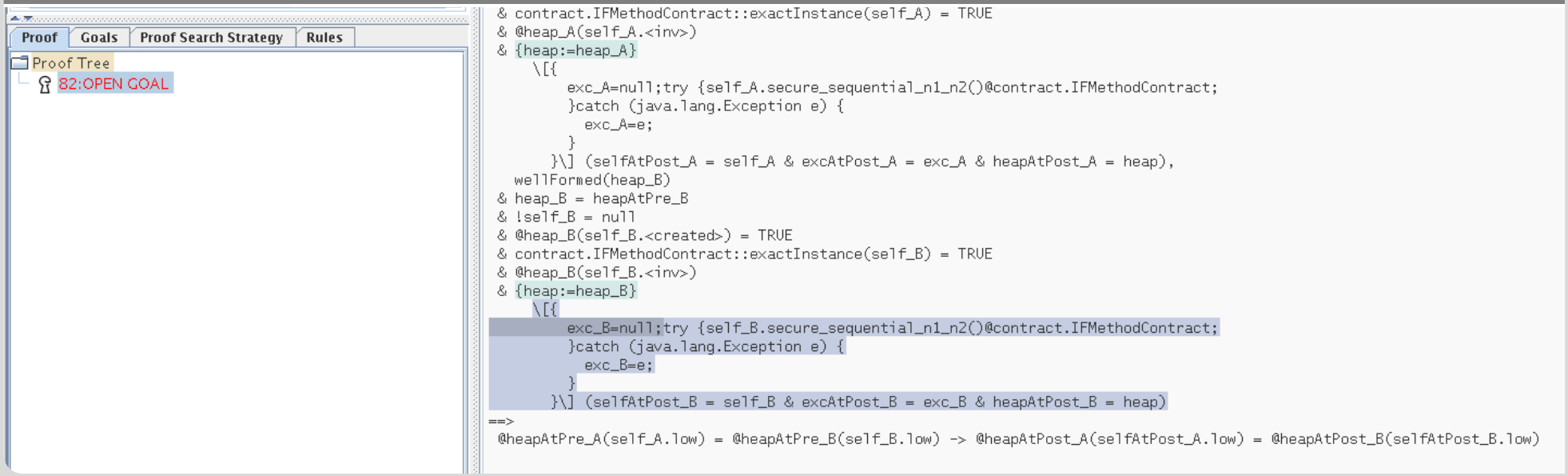
Karlsruhe Institute of Technology

Besprechung der zweiten Praxisaufgabe

Christoph Scheben

Institute for Theoretical Computer Science (ITI)



Aufgabe

Wir wollen aus

- den Peano-Axiomen sowie
- der Definition der Fibonacci-Zahlen

ableiten, dass

für alle natürlichen Zahlen n, m
die $(n + m + 1)$-te Fibonacci-Zahl der Summe aus

- dem Produkt der n-ten und m-ten Fibonacci-Zahl und
- dem Produkt der $(n + 1)$-ten und $(m + 1)$-ten Fibonacci-Zahl

entspricht.

Formalisierung

Signatur

- Die Prädikatenlogik in KeY ist eine sortierte Logik.
- Wir betrachten nur die Sorte nat.

Funktionen

$zero$	:	$\rightarrow nat$
one	:	$\rightarrow nat$
$plus$	:	$nat \times nat \rightarrow nat$
$times$	:	$nat \times nat \rightarrow nat$
fib	:	$nat \rightarrow nat$

Formalisierung

Axiome

Die Funktionen *plus*, *times* und *fib* sind durch folgende Axiome festgelegt:

Peano-Arithmetik (ohne Induktionsschema)

$$\forall\ nat\ x \qquad \neg plus(x, one) \doteq zero$$
$$\forall\ nat\ x \quad \forall\ nat\ y \qquad plus(x, one) \doteq plus(y, one) \rightarrow x \doteq y$$
$$\forall\ nat\ x \qquad plus(x, zero) \doteq x$$
$$\forall\ nat\ x \quad \forall\ nat\ y \qquad plus(x, plus(y, one)) \doteq plus(plus(x, y), one)$$
$$\forall\ nat\ x \qquad times(x, zero) \doteq zero$$
$$\forall\ nat\ x \quad \forall\ nat\ y \qquad times(x, plus(y, one)) \doteq plus(times(x, y), x)$$

Fibonacci-Axiome

$$fib(zero) \doteq zero$$
$$fib(one) \doteq one$$
$$\forall\ nat\ n \qquad fib(plus(n, plus(one, one))) \doteq (plus(fib(n), fib(plus(n, one))))$$

