Technische Universität München **WS 2006/07**
Institut für Informatik
Prof. Manfred Broy
A. Gruler, B. Spanfelner **Musterlösung zu Blatt 3**

Übungen zu „Formale Methoden“

Aufgabe 1 Induktionsbeweise über Int [LÖSUNG]

Für die nachfolgenden Beweise benutzen wir die Axiome der Spezifikation Int. Zusätzlich verwenden wir die Kommutativität $x+y = y+x$ für Int (Beweis siehe Vorlesung/Skript).

Die Funktion $sub : Int, Int \to Int$ sei gegeben durch:

$$sub(x,y) \quad = \quad \begin{cases} x, & \text{falls } y = 0; \\ sub(x-1, y-1), & \text{falls } y > 0; \\ sub(x+1, y+1), & \text{falls } y < 0 \end{cases}$$

$$\overset{(*),(**)}{=} \quad \begin{cases} x, & \text{falls } y = 0; \\ sub\big(pred(x),\ pred(y)\big), & \text{falls } y > 0; \\ sub\big(succ(x),\ succ(y)\big), & \text{falls } y < 0 \end{cases}$$

Hinweis: Es wird hier angenommen, daß die Konstante “1“ als $succ(0)$ in Int definiert ist. Wird das jedoch nicht vorausgesetzt, muss sub über die zweite Gleichheit von oben definiert werden. Die nachfolgenden Theoreme zeigen die Äquivalenz beider Varianten:

$$x - 1 = \quad x - succ(0) = pred(x - 0) = pred(x) \qquad (*)$$

$$x + 1 = \quad x + succ(0) = succ(0) + x = succ(0 + x) = succ(x) \qquad (**)$$

(a) Zu zeigen ist:

$$sub(x, y-1) = sub(x+1, y) \qquad (Lemma\ 1)$$

Beweis mittels Induktion über y:

- Induktionsanfang: $y = 0$

  $sub(x, 0-1) \overset{(*)}{=} sub\big(x, pred(0)\big) \overset{Def.sub}{=} sub\big(succ(x), 0\big) \overset{(**)}{=} sub(x+1, 0)$

- Induktionsschritt: $n \rightsquigarrow n+1$

  Z.z.: $sub\big(x, (n+1)-1\big) = sub\big(x+1, (n+1)\big)$

  Ind. Annahme: $sub\big(x, n-1\big) = sub\big(x+1, n\big)$

  1.Fall: $n < 0$

  $$\begin{aligned} sub\big(x,\ (n+1)-1\big) &= sub\big(x+1,\ (n+1)-1+1\big) && \text{Def. sub} \\ &= sub\Big(x+1,\ succ\big(pred(succ(n))\big)\Big) && (*), (**) \\ &= sub\big(x+1,\ (n+1)\big) && \text{Def. Int, } (**) \end{aligned}$$

2.Fall: $n > 0$

Linke Seite:

$sub\big(x,\ (n+1)-1\big)$	$= sub(x-1,\ n-1)$	Assoz., Def. sub
	$= sub\big((x-1)+1,\ n\big)$	Ind. Annahme
	$= sub(x,\ n)$	

Rechte Seite:

$sub(x+1,\ n+1)$	$= sub(x,\ n)$	Def. sub

□

Weiterhin gilt für alle $x, y \in Int$ die ähnliche Beziehung:

$$sub(x, y+1) = sub(x-1, y) \qquad (Lemma\ 2)$$

(Der Beweis hierzu erfolgt ähnlich zum Beweis für das Lemma 1, ebenfalls durch Induktion.)

(b) Zu zeigen ist für alle $x, y, z \in Int,\ \ 0 \leq z \leq y,\ \$ durch Induktion:

$$sub(x, sub(y, z)) \ = \ sub(x+z, y)$$

Der Übersichtlichkeit halber beweisen wir hier die Aussage bereits für alle $x, y, z \in Int$ und nicht nur für die eingeschränkte Menge aus der Aufgabenstellung. Fall 2 im folgenden Beweis gibt also bereits eine Lösung für Aufgabe 3 (Für eine ausführlichere Erklärung siehe die Lösung zur Aufgabe 3).

