Programmverifikation mit dem Hoare-Kalkül am Beispiel der Fibonacci-Zahlen

Moritz Hammer
(hammer@pst.ifi.lmu.de)

10. Mai 2006

Wir beweisen die Korrektheit eines Programms, das Fibonacci-Zahlen berechnet, im Hoare-Kalkül. Wir geben zwei (im Vorgehen gleiche) Versionen des Beweises an: eine formelle, die mittels der Regeln des Hoare-Kalküls operiert, und eine informelle, die das Vorgehen hervorhebt.

Die Fibonacci-Zahlen werden rekursiv definiert:

$$\mathit{fib}(n) = \begin{cases} 0, & \text{falls } n \leq 0 \\ 1, & \text{falls } n = 1 \\ \mathit{fib}(n-1) + \mathit{fib}(n-2), & \text{falls } n \geq 2 \end{cases}$$

Das Programmstück, das die n-te Fibonacci-Zahl berechnen soll, ist denkbar kurz:

```
int fibonacci(int n) {
    if (n <= 0) {
        f=0;
    } else {
        k=1; g=0; f=1;
        while (k != n) {
            t = g; g = f; f = f+t; k = k+1;
        }
    }
    return f;
}
```

Mit dem Hoare-Kalkül wollen wir zeigen, daß diese Funktion tatsächlich die Fibonacci-Zahlen berechnet. Dazu versehen wir den Funktionsrumpf mit einer geeigneten Nachbedingung; die Vorbedingung ist $\mathbf{true}$, weil keine Annahmen gemacht werden müssen:

$\{\mathbf{true}\}$

```
if (n <= 0) {
    f=0;
} else {
    k=1; g=0; f=1;
```

```
        while (k != n) {
             t = g; g = f; f = f+t; k = k+1;
        }
    }
```

$\{\mathtt{f} = \mathit{fib}(\mathtt{n})\}$

1 Formeller Beweis im Hoare-Kalkül

Der formelle Beweis verwendet ausschliesslich die im Hoare-Kalkül definierten Regeln. Da dies zu relativ breiten Beweisbäumen führt, verwenden wir $\mathbf{F}_\varphi$ als Teilbeweisbäume, die in den Gesamtbeweisbaum eingesetzt werden können. Der Beweis zeigt zuerst die partielle Korrektheit; die notwendigen Schritte für totale Korrektheit werden in einem getrennten Abschnitt beschrieben.

1.1 Nachweis der Schleifeninvariante

$$I \equiv \mathtt{f} = \mathit{fib}(\mathtt{k}) \wedge \mathtt{g} = \mathit{fib}(\mathtt{k}-1)$$

Prämisse der (Iteration$_{\text{partiell}}$)-Regel, $\mathbf{F}_1$:

$$\dfrac{\mathbf{F}_2 \qquad \dfrac{\dfrac{}{\{\mathtt{f}+\mathtt{t} = \mathit{fib}(\mathtt{k}+1) \wedge \mathtt{g} = \mathit{fib}(\mathtt{k})\}\ \mathtt{f=f+t;}\ \{\mathtt{f} = \mathit{fib}(\mathtt{k}+1) \wedge \mathtt{g} = \mathit{fib}(\mathtt{k})\}}\ (\text{Zuw})}{\{I \wedge \mathtt{n} \neq \mathtt{k}\}\ \mathtt{t=g;g=f;f=f+t;}\ \{\mathtt{f} = \mathit{fib}(\mathtt{k}+1) \wedge \mathtt{g} = \mathit{fib}(\mathtt{k})\}}\ (\text{Seq}) \quad \dfrac{\dfrac{}{\{\mathtt{f} = \mathit{fib}(\mathtt{k}+1) \wedge \mathtt{g} = \mathit{fib}(\mathtt{k}+1-1)\}\ \mathtt{k=k+1;}\ \{I\}}\ (\text{Zuw})}{\{\mathtt{f} = \mathit{fib}(\mathtt{k}+1) \wedge \mathtt{g} = \mathit{fib}(\mathtt{k})\}\ \mathtt{k=k+1;}\ \{I\}}\ (\text{Abschw})}{\dfrac{\{I \wedge \mathtt{k} \neq \mathtt{n}\}\ \ \mathtt{t=g;\ g=f;\ f=f+t;\ k=k+1;}\ \ \{I\}}{\{I \wedge \mathtt{k} \neq \mathtt{n}\}\ \mathtt{\{t=g;\ g=f;\ f=f+t;\ k=k+1;\}}\ \{I\}}\ (\text{Block})}\ (\text{Seq})$$