Formalisierung

Induktionsschema / Induktionsregel

Anstatt des Axiomenschemas für die Induktion

$$(\phi(0) \wedge \forall y(\phi(y) \rightarrow \phi(y+1))) \rightarrow \forall x(\phi) \text{ für jede Formel } \phi$$

verwenden wir folgende äquivalente Sequenzenkalkülregel:

$$\frac{\begin{array}{lll} \Gamma & \Longrightarrow \{n/zero\}\varphi,\ \Delta & (1) \\ \Gamma & \Longrightarrow \forall\ nat\ n\ (\varphi \rightarrow \{n/plus(n,one)\}\varphi),\ \Delta & (2) \end{array}}{\Gamma \Longrightarrow \forall\ nat\ n\ \varphi,\ \Delta\ (3)}\ \text{(induction\_on\_naturals)}$$

Um eine Aussage (3) über die natürlichen Zahlen mittels vollständiger Induktion zu beweisen, muss

- der Induktionsanfang (1) (engl. "*Base Case*") und
- der Induktionsschritt (2) (engl. "*Step Case*")

gezeigt werden.

Formalisierung

Hinweis

Wir definieren hier in klassischer Weise einen abstrakten Datentypen.

Formalisierung

Die eigentliche Aussage

Die Aussage

> Für alle natürlichen Zahlen n, m entspricht
> die $(n+m+1)$-te Fibonacci-Zahl der Summe aus
> - dem Produkt der n-ten und m-ten Fibonacci-Zahl und
> - dem Produkt der $(n+1)$-ten und $(m+1)$-ten Fibonacci-Zahl.

"entspricht"

$$\forall\ nat\ n \quad \forall\ nat\ m \qquad fib(plus(n, plus(m, one))) \doteq plus(times(fib(n), fib(m)), times(fib(plus(n, one)), fib(plus(m, one))))$$

Wir Wollen Zeigen

$$\{\text{Peano-Arithmetik (mit Induktionsschema / Induktionsregel),}\ \text{Fibonacci-Axiome}\}$$

$$\models$$

$$\forall\ nat\ n \quad \forall\ nat\ m \qquad fib(plus(n, plus(m, one)))$$
$$\doteq\ plus(times(fib(n), fib(m)),$$
$$times(fib(plus(n, one)), fib(plus(m, one))))$$

Wiederholung

Definition (Folgerbarkeit)

Es sei

- M eine Menge von Formeln aus For und
- A eine einzelne Formel aus For,

wobei weder in M noch in A freie Variablen vorkommen.

$$M \models A \quad :\Leftrightarrow \quad \text{Jedes Modell von } M \text{ ist auch Modell von } A.$$

Lies: Aus M folgt A (über Σ).

Hinweis

- $\mathbb{N}$ ist **ein** Modell der Peano-Arithmetik.
  $\rightsquigarrow$ Es gibt aber noch andere (Nichtstandard-)Modelle.
- D. h. falls

$$\{\text{Peano-Arithmetik (mit Induktionsschema / Induktionsregel), Fibonacci-Axiome}\} \models$$

$$\forall\, nat\ n \quad \forall\, nat\ m \qquad fib(plus(n, plus(m, one))) \doteq plus(times(fib(n), fib(m)), times(fib(plus(n, one)), fib(plus(m, one))))$$

gilt, dann gilt auch:

Für alle natürlichen Zahlen n, m entspricht
die $(n + m + 1)$-te Fibonacci-Zahl der Summe aus

- dem Produkt der n-ten und m-ten Fibonacci-Zahl und
- dem Produkt der $(n + 1)$-ten und $(m + 1)$-ten Fibonacci-Zahl.

(Aber nicht notwendiger Weise anders herum.)

Wir Zeigen

... mit dem Sequenzenkalkül

$$\{\text{Peano-Arithmetik (mit Induktionsschema / Induktionsregel),}\ \text{Fibonacci-Axiome}\} \vdash$$

$$\forall\ nat\ n \quad \forall\ nat\ m \qquad fib(plus(n, plus(m, one))) \doteq plus(times(fib(n), fib(m)), times(fib(plus(n, one)), fib(plus(m, one))))$$

Warum ist das ok?

Wegen der Korrektheit des Sequenzenkalküls:

$$M \vdash A \Rightarrow M \models A$$

Hinweis:

Der Sequenzenkalkül ist (natürlich?) auch vollständig:

$$M \models A \Rightarrow M \vdash A$$

Wobei: Eigentlich Zeigen Wir

... mit dem Sequenzenkalkül

$$\{\text{Induktionsschema / Induktionsregel}\}$$
$$\vdash$$
$$\bigwedge \text{Peano-Arithmetik}$$
$$\wedge \bigwedge \text{Fibonacci-Axiome}$$
$$\rightarrow \forall\ nat\ n \quad \forall\ nat\ m \qquad fib(plus(n, plus(m, one)))$$
$$\doteq\ plus(times(fib(n), fib(m)),$$
$$times(fib(plus(n, one)), fib(plus(m, one))))$$

Warum ist das ok?