Wir benutzen die beiden Hilfslemmata (Beweis siehe Vorlesung/Skript):

$$(x+y)+1 \ = \ x+(y+1) \qquad (Lemma\ 3)$$
$$(x+y)-1 \ = \ x+(y-1) \qquad (Lemma\ 4)$$

Induktion über den Absolutwert $abs(z)$ von z (Entspricht einer strukturellen Induktion über die 3 Konstruktoren 0, *succ* und *pred* von Int):

- Induktionsanfang: $abs(z) = 0 \ \Rightarrow \ z = 0$
  Z.z.: $sub(x, sub(y, 0)) \ = \ sub(x+0, y)$

  Linke Seite: $sub(x, sub(y, 0)) \overset{Def.\ sub}{=} sub(x, y)$
  Rechte Seite: $sub(x+0, y) \overset{Kommut.}{=} sub(0+x, y) \overset{Axiom\ 9}{=} sub(x, y)$

- Induktionsschritt: $abs(z) = n+1$
  Fallunterscheidung:

  1. Fall: $z > 0$: $z = succ^{n+1}(0)$, dann sei $b = succ^n(0)$ und $z = succ(b)$
  Induktionsannahme: $sub(x, sub(y, b)) \ = \ sub(x+b, y)$
  Zu zeigen: $sub(x, sub(y, succ(b))) \ = \ sub(x+succ(b), y)$

$$
\begin{aligned}
sub\Big(x, sub\big(y, succ(b)\big)\Big) &= sub\big(x, sub(y, b+1)\big) && (**)\\
&= sub\big(x, sub(y-1, b)\big) && \text{Lemma 2, } (*)\\
&= sub(x+b, y-1) && \text{Ind. Annahme}\\
&= sub\big((x+b)+1, y\big) && \text{Lemma 1}\\
&= sub\big(x+(b+1), y\big) && \text{Lemma 3}\\
&= sub\big(x+succ(b), y\big) && (**)
\end{aligned}
$$

2. Fall: $z < 0$: $z = pred^{n+1}(0)$, dann sei $b = pred^n(0)$ und $z = pred(b)$
Induktionsannahme: $sub(x, sub(y, b)) \;=\; sub(x+b, y)$
Zu zeigen: $sub(x, sub(y, pred(b))) \;=\; sub(x+pred(b), y)$

$$
\begin{aligned}
sub\Big(x, sub\big(y, pred(b)\big)\Big) &= sub\big(x, sub(y, b-1)\big) && (*)\\
&= sub\big(x, sub(y+1, b)\big) && \text{Lemma 1}\\
&= sub(x+b, y+1) && \text{Ind. Annahme}\\
&= sub\big((x+b)-1, y\big) && \text{Lemma 2}\\
&= sub\big(x+(b-1), y\big) && \text{Lemma 4}\\
&= sub\big(x+pred(b), y\big) && (*)
\end{aligned}
$$

□

Aufgabe 2 **Algebraische Spezifikation von Mengen [LÖSUNG]**

(a) Eine Art, Mengen zu klassifizieren, kann anhand der Eigenschaft erfolgen, ob ein Element nur einmal ($FINSET$) oder mehrfach ($MULTISET$) enthalten sein kann.

(b) Im Folgenden sind die Spezifikationen für einfache ($FINSET$) bzw. Mehrfachmengen ($MULTISET$) gegeben. Wesentliche Unterschiede bestehen bei den Einfüge-/Löschoperationenen für einzelne Elemente und den zugehörigen Axiomen bzw. bei der Überprüfung, ob ein Element in einer Menge enthalten ist oder nicht.

SPEC FINSET = {

based_on BOOL,
sort Fset α,

eset : Fset α,
add, del : Fset α, $\alpha \rightarrow$ Fset α,
iseset : Fset $\alpha \rightarrow$ Bool,
isel : Fset α, $\alpha \rightarrow$ Bool,

Fset α generated_by eset, add,

$\mathsf{iseset}(\mathsf{eset}) = \mathsf{true}$,
$\mathsf{iseset}\big(\mathsf{add}\ (s, x)\big) = \mathsf{false}$,
$\mathsf{isel}(\mathsf{eset}, x) = \mathsf{false}$,
$\mathsf{isel}\big(\mathsf{add}(s, x),\ x\big) = \mathsf{true}$,
$\mathsf{isel}(s,\ x) = \mathsf{true} \quad \Rightarrow \quad \mathsf{isel}\big(\mathsf{add}(s, y),\ x\big) = \mathsf{true}$,
$x \neq y \quad \Rightarrow \quad \mathsf{isel}\big(\mathsf{add}(s, y),\ x\big) = \mathsf{isel}(s, x)$,
$\mathsf{del}(\mathsf{eset}, x) = \mathsf{eset}$,
$\mathsf{del}\big(\mathsf{add}(s, x),\ x\big) = \mathsf{del}(s, x)$,
$x \neq y \quad \Rightarrow \quad \mathsf{del}\big(\mathsf{add}(s, y),\ x\big) = \mathsf{add}\big(\mathsf{del}(s, x),\ y\big)$,
$\mathsf{add}\big(\mathsf{add}(s, x),\ y\big) = \mathsf{add}\big(\mathsf{add}(s, y),\ x\big)$,
$\mathsf{isel}(s,\ x) = \mathsf{true} \quad \Rightarrow \quad \mathsf{add}(s,\ x) = s$