Fortsetzung (aus Platzgründen) $\mathbf{F}_2$:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\{\mathtt{f}+\mathtt{g} = \mathit{fib}(\mathtt{k}+1) \wedge \mathtt{f} = \mathit{fib}(\mathtt{k})\}\ \mathtt{t=g;}\ \{\mathtt{f}+\mathtt{t} = \mathit{fib}(\mathtt{k}+1) \wedge \mathtt{f} = \mathit{fib}(\mathtt{k})\}}\ (\text{Zuw})}{\{I\}\ \mathtt{t=g;}\ \{\mathtt{f}+\mathtt{t} = \mathit{fib}(\mathtt{k}+1) \wedge \mathtt{f} = \mathit{fib}(\mathtt{k})\}}\ (\text{Abschw})}{\{I \wedge \mathtt{n} \neq \mathtt{k}\}\ \mathtt{t=g;}\ \{\mathtt{f}+\mathtt{t} = \mathit{fib}(\mathtt{k}+1) \wedge \mathtt{f} = \mathit{fib}(\mathtt{k})\}}\ (\text{Abschw}) \quad \dfrac{\dfrac{}{\{\mathtt{f}+\mathtt{t} = \mathit{fib}(\mathtt{k}+1) \wedge \mathtt{f} = \mathit{fib}(\mathtt{k})\}\ \mathtt{g=f;}\ \{\mathtt{f}+\mathtt{t} = \mathit{fib}(\mathtt{k}+1) \wedge \mathtt{g} = \mathit{fib}(\mathtt{k})\}}\ (\text{Zuw})}{\{I \wedge \mathtt{n} \neq \mathtt{k}\}\ \mathtt{t=g;g=f;}\ \{\mathtt{f}+\mathtt{t} = \mathit{fib}(\mathtt{k}+1) \wedge \mathtt{g} = \mathit{fib}(\mathtt{k})\}}\ (\text{Seq})$$

Partielle Korrektheit der **`while`**-Schleife, $\mathbf{F}_{\mathtt{while}}$:

$$\dfrac{\mathbf{F}_1}{\{I\}\ \mathtt{while(n\ !=\ k)\{t=g;\ g=f;\ f=f+t;\ k=k+1;\}}\ \{I \wedge \mathtt{n} = k\}}\ (\text{Iteration}_{\text{partiell}})$$

1.2 Nachweis false-Zweig

$\mathbf{F_{false}}$:

$$\dfrac{\dfrac{\dfrac{\mathbf{F_3}}{\{\mathsf{n} > 0\}\,\mathtt{k=1;\ g=0;\ f=1;}\,\{\mathsf{k} = 1 \wedge \mathsf{g} = 0 \wedge \mathsf{f} = 1\}}\,(\text{Abschw})}{\{\mathsf{n} > 0\}\,\mathtt{k=1;\ g=0;\ f=1;}\,\{I\}}\,(\text{Abschw}) \quad \dfrac{\mathbf{F_{while}}}{\{I\}\,\mathtt{while(n\ !=\ k)\ \{t=g;\ g=f;\ f=f+t;\ k=k+1;\}}\,\{\mathsf{f} = \mathit{fib}(\mathsf{n})\}}\,(\text{Abschw})}{\{\mathsf{n} > 0\}\,\mathtt{k=1;\ g=0;\ f=1;}\mathtt{while(n\ !=\ k)\ \{t=g;\ g=f;\ f=f+t;\ k=k+1;\}}\,\{\mathsf{f} = \mathit{fib}(\mathsf{n})\}}\,(\text{Seq})$$
$$\dfrac{\{\mathbf{true} \wedge \mathsf{n} > 0\}\,\mathtt{k=1;\ g=0;\ f=1;}\mathtt{while(n\ !=\ k)\ t=g;\ g=f;\ f=f+t;\ k=k+1;}\,\{\mathsf{f} = \mathit{fib}(\mathsf{n})\}}{}\,(\text{Abschw})$$

