Korrekte Software: Grundlagen und Methoden
Vorlesung 11 vom 20.06.22
Funktionen und Prozeduren II

Serge Autexier, Christoph Lüth

Universität Bremen

Sommersemester 2024

Fahrplan

Modellierung und Spezifikation von Funktionen

Wir brauchen:

1. Von Anweisungen zu Funktionen: Deklarationen und Parameter ✓
2. Semantik von Funktionsdefinitionen ✓
3. Spezifikation von Funktionsdefinitionen ✓
4. Beweisregeln für Funktionsdefinitionen ✓
5. Semantik des Funktionsaufrufs
6. Beweisregeln für Funktionsaufrufe

Funktionsaufrufe und Rückgaben

Neue Ausdrücke und Anweisungen:

- Funktionsaufrufe
- Prozeduraufrufe (mit Zuweisung eines Rückgabewertes)

$$\begin{aligned}
\textbf{Aexp}\ a &::= \mathbf{Z} \mid \mathbf{C} \mid \mathbf{Lexp} \mid a_1 + a_2 \mid a_1 - a_2 \mid a_1 * a_2 \mid a_1/a_2 \\
\textbf{Bexp}\ b &::= \mathbf{1} \mid \mathbf{0} \mid a_1 == a_2 \mid a_1 < a_2 \mid !\, b \mid b_1 \,\&\&\, b_2 \mid b_1 \,||\, b_2 \\
\textbf{Exp}\ e &:= \mathbf{Aexp} \mid \mathbf{Bexp} \\
\textbf{Stmt}\ c &::= l = e \mid c_1; c_2 \mid \{\,\} \mid \textbf{if}\ (b)\ c_1\ \textbf{else}\ c_2 \\
&\quad \mid \textbf{while}\ (b)\ /{*}{*}\ \textbf{inv}\ a\ {*}/\ c \mid /{*}{*}\ \{a\}\ {*}/ \\
&\quad \mid \mathbf{Idt}(a^*) \\
&\quad \mid l = \mathbf{Idt}(a^*) \\
&\quad \mid \textbf{return}\ a^?
\end{aligned}$$

Zur Erinnerung: Semantik von Funktionsdefinitionen

$$[\![.]\!]_{fd} : \mathbf{FunDef} \to \mathbf{Env} \to \mathbf{V}^n \rightharpoonup \Sigma \rightharpoonup \Sigma \times \mathbf{V}_U$$

- Das Denotat einer Funktion ist eine Anweisung, die über den tatsächlichen Werten für die Funktionsargumente parametriert ist.
  $[\![f(t_1\ p_1, t_2\ p_2, \ldots, t_n\ p_n)\ ds\ c]\!]_{fd}\ \Gamma\ v_1, \ldots, v_n = [\![(t_1\ p_1\ v_1, t_2\ p_2\ v_2, \ldots, t_n\ p_n\ v_n, ds)\ c]\!]_{blk}\ \Gamma$
- **Aufruf** der Funktion $f(e_1, \ldots, e_n)$ mit Argumenten $e_1, \ldots, e_n$:
  - **Auswertung** der Argumente $v_i = [\![e_i]\!]_{\mathcal{A}}$
  - Einsetzen in die **Semantik** $[\![f]\!]_{fd}(v_1, \ldots, v_n)$

Seiteneffekte bei Funktionsaufrufe

- Seiteneffekte:
  - Funktionen mit Seiteneffekten in zusammengesetzten Ausdrücken sind problematisch
  - In Java ist die Auswertungsreihenfolge fest (links nach rechts)
  - In C unspezifiziert (!)
- Deshalb keine Funktionen in zusammengesetzten Ausdrücken.
- Funktionsaufrufe nur in zwei Formen:
  - Als reine Prozeduren ($\mathbf{Idt}(a^*)$) vom Typ **void**
  - Als direkte Zuweisung ($l = \mathbf{Idt}(a^*)$) des Rückgabewertes
- Call by name, call by value, call by reference. . . ?

Arbeitsblatt 11.1: Funktionsaufrufe

Wie werden Parameter in folgenden Programmiersprachen übergeben?