Weil in Prädikatenlogik erster Stufe

$$M \models A \to B \quad \Rightarrow \quad M \cup \{A\} \models B$$

gilt ($\rightsquigarrow$ Modus Ponens).

Sequenzenkalkül

Definitionen

Definition (Sequenz)

Eine Sequenz wird notiert als eine Folge zweier endlicher Mengen prädikatenlogischer Formeln getrennt durch das Symbol $\Longrightarrow$:

$$\Gamma \Longrightarrow \Delta$$

Γ wird Antezedent und Δ Sukzedent genannt. Sowohl links wie rechts vom Sequenzenpfeil $\Longrightarrow$ kann auch die leere Menge stehen.

Definition (Auswertung von Sequenzen)

Sei $\mathcal{D}$ eine prädikatenlogische Struktur und β eine Variablenbelegung:

$$val_{\mathcal{D},\beta}(\Gamma \Longrightarrow \Delta) = val_{\mathcal{D},\beta}(\bigwedge \Gamma \rightarrow \bigvee \Delta)$$

Es gelten die üblichen Vereinbarungen für leere Disjunktionen und Konjunktionen.

Sequenzenkalkül

Axiome und Regeln

Karlsruhe Institute of Technology

axiom $\dfrac{}{\Gamma, F \Longrightarrow F, \Delta}$

0Left $\dfrac{}{\Gamma, \mathbf{0} \Longrightarrow \Delta}$

1Right $\dfrac{}{\Gamma \Longrightarrow \mathbf{1}, \Delta}$

notLeft $\dfrac{\Gamma, \Longrightarrow F, \Delta}{\Gamma, \neg F \Longrightarrow \Delta}$

notRight $\dfrac{\Gamma, F \Longrightarrow \Delta}{\Gamma \Longrightarrow \neg F, \Delta}$

implLeft $\dfrac{\Gamma \Longrightarrow F, \Delta \quad \Gamma, G \Longrightarrow \Delta}{\Gamma, F \to G \Longrightarrow \Delta}$

implRight $\dfrac{\Gamma, F \Longrightarrow G, \Delta}{\Gamma \Longrightarrow F \to G, \Delta}$

andLeft $\dfrac{\Gamma, F, G \Longrightarrow \Delta}{\Gamma, F \wedge G \Longrightarrow \Delta}$

andRight $\dfrac{\Gamma \Longrightarrow F, \Delta \quad \Gamma \Longrightarrow G, \Delta}{\Gamma \Longrightarrow F \wedge G, \Delta}$

orLeft $\dfrac{\Gamma, F \Longrightarrow \Delta \quad \Gamma, G \Longrightarrow \Delta}{\Gamma, F \vee G \Longrightarrow \Delta}$

orRight $\dfrac{\Gamma \Longrightarrow F, G, \Delta}{\Gamma \Longrightarrow F \vee G, \Delta}$

Sequenzenkalkül

Axiome und Regeln

allLeft $$\frac{\Gamma, \forall x F, F(x/X) \Longrightarrow \Delta}{\Gamma, \forall x F \Longrightarrow \Delta}$$

wobei X eine neue Variable ist.

allRight $$\frac{\Gamma \Longrightarrow F(x/f(x_1, \ldots, x_n)), \Delta}{\Gamma \Longrightarrow \forall x F, \Delta}$$

wobei f ein neues Funktionssymbol ist und $x_1, \ldots, x_n$ alle freien Variablen in $\forall x F$.

exRight $$\frac{\Gamma \Longrightarrow \exists x F, F(x/X), \Delta}{\Gamma, \Longrightarrow \exists x F, \Delta}$$

wobei X eine neue Variable ist.

exLeft $$\frac{\Gamma, F(x/f(x_1, \ldots, x_n)) \Longrightarrow \Delta}{\Gamma, \exists x F \Longrightarrow \Delta}$$

wobei f ein neues Funktionssymbol ist und $x_1, \ldots, x_n$ alle freien Variablen in $\exists x F$.