$\mathbf{F_3}$:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\{1 = 1\}\,\mathtt{k=1;}\,\{\mathsf{k} = 1\}}\,(\text{Zuw})}{\{\mathbf{true}\}\,\mathtt{k=1;}\,\{\mathsf{k} = 1\}}\,(\text{Abschw}) \quad \dfrac{\dfrac{}{\{\mathsf{k} = 1 \wedge 0 = 0\}\,\mathtt{g=0;}\,\{\mathsf{k} = 1 \wedge \mathsf{g} = 0\}}\,(\text{Zuw})}{\{\mathsf{k} = 1\}\,\mathtt{g=0;}\,\{\mathsf{k} = 1 \wedge \mathsf{g} = 0\}}\,(\text{Abschw})}{\{\mathbf{true}\}\,\mathtt{k=1;\ g=0;}\,\{\mathsf{k} = 1 \wedge \mathsf{g} = 0\}}\,(\text{Seq}) \quad \dfrac{\dfrac{}{\{\mathsf{k} = 1 \wedge \mathsf{g} = 0 \wedge 1 = 1\}\,\mathtt{f=1;}\,\{\mathsf{k} = 1 \wedge \mathsf{g} = 0 \wedge \mathsf{f} = 1\}}\,(\text{Zuw})}{\{\mathsf{k} = 1 \wedge \mathsf{g} = 0\}\,\mathtt{f=1;}\,\{\mathsf{k} = 1 \wedge \mathsf{g} = 0 \wedge \mathsf{f} = 1\}}\,(\text{Abschw})}{\{\mathbf{true}\}\,\mathtt{k=1;\ g=0;\ f=1;}\,\{\mathsf{k} = 1 \wedge \mathsf{g} = 0 \wedge \mathsf{f} = 1\}}\,(\text{Seq})$$

1.3 Nachweis true-Zweig

$\mathbf{F_{true}}$:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\{\mathsf{n} \leq 0 \wedge 0 = 0\}\,\mathtt{f=0;}\,\{\mathsf{f} = 0 \wedge \mathsf{n} \leq 0\}}\,(\text{Zuw})}{\{\mathsf{n} \leq 0\}\,\mathtt{f=0;}\,\{\mathsf{f} = 0 \wedge \mathsf{n} \leq 0\}}\,(\text{Abschw})}{\{\mathsf{n} \leq 0\}\,\mathtt{f=0;}\,\{\mathsf{f} = \mathit{fib}(\mathsf{n})\}}\,(\text{Abschw})}{\{\mathbf{true} \wedge \mathsf{n} \leq 0\}\,\mathtt{f=0;}\,\{\mathsf{f} = \mathit{fib}(\mathsf{n})\}}\,(\text{Abschw})$$