- **C:**
- **Java**:
- **Haskell**:
- **Python**:
- **Other:** (specify)

Funktionsaufrufe

- Um eine Funktion f aufzurufen, müssen wir (statisch!) die Semantik der **Definition** von f dem Bezeichner f zuordnen.
- Aufruf einer nicht-definierten Funktion f oder mit falscher Anzahl n von Parametern ist nicht definiert
  - Muss durch **statische Analyse** verhindert werden
- Deshalb muss die **Umgebung** erweitert werden:

$$\mathbf{Env} = \mathbf{Idt} \rightharpoonup \mathbf{LocEnv} \qquad = \mathbf{Idt} \rightharpoonup (\mathbf{Loc} + (\mathbf{V}^N \rightharpoonup \Sigma \rightharpoonup (\Sigma \times \mathbf{V}_u)))$$

- Wir haben hier den selben einen **Namensraum** für Funktionen und Variablen.

Semantik von Funktionsaufrufen

- Gegegeben Funktionsbezeichner f, Semantik ist

$$\Gamma(f) = \{(\underbrace{(v_1,\ldots,v_n)}_{\text{Parameterwerte}}, (\underbrace{\sigma}_{\text{Anfangszustand}}, \underbrace{(\sigma', a)}_{\text{Endzustand, Rückgabewert}}))\}$$

- Damit:

$$[\![f(t_1,\ldots,t_n)]\!]^\Gamma_{\mathcal{C}} = \{(\sigma,\sigma') \mid ((v_1,\ldots,v_n),\sigma,(\sigma',a)) \in \Gamma(f) \wedge (\sigma, v_i) \in [\![t_i]\!]^\Gamma_{\mathcal{A}}\}$$
$$[\![x = f(t_1,\ldots,t_n)]\!]^\Gamma_{\mathcal{C}} = \{(\sigma,\sigma'[x \mapsto a]) \mid ((v_1,\ldots,v_n),\sigma,(\sigma',a)) \in \Gamma(f) \wedge (\sigma, v_i) \in [\![t_i]\!]^\Gamma_{\mathcal{A}}\}$$

- Aufruf einer Prozedur $[\![f(t_1,\ldots,t_n)]\!]_{\mathcal{C}}$ ignoriert Rückgabewert
  - Somit: Kombination mit Zuweisung
- Wir modellieren nur call-by-value.
  - C kennt nur call by value, allerdings sind Referenzen auch Werte (kommt noch)

Umgebung für den Kalkül

- Für Funktionsaufrufe gibt es eine **Umgebung**:

$$\mathbf{Env} = \mathbf{Idt} \rightharpoonup (\mathbf{Loc} + (\mathbf{V}^N \rightharpoonup \Sigma \rightharpoonup (\Sigma \times \mathbf{V}_u)))$$

- Deshalb muss für den Kalkül eine **Umgebung** Δ Funktionsbezeichnern ihre **Spezifikation** (Vor- und Nachbedingung, sowie Parameter) zuordnen:

$$\mathbf{Env}_{\text{fun}} = \mathbf{Idt} \rightharpoonup (\mathbf{Idt}^N \times \mathbf{Assn} \times \mathbf{Assn})$$

- $\Delta(f) = \forall x_1,\ldots,x_n.(P,Q)$, für $f(x_1,\ldots,x_n)$/** pre P post Q */
- Korrektheit gilt immer nur im **Kontext** einer Umgebung, dadurch kann jede Funktion separat verifiziert werden (**Modularität**).
  - Umgebung wird zusätzliches Argument der Regeln.
  - Notation: $\Delta \vdash \{P\}\, c\, \{Q \mid Q_R\}$.

