ALP2 SS 2012
Prof. Dr. Margarita Esponda-Argüero
Thema: Hoare-Kalkül

2. Vorlesungsbeispiel am 24.05.2012

Gegeben sei das folgende Python-Programm, das bei Eingabe einer positiven natürlichen Zahl **n**, die Summe aller Zahlen von **1** bis **n** berechnet.

```
n = int ( input( 'n=' ))  # Eingabe

i = 1

sum = 0

while i <= n:

        sum = sum + i

        i = i + 1
```

Wir lassen den Eingabe-Teil außer acht und möchten die Gültigkeit folgender Programmformel beweisen:

$$\{P\} \equiv \{n > 0\}$$

```
i = 1
sum = 0
while i <= n:
        sum = sum + i
        i = i + 1
```

$$\{Q\} \equiv \left\{ sum == \frac{n \cdot (n+1)}{2} \right\} \qquad \text{. . . . . } \mathbf{(0)}$$

Wir hätten damit nur die partielle Korrektheit unseres Programms bewiesen. Das bedeutet, dass, wenn die Schleife terminiert, das Programm für alle positiven Zahlen ein richtiges Ergebnis liefern würde.

Zuerst müssen wir eine Invariante für unsere **while**-Schleife finden und wählen

folgende Invariante:

$$\{INV\} \equiv \left\{ sum == \frac{i(i-1)}{2} \right\}$$

und möchten zeigen, dass $sum == \frac{i(i-1)}{2}$ eine Invariante der **while**-Schleife ist.

Das bedeutet, wir müssen zuerst zeigen, dass die Formel **(1)** gilt:

$$\{P\} \equiv \{n > 0\}$$

```
i = 1
sum = 0
```

$$\{INV\} \equiv \left\{(sum == \frac{i(i-1)}{2})\right\}$$

```
while i<=n:
    sum = sum + i
    i = i + 1
```

$$\{INV \wedge \neg B\} \equiv \left\{sum == \frac{i(i-1)}{2} \wedge (i > n\right\} \qquad \text{. . . . . } \textbf{(1)}$$

$$\{Q\} \equiv \left\{sum == \frac{n \cdot (n+1)}{2}\right\}$$

Wir müssen dann nach der **while**-Regel zeigen, dass

$$\{INV \wedge B\} \equiv \left\{(sum == \frac{i(i-1)}{2}) \wedge (i \leq n)\right\}$$

```
sum = sum + i
i  = i + 1
```

$$\{INV\} \equiv \left\{sum == \frac{i(i-1)}{2}\right\} \qquad \text{. . . . . } \textbf{(2)}$$

gültig ist.

Gemäß der Sequenzregel ist **(2)** gültig, wenn wir ein Prädikat ***R*** finden, sodass folgende Programmformeln

$$\left\{(sum == \frac{i(i-1)}{2}) \wedge (i \leq n)\right\}$$

```
sum = sum + i
```

$$\{R\} \qquad \text{. . . . . } \textbf{(3)}$$

```
i   = i + 1
```

$$\left\{sum == \frac{i(i-1)}{2}\right\} \qquad \text{. . . . . } \textbf{(4)}$$

gelten.

Nach dem Zuweisungsaxiom gilt:

$$\{R\} \equiv \left\{ sum == \frac{(i+1)((i+1)-1)}{2} \right\} \Leftrightarrow \left\{ sum == \frac{(i+1)i}{2} \right\}$$

i = i + 1

$$\left\{ sum == \frac{i(i-1)}{2} \right\} \qquad \text{. . . . .} \quad \textbf{(4)}$$