1.4 Nachweis partielle Korrektheit

$$\dfrac{\dfrac{\mathbf{F_{true}}}{\{\mathbf{true} \wedge \mathsf{n} \leq 0\}\,\mathtt{\{f=0;\ \}}\,\{\mathsf{f} = \mathit{fib}(\mathsf{n})\}}\,(\text{Block}) \quad \dfrac{\dfrac{\mathbf{F_{false}}}{\{\mathbf{true} \wedge \mathsf{n} > 0\}\,\mathtt{\{\ldots\}}\,\{\mathsf{f} = \mathit{fib}(\mathsf{n})\}}\,(\text{Block})}{\{\mathbf{true} \wedge \neg(\mathsf{n} \leq 0)\}\,\mathtt{\{\ldots\}}\,\{\mathsf{f} = \mathit{fib}(\mathsf{n})\}}\,(\text{Abschw})}{\{\mathbf{true}\}\,\mathtt{if(n\ <=\ 0)}\ldots\mathtt{else}\ldots\,\{\mathsf{f} = \mathit{fib}(\mathsf{n})\}}\,(\text{Falluntersch})$$

1.5 Änderungen für totale Korrektheit

Da totale Korrektheit für Schleifen eine andere Regel benötigt, ändert sich hier zuerst $\mathbf{F}_{\texttt{while}}$. Wir setzen $t \equiv \texttt{n-k}$:

$\mathbf{F}_{\mathbf{Abst}}$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\{\texttt{n}-\texttt{k}=z\}\,\texttt{t=g;}\,\{\texttt{n}-\texttt{k}=z\}}\,(\text{Zuw}) \quad \dfrac{}{\{\texttt{n}-\texttt{k}=z\}\,\texttt{g=f;}\,\{\texttt{n}-\texttt{k}=z\}}\,(\text{Zuw})}{\{\texttt{n}-\texttt{k}=z\}\,\texttt{t=g;g=f;}\,\{\texttt{n}-\texttt{k}=z\}}\,(\text{Seq}) \quad \dfrac{}{\{\texttt{n}-\texttt{k}=z\}\,\texttt{f=f+t;}\,\{\texttt{n}-\texttt{k}=z\}}\,(\text{Zuw})}{\{\texttt{n}-\texttt{k}=z\}\,\texttt{t=g;g=f;f=f+t;}\,\{\texttt{n}-\texttt{k}=z\}}\,(\text{Seq}) \quad \dfrac{\dfrac{}{\{\texttt{n}-(\texttt{k+1})=z-1\}\,\texttt{k=k+1;}\,\{\texttt{n-k}=z-1\}}\,(\text{Zuw})}{\{\texttt{n}-\texttt{k}=z\}\,\texttt{k=k+1;}\,\{\texttt{n-k}=z-1\}}\,(\text{Abs.})}{\{\texttt{n-k}=z\}\,\texttt{t=g; g=f; f=f+t; k=k+1;}\,\{\texttt{n-k}=z-1\}}\,(\text{Seq})}{\{I \wedge \texttt{n} \neq \texttt{k} \wedge \texttt{n-k}=z\}\,\texttt{t=g; g=f; f=f+t; k=k+1;}\,\{\texttt{n-k}<z\}}\,(\text{Abschw})$$

Problem: $I \implies \texttt{n-k} \geq 0$ gilt nicht! Also wird die Invariante verstärkt:

$$I \equiv \texttt{f} = \mathit{fib}(\texttt{k}) \wedge \texttt{g} = \mathit{fib}(\texttt{k}-1) \wedge \texttt{k} \leq \texttt{n}$$

Jetzt gilt $I \implies \texttt{n-k} \geq 0$. $\mathbf{F}_1, \mathbf{F}_2$ und $\mathbf{F}_{\mathbf{false}}$ berechnen sich analog (zu beachten ist, daß nun die Vorbedingung $\texttt{n} \neq \texttt{k}$ wichtig wird!). Das neue $\mathbf{F}_{\texttt{while}}$:

$$\dfrac{\mathbf{F}_1 \qquad \mathbf{F}_{\mathbf{Abst}}}{\{I\}\,\texttt{while}(\texttt{n != k})\{\texttt{t=g; g=f; f=f+t; k=k+1;}\}\,\{I \wedge \texttt{n} = k\}}\,(\text{Iteration}_{\text{total}})$$

2 Ein informeller Beweis

Schon aus Platzgründen ist ein formaler Beweis extrem unübersichtlich. Wir geben den obrigen Beweis in einem informelleren Schema wieder, das jedoch exakt die gleichen Beweisschritte enthält.