Erweiterung des Floyd-Hoare-Kalküls: Aufruf

$$\frac{\Delta(f) = \forall x_1,\ldots,x_n.(P,Q)}{\Delta \vdash \{P[t_i/x_i]\}\, l = f(t_1,\ldots,t_n)\, \{Q[t_i/x_i][l/\backslash\mathbf{result}] \mid Q_R\}}$$

- Δ muss f mit der Vor-/Nachbedingung P, Q enthalten
- In P und Q werden Parameter x_i durch Argumente t_i ersetzt.
- $\backslash$**result** in Q wird durch l ersetzt

Beispiel: die Fakultätsfunktion, rekursiv

```
1  int fac(int x)
2  /** pre  0 ≤ x;
3      post \result = x!; */
4  {
5   int r = 0;
6
7   // {(x = 0 ∧ 1 = x @pre!) ∨ (x ≠ 0 ∧ 0 ≤ x − 1)}
8   if (x == 0) {
9     // {1 = x @pre!}
10    return 1;
11    // {0 ≤ x − 1 | \result = x @pre!}
12    } else {
13    // {0 ≤ x − 1}
14    }
15  // {0 ≤ x − 1}
16  r = fac(x− 1);
17  // {r = (x − 1)!}
18  // {r · x = x @pre!}
19  return r* x;
20  // {false | \result = x @pre!}
21 }
```

Verifikationsbedingungen:

(1) $0 \le x \wedge x = x\,\texttt{@pre} \longrightarrow (x = 0 \wedge 1 = x\,\texttt{@pre!}) \vee (x \neq 0 \wedge 0 \le x - 1)$

(1.1) $0 \le x \wedge x = x\,\texttt{@pre} \wedge x = 0 \longrightarrow 1 = x\,\texttt{@pre!}$ ✓

(1.2) $0 \le x \wedge x = x\,\texttt{@pre} \wedge x \neq 0 \longrightarrow 0 \le x - 1$ ✓

(2) $r = (x-1)! \longrightarrow r \cdot x = x\,\texttt{@pre!}$

Problem: Beweis von (2) benötigt Voraussetzung $x = x$ **@pre**!

Beobachtungen

- Bei der Verifikation von f muss die Spezifikation von f Teil des Kontextes sein.
- Wir brauchen **gar keine** Invariante — ist durch die Nachbedingung gegeben
- Rekursion benötigt keine Extrabehandlung
  - Termination von rekursiven Funktionen wird extra gezeigt
- Der Aufruf einer Funktion **ersetzt** die momentane Nachbedingung — das ist ein Problem!

Frame Rule

- Konstanzregel (Rule of Constancy):

$$\frac{\Delta \vdash \{P\}\, c\, \{Q \mid Q_R\}}{\Delta \vdash \{P \wedge R\}\, c\, \{Q \wedge R \mid Q_R\}}$$

- Nebenbedingung:
  - c verändert keine Variablen in R, **oder**
  - für **keine** der Programm-Variablen x, die in R vorkommen, gibt es eine Zuweisung $x = \ldots$ in c
- Das ist eine **neue Regel**, die **bewiesen** werden muss.
- Schwierig zu handhaben bei Rückwärtsrechnung: R muss **annotiert** werden.

Funktionsaufrufe und Rückgaben

Neue Ausdrücke und Anweisungen:

- Funktionsaufrufe mit Zuweisung eines Rückgabewertes

$$\begin{aligned}
\textbf{Stmt}\ c ::=\ & l = e \mid c_1; c_2 \mid \{\,\} \mid \textbf{if}\ (b)\ c_1\ \textbf{else}\ c_2 \\
\mid\ & \textbf{while}\ (b)\ /{*}{*}\ \textbf{inv}\ a\ {*}/\ c \mid /{*}{*}\ \{a\}\ {*}/ \\
\mid\ & \mathbf{Idt}(a^*) \\
\mid\ & /{*}{*}\,\textbf{const}\ R\ {*}/\ l = \mathbf{Idt}(a^*) \\
\mid\ & \textbf{return}\ a^?
\end{aligned}$$

Approximative schwächste Vorbedingung & Verifikationsbedingung für Funktionsaufrufe