Wenn wir das Zuweisungsaxiom noch einmal anwenden, erhalten wir in **(3)** als Vorbedingung das Prädikat $\{R'\}$

$$\{R'\} \equiv \left\{ (sum+i) == \frac{(i+1)i}{2} \right\}$$

sum = sum + i

$$\{R\} \equiv \left\{ sum == \frac{(i+1)i}{2} \right\},$$

aber

$$\{R'\} \equiv \left\{ (sum+i) == \frac{(i+1)i}{2} \right\} \Leftrightarrow \left\{ sum == \frac{(i+1)i}{2} - i \right\}$$

$$\Leftrightarrow \left\{ sum == \frac{(i+1)i}{2} - \frac{2i}{2} \right\}$$

$$\Leftrightarrow \left\{ sum == \frac{i(i-1)}{2} \right\}$$

mit folgender logischer Implikation,

$$\left\{ (sum == \frac{i(i-1)}{2}) \wedge (i \leq n) \right\} \Rightarrow \left\{ sum == \frac{i(i-1)}{2} \right\} \equiv \{R'\}$$

und nach der zweiten Konsequenz-Regel erhalten wir die Gültigkeit von **(3),** und damit ist nach der Sequenz-Regel und der **while**-Regel gezeigt, dass

$$INV \equiv sum == \frac{i(i-1)}{2}$$

eine Invariante der **while**-Schleife ist.

Leider können wir mit dieser Invariante die partielle Korrektheit des Programms nicht zeigen. Um die partielle Korrektheit des Programms zu beweisen, müssen wir zunächst einmal die Invariante der **while**-Schleife wie folgt ergänzen:

$$INV2 \equiv sum == \frac{i(i-1)}{2} \wedge i \leq (n+1)$$

Wir müssen dann beweisen, dass INV2 auch eine gültige Invariante der Schleife ist.
D.h. nach der **while**-Regel müssen wir zeigen, dass

$$\{INV2 \wedge B\} \equiv \left\{(sum == \frac{i(i-1)}{2}) \wedge i \leq (n+1) \wedge (i \leq n)\right\}$$

sum = sum + i
i = i + 1

$$INV2 \equiv \left\{sum == \frac{i(i-1)}{2} \wedge i \leq (n+1)\right\} \quad \text{. . . . .} \quad \textbf{(2')}$$

gilt.
Wir wissen aber, dass vor und nach der Schleife $i \leq n+1$ gilt, und dass die Implikation $i \leq n \Rightarrow i \leq n+1$ wahr ist, also ist es offensichtlich, dass wir davon ausgehen können, dass INV2 auch eine Invariante der **while**-Schleife ist.
Wenn wir die Gültigkeit von INV2 voraussetzen, können wir die erste Programmformel

$$\{P\} \equiv \{n > 0\}$$

i = 1
sum = 0

$$INV2 \equiv \left\{sum == \frac{i(i-1)}{2} \wedge i \leq (n+1)\right\} \quad \text{. . . . .} \quad \textbf{(1)}$$

mit der folgenden kompakten Beweisdarstellung zusammenfassen:

$$\{P\} \equiv \{n > 0\}$$

$$\{R\} \equiv \left\{0 == \frac{1 \cdot (1-1)}{2} \wedge 0 \leq (n+1)\right\} \Leftrightarrow \{(n+1) \geq 0\} \quad \text{. . . . Zuweisungsaxiom}$$

$$\Leftrightarrow \{n > 0\}$$

i = 1

$$\{R\} \equiv \left\{0 == \frac{i(i-1)}{2} \wedge i \leq (n+1)\right\} \quad \text{. . . . . Zuweisungsaxiom}$$

sum = 0

$$\{INV2\} \equiv \left\{sum == \frac{i(i-1)}{2} \wedge i \leq (n+1)\right\} \quad \text{. . . . . Sequenzregel}$$

```
while  i<=n:
          sum = sum + i
          i = i + 1
```

$$\{INV2 \wedge \neg B\} \equiv \left\{sum == \frac{i(i-1)}{2} \wedge i \leq (n+1) \wedge i > n\right\} \Rightarrow \left\{sum == \frac{i(i-1)}{2} \wedge i == (n+1)\right\}$$

$$\Rightarrow \left\{sum == \frac{(n+1)n}{2}\right\} \equiv Q$$

. . . . while-Regel + Konsequenz-Regel 1