2.1 Partielle Korrektheit

Betrachten wir den Aufbau des Programmstücks: „Aussen“ ist eine Fallunterscheidung. Der **true**-Zweig ist einfach. Für den **false**-Zweig brauchen wir die Sequenzregel und die Iterations-Regel für das **while**-Konstrukt. Innerhalb des **while**-Konstrukt brauchen wir nur die Sequenzregel. (Und natürlich immer die Zuweisungsregel.)

Beginnen wir also mit der Schleife. Die Invariante $I \equiv \texttt{f} = \mathit{fib}(\texttt{k}) \wedge \texttt{g} = \mathit{fib}(\texttt{k}-1)$ erhalten wir durch Beobachtung des Effekts der Schleife (und mit Wissen über die Definition der Fibonacci-Zahlen). Ausserdem soll die Invariante uns „nützlich“ sein, d.h. wir schauen schon auf den Gesamtbeweis und versuchen die Invariante so zu wählen, daß am Ende $\texttt{f} = \mathit{fib}(\texttt{n})$ herauskommt (formell versuchen wir, daß $I \wedge \texttt{n} = \texttt{k} \implies \texttt{f} = \mathit{fib}(\texttt{n})$ gilt, und wir damit die Abschwächungsregel anwenden können). Wir können hier auch raten: Eine ungültige Invariante kann später nicht als korrekt bewiesen werden. Mittels der Zuweisungsregel wenden wir nun die Anweisungen des Schleifenrumpfes auf die Invariante an - von hinten nach vorne:

$$
\begin{array}{c}
\{\texttt{f} = \mathit{fib}(\texttt{k}) \wedge \texttt{g} = \mathit{fib}(\texttt{k}-1)\} \\
\texttt{k=k+1;} \\
\{\texttt{f} = \mathit{fib}(\texttt{k}+1) \wedge \texttt{g} = \mathit{fib}(\texttt{k}+1-1)\} \qquad (\star) \\
\texttt{f=f+t;} \\
\{\texttt{f+t} = \mathit{fib}(\texttt{k}+1) \wedge \texttt{g} = \mathit{fib}(\texttt{k}+1-1)\} \\
\texttt{g=f;} \\
\{\texttt{f+t} = \mathit{fib}(\texttt{k}+1) \wedge \texttt{f} = \mathit{fib}(\texttt{k}+1-1)\} \\
\texttt{t=g;} \\
\{\texttt{f+g} = \mathit{fib}(\texttt{k}+1) \wedge \texttt{f} = \mathit{fib}(\texttt{k}+1-1)\}
\end{array}
$$

Man beachte, daß wir in mit $(\star)$ bezeichneten Zeile die offensichtliche Transformation $\texttt{k}+1-1 \to \texttt{k}$ nicht anwenden, da wir hier nur die Zuweisungsregel und die Sequenzenregel verwenden, und diese beinhalten keine „Rechnerei“! Erst jetzt „rechnen“ wir, und erhalten:

$$
\begin{array}{ll}
 & \{\texttt{f+g} = \mathit{fib}(\texttt{k}+1) \wedge \texttt{f} = \mathit{fib}(\texttt{k}+1-1)\} \\
\Leftrightarrow & \{\mathit{fib}(\texttt{k}) + \texttt{g} = \mathit{fib}(\texttt{k}+1) \wedge \texttt{f} = \mathit{fib}(\texttt{k})\} \\
\Leftrightarrow & \{\texttt{g} = \mathit{fib}(\texttt{k}+1) - \mathit{fib}(\texttt{k}) \wedge \texttt{f} = \mathit{fib}(\texttt{k})\} \\
\Leftrightarrow & \{\texttt{g} = \mathit{fib}(\texttt{k}-1) \wedge \texttt{f} = \mathit{fib}(\texttt{k})\}
\end{array}
$$