Sei $\Delta(f) = \forall x_1,\ldots,x_n.(P,Q)$

$$\text{awp}(\Delta, /{*}{*}\,\textbf{const}\ R\ {*}/ l = f(t_1,\ldots,t_n), U, U_R) \stackrel{def}{=} R \wedge P[t_i/x_i] \quad \text{wenn } l \notin FV(R)$$

$$\text{wvc}(\Delta, /{*}{*}\,\textbf{const}\ R\ {*}/ l = f(t_1,\ldots,t_n), U, U_R) \stackrel{def}{=} \{R \wedge Q[t_i/x_i][l/\backslash\mathbf{result}] \longrightarrow U\} \quad \text{wenn } l \notin FV(R)$$

Beispiel: die Fakultätsfunktion

```
1  int fac(int x)
2  /** pre   0 ≤ x;
3      post  \result = x!; */
4  {
5   int r = 0;
6
7   // {(x = 0 ∧ 1 = x@pre!) ∨ (x ≠ 0 ∧ 0 ≤ x − 1 ∧ x = x@pre)}
8   if (x == 0) {
9     // {1 = x@pre!}
10    return 1;
11    // {0 ≤ x − 1 ∧ x = x@pre | \result = x@pre!}
12    } else {
13    // {0 ≤ x − 1 ∧ x = x@pre}
14    }
15  // {0 ≤ x − 1 ∧ x = x@pre}
16  /** const x= x@pre */ r = fac(x− 1);
17  // {r · x = x@pre!}
18  return r* x;
19  // {false | \result = x@pre!}
20 }
```

Verifikationsbedingungen:

(1) $0 \le x \wedge x = x\,@\mathbf{pre} \longrightarrow (x = 0 \wedge 1 = x\,@\mathbf{pre}!) \vee (x \neq 0 \wedge 0 \le x - 1 \wedge x = x\,@\mathbf{pre})$

(1.1) $0 \le x \wedge x = x\,@\mathbf{pre} \wedge x = 0 \longrightarrow 1 = x!$ ✓

(1.2) $0 \le x \wedge x = x\,@\mathbf{pre} \wedge x \neq 0 \longrightarrow 0 \le x - 1$ ✓

(1.3) $0 \le x \wedge x = x\,@\mathbf{pre} \wedge x \neq 0 \longrightarrow x = x\,@\mathbf{pre}$ ✓

(2) $x = x\,@\mathbf{pre} \wedge r = (x-1)! \longrightarrow r \cdot x = x\,@\mathbf{pre}!$ ✓

Arbeitsblatt 11.2: Fakultät endrekursiv

Hier nochmal die Fakultät (endrekursiv und buggy):

```
int factorial(int n)
/** pre ???;
    post ???; */
{
  int f;

  f= fact(0, n);
  return f;

}

int fact(int acc, int n)
/** pre ???;
    post ???; */
{
  int r;

  if (n == 0) return 1;
  r= fact(acc* n, n−1);
  return r;
}
```

1. Annotiert das Programm mit Vor/Nachbedingungen.
2. Findet und berichtigt die Fehler.
3. Berechnet die Verifikationsbedingungen.
4. Beweist die Verifikationsbedingungen.

Zusammenfassung

- Funktionen sind **zentrales Modularisierungskonzept**
- Behandlung von Funktionen erfordert **vielfältige Erweiterungen**
- Erweiterung der **Semantik:**
  - Erweiterung der Semantik um **Rückgabezustand** $\Sigma \rightharpoonup (\Sigma \cup \Sigma \times \mathbf{V}_U)$
  - Die Semantik einer Funktion ist **parametrisiert** $\mathbf{V}^n \rightharpoonup \Sigma \rightharpoonup \Sigma \times \mathbf{V}_U$
- Erweiterung der **Spezifikationen:**
  - Spezifikation von Funktionen: **Vor-/Nachzustand** statt logischer Variablen
- Erweiterung des **Hoare-Kalküls**:
  - **Gesonderte Nachbedingung** für Rückgabewert/Endzustand
  - Aufruf einer Funktion **ersetzt** Vor/Nachbedingung, daher **Framing**
- **Einschränkungen**: nur call-by-value
- Fazit: **ohne Referenzen** sind Funktionen wenig brauchbar