Sequenzenkalkül

Axiome und Regeln

$$\text{identity}\ \frac{}{\Gamma \Longrightarrow s \doteq s, \Delta}$$

$$\text{symmetryRight}\ \frac{\Gamma \Longrightarrow s \doteq t, \Delta}{\Gamma \Longrightarrow t \doteq s, \Delta}$$

$$\text{symmetryLeft}\ \frac{\Gamma, s \doteq t \Longrightarrow \Delta}{\Gamma, t \doteq s \Longrightarrow \Delta}$$

$$\text{eqSubstRight}\ \frac{\Gamma, s \doteq t \Longrightarrow F(t), \Delta}{\Gamma, s \doteq t \Longrightarrow F(s), \Delta}$$

$$\text{eqSubstLeft}\ \frac{\Gamma, F(t), s \doteq t \Longrightarrow \Delta}{\Gamma, F(s), s \doteq t \Longrightarrow \Delta}$$

Sequenzenkalkül

Beispiel Ableitung

$$\frac{}{\Longrightarrow (\forall nat\, x;\ p(x)) \rightarrow (p(c) \wedge p(d))}$$

Sequenzenkalkül

Beispiel Ableitung

$$\text{implRight}\ \frac{\dfrac{}{\forall nat\, x;\ p(x) \Longrightarrow p(c) \wedge p(d)}}{\Longrightarrow (\forall nat\, x;\ p(x)) \rightarrow (p(c) \wedge p(d))}$$

Sequenzenkalkül

Beispiel Ableitung

$$\text{implRight}\ \dfrac{\text{andRight}\ \dfrac{\dfrac{}{\forall nat\, x;\ p(x) \Longrightarrow p(c)} \qquad \dfrac{}{\forall nat\, x;\ p(x) \Longrightarrow p(d)}}{\forall nat\, x;\ p(x) \Longrightarrow p(c) \wedge p(d)}}{\Longrightarrow (\forall nat\, x;\ p(x)) \rightarrow (p(c) \wedge p(d))}$$

Sequenzenkalkül

Beispiel Ableitung

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\forall nat\, x;\ p(x),\ p(c) \Longrightarrow p(c)}}{\forall nat\, x;\ p(x) \Longrightarrow p(c)}\,\text{allLeft} \qquad \dfrac{}{\forall nat\, x;\ p(x) \Longrightarrow p(d)}}{\forall nat\, x;\ p(x) \Longrightarrow p(c) \wedge p(d)}\,\text{andRight}}{\Longrightarrow (\forall nat\, x;\ p(x)) \rightarrow (p(c) \wedge p(d))}\,\text{implRight}$$

Sequenzenkalkül

Beispiel Ableitung

$$\dfrac{\dfrac{\dfrac{\dfrac{*}{\forall nat\, x;\ p(x),\ p(c) \Longrightarrow p(c)}\,\text{axiom}}{\forall nat\, x;\ p(x) \Longrightarrow p(c)}\,\text{allLeft} \qquad \dfrac{}{\forall nat\, x;\ p(x) \Longrightarrow p(d)}}{\forall nat\, x;\ p(x) \Longrightarrow p(c) \wedge p(d)}\,\text{andRight}}{\Longrightarrow (\forall nat\, x;\ p(x)) \rightarrow (p(c) \wedge p(d))}\,\text{implRight}$$

Sequenzenkalkül

Beispiel Ableitung

$$\dfrac{\dfrac{\dfrac{\dfrac{*}{\forall nat\, x;\ p(x),\ p(c) \Longrightarrow p(c)}\,\text{axiom}}{\forall nat\, x;\ p(x) \Longrightarrow p(c)}\,\text{allLeft} \qquad \dfrac{\dfrac{}{\forall nat\, x;\ p(x),\ p(d) \Longrightarrow p(d)}\,\text{axiom}}{\forall nat\, x;\ p(x) \Longrightarrow p(d)}\,\text{allLeft}}{\forall nat\, x;\ p(x) \Longrightarrow p(c) \wedge p(d)}\,\text{andRight}}{\Longrightarrow (\forall nat\, x;\ p(x)) \rightarrow (p(c) \wedge p(d))}\,\text{implRight}$$

Sequenzenkalkül

Beispiel Ableitung

$$\dfrac{\dfrac{\dfrac{*}{\forall nat\, x;\ p(x),\ p(c) \Longrightarrow p(c)}\,\text{axiom}}{\forall nat\, x;\ p(x) \Longrightarrow p(c)}\,\text{allLeft} \qquad \dfrac{\dfrac{*}{\forall nat\, x;\ p(x),\ p(d) \Longrightarrow p(d)}\,\text{axiom}}{\forall nat\, x;\ p(x) \Longrightarrow p(d)}\,\text{allLeft}}{\dfrac{\forall nat\, x;\ p(x) \Longrightarrow p(c) \wedge p(d)}{\Longrightarrow (\forall nat\, x;\ p(x)) \rightarrow (p(c) \wedge p(d))}\,\text{implRight}}\,\text{andRight}$$

Verifikation in KeY

example.key

addcomm.key

fib.key

fibTaclet.key

fibOnInt.key

Karlsruhe Institute of Technology

Das ist das Ende!