Damit ist gezeigt, daß die I tatsächlich invariant bzgl. des **`while`**-Blocks ist. Im formellen Beweis heisst das nun hergeleitete Hoare-Tripel $\mathbf{F}_1$. Mit der Abschwächungsregel, die uns immer hilft, wenn wir „rechnen“ wollen, können wir jetzt auch noch $n \neq k$ in die Vorbedingung schreiben, und können nun die partielle Iterationsregel anwenden, um $\mathbf{F}_{\texttt{while}}$ zu erhalten:

$$\{\texttt{f} = \mathit{fib}(\texttt{k}) \wedge \texttt{g} = \mathit{fib}(\texttt{k}-1)\}\ \texttt{while}(\ldots)\ldots\ \{\texttt{f} = \mathit{fib}(\texttt{k}) \wedge \texttt{g} = \mathit{fib}(\texttt{k}-1) \wedge \texttt{k} = \texttt{n}\}$$

Nun müssen wir per Sequenz- und Zuweisungsregel noch den „Initialisierungsteil“ des **false**-Zweiges bearbeiten. Da wir als Nachbedingung die Invariante erreichen müssen, gehen wir wieder, ausgehend von der Invariante, nach vorne:

$$
\begin{array}{c}
\{\texttt{f} = \mathit{fib}(\texttt{k}) \wedge \texttt{g} = \mathit{fib}(\texttt{k}-1)\} \\
\texttt{f=1;} \\
\{\texttt{1} = \mathit{fib}(\texttt{k}) \wedge \texttt{g} = \mathit{fib}(\texttt{k}-1)\} \\
\texttt{g=0;} \\
\{\texttt{1} = \mathit{fib}(\texttt{k}) \wedge \texttt{0} = \mathit{fib}(\texttt{k}-1)\} \\
\texttt{k=1;} \\
\{\texttt{1} = \mathit{fib}(1) \wedge \texttt{0} = \mathit{fib}(1-1)\}
\end{array}
$$

Ein kurzer Blick in die Definition der Fibonacci-Zahlen genügt um zu sehen, daß das $\{\mathbf{true}\}$ ergibt.

Da wir am Ende auf $\mathtt{f} = \mathit{fib}(\mathtt{n})$ kommen wollen, nehmen wir dies als Nachbedingung des **else**-Zweiges. Mit Blockregel und Abschwächung können wir aus dem bereits bewiesenen Tripel $\{\mathbf{true}\}\ \ldots\ \{I\}$ das Tripel

$$\{\mathtt{n} > 0\}\ \mathtt{\{\ldots\}}\ \{\mathtt{f} = \mathit{fib}(\mathtt{n})\}$$

erhalten, und das ist genau das, was wir brauchen.

Wenden wir uns nun dem **true**-Zweig zu. Wir wollen auf die gleiche Nachbedingung kommen, aber das funktioniert nur, wenn wir wissen, daß $n \leq 0$ gilt. Also rechnen wir mit dieser Nachbedingung los:

$$\begin{array}{c}\{\mathtt{f} = 0 \wedge \mathtt{n} \leq 0\}\\ \mathtt{f=0;}\\ \{0 = 0 \wedge \mathtt{n} \leq 0\}\end{array}$$