}

SPEC MULTISET = {

based_on BOOL,
sort Mset α,

emset : Mset α,
add, del : Mset α, $\alpha \rightarrow$ Mset α,
isemset : Mset $\alpha \rightarrow$ Bool,
isel : Mset α, $\alpha \rightarrow$ Bool,

Mset α generated_by emset, add,

$\mathsf{isemset}(\mathsf{emset}) = \mathsf{true}$,
$\mathsf{isemset}\big(\mathsf{add}(s, x)\big) = \mathsf{false}$,
$\mathsf{isel}(\mathsf{emset}, x) = \mathsf{false}$,
$\mathsf{isel}\big(\mathsf{add}(s, x), x\big) = \mathsf{true}$,
$\mathsf{isel}(s, x) = \mathsf{true} \quad \Rightarrow \quad \mathsf{isel}\big(\mathsf{add}(s, y), x\big) = \mathsf{true}$,
$x \neq y \quad \Rightarrow \quad \mathsf{isel}\big(\mathsf{add}(s, y), x\big) = \mathsf{isel}(s, x)$,
$\mathsf{del}(\mathsf{emset}, x) = \mathsf{emset}$,
$\mathsf{del}\big(\mathsf{add}(s, x), x\big) = s$,
$x \neq y \quad \Rightarrow \quad \mathsf{del}\big(\mathsf{add}(s, y), x\big) = \mathsf{add}\big(\mathsf{del}(s, x), y\big)$,
$\mathsf{add}\big(\mathsf{add}(s, x), y\big) = \mathsf{add}\big(\mathsf{add}(s, y), x\big)$

}

Aufgabe 3 Induktionsbeweis über Int [LÖSUNG]

Hier sollte das Theorem von Aufgabe 1(b) in seiner allgemeinen Form für alle $x, y, z \in Int$ betrachtet werden. Durch die gegebene Einschränkung $y, z \in Int, \quad 0 \leq z \leq y, \quad$ mussten in Aufgabe 1 für die Induktion nur Terme betrachtet werden mit der Form $\mathsf{succ}^n(0)$. Um zu zeigen, dass die Aussage für alle $x, y, z \in Int$ gilt müssen zusätzlich noch die Terme betrachtet werden, die mittels der verbleibenden Konstruktur-Funktion pred aufgebaut sind, also die Form $\mathsf{pred}^m(0)$ haben.
Der Beweis für derart aufgebaute Terme wurde unter Fall 2 der Lösung von Aufgabe 1(b) bereits behandelt.

Aufgabe 4 Induktionsbeweis über Nat [LÖSUNG]

Induktion über x:

- Induktionsanfang: $x = 0$
  Linke Seite der Implikation (*Prämisse*): $\neg\big(\mathsf{iszero}(0)\big) = false$
  Die Prämisse ist $false$, wodurch die gesamte Implikation $true$ wird und somit die Aussage für $x = 0$ gilt.

- Induktions-Schritt: $n \rightsquigarrow succ(n)$
  Ind. Ann.: Implikation gelte für $x = n$, also $\neg\big(\mathsf{iszero}(n)\big) \;\Rightarrow\; \mathsf{succ}\big(\mathsf{pred}(n)\big) = n$
  Z.z.: $\neg\Big(\mathsf{iszero}\big(succ(n)\big)\Big) \;\Rightarrow\; \mathsf{succ}\Big(\mathsf{pred}\big(\mathsf{succ}(n)\big)\Big) = \mathsf{succ}(n)$
  Prämisse ist $true$, da $\forall n : \;\; \mathsf{iszero}\big(succ(n)\big) = true$
  Rechte Seite ist $true$, da laut Axiom aus Int gilt: $\underbrace{\mathsf{succ}\Big(\mathsf{pred}\big(\mathsf{succ}(n)\big)\Big)}_{=\,\mathsf{succ}\;(n)} = \mathsf{succ}(n)$
  Somit ist die gesamte Implikation $true$, da von der Form: $true \rightarrow true$.

□