t_2\} : b\ t' \leq 2^{d\ t'}$

  Da $t = [t_1, t_2]$ wissen wir, dass $d\ t > 0$ sein muss. Außerdem folgt aus der Definition von d und max, dass $d\ t_1 \leq d\ t - 1$ und $d\ t_2 \leq d\ t - 1$.

  Damit gilt:

$$\begin{aligned} b\ t &= b\ t_1 + b\ t_2 && \text{Definition von } b \\ &\leq 2^{d\ t_1} + b\ t_2 && \text{Induktion für } t' = t_1 \\ &\leq 2^{d\ t_1} + 2^{d\ t_2} && \text{Induktion für } t' = t_2 \\ &\leq 2^{d\ t-1} + 2^{d\ t_2} && d\ t_1 \leq d\ t - 1 \\ &\leq 2^{d\ t-1} + 2^{d\ t-1} && d\ t_2 \leq d\ t - 1 \\ &= 2 \cdot 2^{d\ t-1} && \text{Arithmetik} \\ &= 2^{d\ t} && \text{Definition Potenz} \end{aligned}$$

■

(b) *Beweis.* Wir zeigen die Aussage

$$\forall t \in \mathcal{M} : s\ t \leq 2^{d\ t+1} - 1$$

durch strukturelle Induktion über $t \in \mathcal{M}$. Wir unterscheiden zwei Fälle:

- Sei $t = []$.

  Dann gilt:

$$\begin{aligned} s\ [] &= 1 && \text{Definition von } s \\ &= 2^1 - 1 && \text{Arithmetik} \\ &= 2^{d\ []+1} - 1 && \text{Definition von } d \end{aligned}$$

- Sei $t = [t_1, t_2]$ mit $t_1, t_2 \in \mathcal{M}$.

  Induktionsannahme: $\forall t' \in \{t_1, t_2\} : s\ t' \leq 2^{d\ t'+1} - 1$

  Da $t = [t_1, t_2]$ wissen wir, dass $d\ t > 0$ sein muss. Außerdem folgt aus der Definition von d und max, dass $d\ t_1 \leq d\ t - 1$ und $d\ t_2 \leq d\ t - 1$.

  Damit gilt:

$$\begin{aligned} s\ t &= 1 + s\ t_1 + s\ t_2 && \text{Definition von } s \\ &\leq 1 + (2^{d\ t_1+1} - 1) + s\ t_2 && \text{Induktion für } t' = t_1 \\ &\leq 1 + (2^{d\ t_1+1} - 1) + (2^{d\ t_2+1} - 1) && \text{Induktion für } t' = t_2 \\ &\leq 1 + (2^{(d\ t-1)+1} - 1) + (2^{d\ t_2+1} - 1) && \text{da } d\ t_1 \leq d\ t - 1 \text{ und } a \leq b \Rightarrow 2^a \leq 2^b \\ &\leq 1 + (2^{(d\ t-1)+1} - 1) + (2^{(d\ t-1)+1} - 1) && \text{da } d\ t_2 \leq d\ t - 1 \text{ und } a \leq b \Rightarrow 2^a \leq 2^b \\ &= 1 + 2 \cdot (2^{(d\ t-1)+1} - 1) && \text{Arithmetik} \\ &= 1 + 2 \cdot 2^{(d\ t-1)+1} - 2 && \text{Arithmetik} \\ &= 2 \cdot 2^{d\ t} - 1 && \text{Arithmetik} \\ &= 2^{d\ t+1} - 1 && \text{Definition Potenz} \end{aligned}$$

■

Verstärkung

Aufgabe Z4.8 *(powi)*
Beweisen Sie, dass folgende Aussage gilt: $powi(x, n, 1) = x^n$. *powi* ist dabei wie folgt definiert:

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

Lösungsvorschlag Z4.8
Wir verstärken die Aussage folgendermaßen:
$\forall a.\ powi(x, n, a) = x^n \cdot a$

Beweis. Durch Induktion über n. Sei $a \in \mathbb{N}$ beliebig.

- Fall $n = 0$:

$$\begin{aligned} powi(x, 0, a) &= a && \text{Def. } powi \\ &= x^0 \cdot a \end{aligned}$$

- Fall $n > 0$:
  Induktionsannahme : $\forall a, x \in \mathbb{N} : \forall m < n : powi(x, m, a) = x^m \cdot a$

$$\begin{aligned} powi(x, n, a) &= powi(x, n-1, a \cdot x) && \text{Def. } powi \\ &= x^{n-1} \cdot (a \cdot x) && \text{Induktion für } n \\ &= x^n \cdot a \end{aligned}$$

Die zu zeigende Aussage folgt dann mit $a = 1$. ■

Aufgabe Z4.9 *(Der kleine Gauß)*
Sei die Prozedur *iterdn* wie folgt gegeben:

$$\begin{aligned} &iterdn : \mathbb{N} \times \mathbb{N} \times X \times (\mathbb{N} \times X \to X) \to X \\ &iterdn(n, m, s, f) = \text{if } n < m \text{ then } s \text{ else } iterdn(n-1, m, f(n, s), f) \end{aligned}$$

Weiterhin sei $f = \lambda(a, b) \in \mathbb{N} \times \mathbb{N}.\ a + b$.