Und daraus lässt sich sehr einfach das Hoare-Tripel

$$\{\mathtt{n} \leq 0\}\ \mathtt{f=0;}\ \{\mathtt{f} = \mathit{fib}(\mathtt{n})\}$$

mit der Abschwächungsregel gewinnen. Damit haben wir zusammen, was wir für die Fallunterscheidungsregel brauchen. Mit etwas Abschwächung, damit der Syntax passt, erhalten wir die beiden Tripel

$$\{\mathbf{true} \wedge \neg(\mathtt{n} \leq 0)\}\ \mathtt{\{\ldots\}}\ \{\mathtt{f} = \mathit{fib}(\mathtt{n})\} \qquad \{\mathbf{true} \wedge \mathtt{n} \leq 0\}\ \mathtt{f=0;}\ \{\mathtt{f} = \mathit{fib}(\mathtt{n})\}$$

und können nun die Fallunterscheidungsregel anwenden, wobei (und daher noch einmal die obrige Umformung) wir nicht im geringsten rechnen müssen:

$$\{\mathbf{true}\}\ \mathtt{if}(\mathtt{n <= 0}) \ldots \mathbf{else} \ldots\ \{\mathtt{f} = \mathit{fib}(\mathtt{n})\}$$

Und damit ist die partielle Korrektheit gezeigt.

2.2 Totale Korrektheit

Für totale Korrektheit ändert sich nur die Iterationsregel. Hier jedoch gibt es ein Problem: Um die totale Iterationsregel anwenden zu dürfen, muß $I \implies \mathtt{n-k} \geq 0$ gelten, und das ist momentan natürlich nicht der Fall. Zwar ist I eine Invariante, aber sie ist zu schwach, um diese Implikation zu ermöglichen. Also muß die Invariante verstärkt werden (durch Hinzunahme weiterer „Fakten“ über die Schleife):

$$I' \equiv \mathtt{f} = \mathit{fib}(\mathtt{k}) \wedge \mathtt{g} = \mathit{fib}(\mathtt{k} - 1) \wedge \mathtt{k} \leq \mathtt{n}$$

Daraus folgt nun zwar $I \implies \mathtt{n-k} \geq 0$, aber wir müssen natürlich noch zeigen, daß dieses stärkere Konstrukt tatsächlich eine Invariante ist.

Wir gehen also noch einmal den Nachweis der Invariante I' durch:

$$\{\mathtt{f} = \mathit{fib}(\mathtt{k}) \wedge \mathtt{g} = \mathit{fib}(\mathtt{k}-1) \wedge \mathtt{k} \leq \mathtt{n}\}$$
$$\mathtt{k=k+1;}$$
$$\{\mathtt{f} = \mathit{fib}(\mathtt{k}+1) \wedge \mathtt{g} = \mathit{fib}(\mathtt{k}+1-1) \wedge \mathtt{k}+1 \leq \mathtt{n}\}$$
$$\mathtt{f=f+t;}$$
$$\{\mathtt{f+t} = \mathit{fib}(\mathtt{k}+1) \wedge \mathtt{g} = \mathit{fib}(\mathtt{k}+1-1) \wedge \mathtt{k}+1 \leq \mathtt{n}\}$$
$$\mathtt{g=f;}$$
$$\{\mathtt{f+t} = \mathit{fib}(\mathtt{k}+1) \wedge \mathtt{f} = \mathit{fib}(\mathtt{k}+1-1) \wedge \mathtt{k}+1 \leq \mathtt{n}\}$$
$$\mathtt{t=g;}$$
$$\{\mathtt{f+g} = \mathit{fib}(\mathtt{k}+1) \wedge \mathtt{f} = \mathit{fib}(\mathtt{k}+1-1) \wedge \mathtt{k}+1 \leq \mathtt{n}\}$$

Glücklicherweise fordern die Iterationsregeln nur, daß die Invariante unter der Bedingung, daß die Schleifenbedingung wahr ist, gilt, und damit können wir weitermachen:

$$\begin{aligned}
& \{\mathtt{f+g} = \mathit{fib}(\mathtt{k}+1) \wedge \mathtt{f} = \mathit{fib}(\mathtt{k}+1-1) \wedge \mathtt{k}+1 \leq \mathtt{n}\} \\
\Leftrightarrow \quad & \{\mathtt{f+g} = \mathit{fib}(\mathtt{k}+1) \wedge \mathtt{f} = \mathit{fib}(\mathtt{k}+1-1) \wedge \mathtt{k} < \mathtt{n}\} \\
\Leftrightarrow \quad & \{\mathtt{f+g} = \mathit{fib}(\mathtt{k}+1) \wedge \mathtt{f} = \mathit{fib}(\mathtt{k}+1-1) \wedge \mathtt{k} \leq \mathtt{n} \wedge \mathtt{n} \neq \mathtt{k}\} \\
\Leftrightarrow \quad & \{\mathtt{g} = \mathit{fib}(\mathtt{k}-1) \wedge \mathtt{f} = \mathit{fib}(\mathtt{k}) \wedge \mathtt{k} \leq \mathtt{n} \wedge \mathtt{n} \neq \mathtt{k}\}
\end{aligned}$$

Nun müssen wir noch den Rest des **false**-Zweiges überprüfen, ob wir die verstärkte Vorbedingung des **`while`**-Blocks zusichern können. Wir rechnen also noch einmal die Initialisierung durch:

$$\{\mathtt{f} = \mathit{fib}(\mathtt{k}) \wedge \mathtt{g} = \mathit{fib}(\mathtt{k}-1) \wedge \mathtt{k} \leq \mathtt{n}\}$$
$$\mathtt{f=1;}$$
$$\{\mathtt{1} = \mathit{fib}(\mathtt{k}) \wedge \mathtt{g} = \mathit{fib}(\mathtt{k}-1) \wedge \mathtt{k} \leq \mathtt{n}\}$$
$$\mathtt{g=0;}$$
$$\{\mathtt{1} = \mathit{fib}(\mathtt{k}) \wedge \mathtt{0} = \mathit{fib}(\mathtt{k}-1) \wedge \mathtt{k} \leq \mathtt{n}\}$$
$$\mathtt{k=1;}$$
$$\{\mathtt{1} = \mathit{fib}(1) \wedge \mathtt{0} = \mathit{fib}(1-1) \wedge 1 \leq \mathtt{n}\}$$

Und wenn wir diese Vorbedingung zu $\{\mathtt{1} = \mathit{fib}(1) \wedge \mathtt{0} = \mathit{fib}(1-1) \wedge \mathtt{n} > 0\}$ umschreiben, können wir die Fallunterscheidungsregel wie oben schon verwenden - wobei hier wichtig ist, daß $\mathtt{n} > 0$ zugesichert wird.

Wir haben also gezeigt, daß I' eine Invariante der Schleife ist und daß $I \implies \mathtt{n-k} \geq 0$ gilt. Nun müssen wir noch nachweisen, daß `n-k` bei jedem Schleifendurchlauf kleiner wird. Dazu müssen wir feststellen, daß `n-k` bei jedem Schleifendurchlauf um exakt 1 abnimmt.

$$\{\texttt{n-k} = z - 1\}$$
$$\texttt{k=k+1;}$$
$$\{\texttt{n-(k+1)} = z - 1\}$$
$$\texttt{f=f+t;}$$
$$\{\texttt{n-(k+1)} = z - 1\}$$
$$\texttt{g=f;}$$
$$\{\texttt{n-(k+1)} = z - 1\}$$
$$\texttt{t=g;}$$
$$\{\texttt{n-(k+1)} = z - 1\}$$

Und dies rechnen wir um zu $\{\texttt{n-k} = z\}$ und können nun das Hoare-Tripel

$$\{I \wedge \texttt{n} \neq \texttt{k} \wedge \texttt{n-k} = z\} \ldots \{\texttt{n-k} = z - 1\}$$

herleiten und zu

$$\{I \wedge \texttt{n} \neq \texttt{k} \wedge \texttt{n-k} = z\} \ldots \{\texttt{n-k} < z\}$$

abschwächen, und damit die ($\text{Iteration}_{\text{total}}$)-Regel anwenden. Diese wird genauso wie die partielle Iterationsregel in den Gesamtbeweis eingebaut, und die totale Korrektheit ist gezeigt.