Zeigen Sie mittels Induktion die folgende Aussage. Überlegen Sie sich zuvor, ob Sie die Induktionshypothese verstärken müssen: $\forall n \in \mathbb{N}.\ iterdn(n, 1, 0, f) = \sum_{i=1}^{n} i$

Lösungsvorschlag Z4.9
Wir verstärken die Aussage:
Behauptung: $\forall n \in \mathbb{N} : \forall a \in \mathbb{N} : iterdn(n, 1, a, f) = a + \sum_{i=1}^{n} i$ mit $f = \lambda(a, b) \in \mathbb{N} \times \mathbb{N}. a + b$

Beweis. Durch Induktion über $n \in \mathbb{N}$. Fallunterscheidung:

- Sei $n = 0$ und $a \in \mathbb{N}$. Dann gilt:

$$\begin{aligned} iterdn(n, 1, a, f) &= iterdn(0, 1, a, f) && n = 0 \\ &= a && \text{Def. von } iterdn \\ &= a + \textstyle\sum_{i=1}^{0} && \text{Def. von } \textstyle\sum \\ &= a + \textstyle\sum_{i=1}^{n} && n = 0 \end{aligned}$$

- Sei $n > 0$ und $a \in \mathbb{N}$.
  Induktionsannahme: Für alle $m < n$ gilt $\forall a \in \mathbb{N} : iterdn(m, 1, a, f) = a + \sum_{i=1}^{m} i$ mit $f = \lambda(a, b) \in \mathbb{N} \times \mathbb{N}.a + b$.
  Dann gilt:

$$\begin{aligned}
iterdn(n, 1, a, f) &= iterdn(n-1, 1, f(n, a), f) && \text{Def. von } iterdn \\
&= f(n, a) + \textstyle\sum_{i=1}^{n-1} i && \text{Induktion für } m = n-1 \\
&= n + a + \textstyle\sum_{i=1}^{n-1} i && \text{Def. von } f \\
&= a + \textstyle\sum_{i=1}^{n} i && \text{Def. von } \textstyle\sum
\end{aligned}$$

■

Aufgabe Z4.10 *(Länge endrekursiv)*
Gegeben sei die Prozedur $L' : \mathscr{L}(X) \times \mathbb{N} \to \mathbb{N}$

$$\begin{aligned}
L'([], n) &= n \\
L'(x :: A, n) &= L'(A, n+1)
\end{aligned}$$

Beweisen Sie $L'(A, 0) = |A|$.

Lösungsvorschlag Z4.10
Wir verstärken die Aussage zu $\forall n.\ L'(A, n) = |A| + n$. Die eigentliche Aussage folgt dann sofort mit $n = 0$.

Beweis. Durch Induktion über $xs \in \mathscr{L}(X)$. Sei $n \in \mathbb{N}$ beliebig.

- Fall $xs = nil$:

$$\begin{aligned}
L'(xs, n) &= L'(nil, n) && xs = nil \\
&= n && \text{Def. } L' \\
&= 0 + n && \\
&= |nil| + n && \text{Def. } |\cdot|
\end{aligned}$$

- Fall $xs = x :: A$:
  Induktionsannahme: $\forall n :\ L'(A, n) = |A| + n$.

$$\begin{aligned}
L'(xs, n) &= L'(x :: A, n) && xs = x :: A \\
&= L'(A, n+1) && \text{Def. } L' \\
&= |A| + (n+1) && \text{Induktion für } A \\
&= 1 + |A| + n && \\
&= |x :: A| + n && \text{Def. } |\cdot|
\end{aligned}$$

■

Aufgabe Z4.11 *(Strukturelle Verstärkung)*
In Kapitel 4.4 haben Sie gelernt, dass Listen mit `foldl` reversiert werden können. Jetzt können Sie die Korrektheit dieses Vorgehens beweisen.

Sei X eine Menge und sei f die Funktion $\lambda(x, xs) \in X \times \mathscr{L}(X)\,.\, x :: xs$. Für die Korrektheit der Reversion mit `foldl` muss die Gültigkeit der Aussage $\forall xs \in \mathscr{L}(X) : rev\ xs = foldl\ (f, nil, xs)$ gezeigt werden.

Suchen Sie eine geeignete Verstärkung dieser Korrektheitsaussage und beweisen Sie die Gültigkeit der Verstärkung durch strukturelle Induktion über xs.

Lösungsvorschlag Z4.11
Unsere Verstärkung lautet:

$$\forall xs \in \mathscr{L}(X) : \forall ys \in \mathscr{L}(X) : (rev\ xs)\ @\ ys = foldl\ (f, ys, xs)$$

Beweis. Beweis durch strukturelle Induktion über $xs \in \mathscr{L}(X)$.

Wir unterscheiden zwei Fälle.

- Sei $xs = nil$. Dann gilt für ein beliebiges $ys \in \mathscr{L}(X)$:

$$\begin{aligned} foldl\ (f, ys, xs) &= ys && \text{Definition von } foldl \\ &= xs\ @\ ys && \text{Definition von } @ \\ &= rev\ xs\ @\ ys && \text{Definition von } rev \end{aligned}$$

- Sei $xs = x :: xr$ und $ys \in \mathscr{L}(X)$ beliebig.
  Induktionsannahme : $(rev\ xs)\ @\ ys = foldl\ (f, ys, xs)$

$$\begin{aligned} foldl\ (f, ys, xs) &= foldl\ (f, f\ (x, ys), xr) && \text{Definition von } foldl \\ &= foldl\ (f, x :: ys, xr) && \text{Definition von } f \\ &= rev\ xr\ @\ (x :: ys) && \text{Induktion für } xr \text{ und } x :: ys \\ &= rev\ xr\ @\ (x :: (nil\ @\ ys)) && \text{Definition von } @ \\ &= rev\ xr\ @\ ((x :: nil)\ @\ ys) && \text{Definition von } @ \\ &= rev\ xr\ @\ ([x]\ @\ ys) && \text{Definition von } :: \\ &= (rev\ xr\ @\ [x])\ @\ ys && \text{Proposition 10.5: Assoziativität von } @ \\ &= (rev\ xs)\ @\ ys && \text{Definition von } rev \end{aligned}$$

■