Theoretische Informatik und Logik
Übungsblatt 4 (2019W)
Lösungsvorschlag

Allgemeine Hinweise: Nummerieren Sie alle auftretenden Formeln in Tableau-Beweisen und geben Sie entsprechende Herkunftshinweise bei allen Regelanwendungen an. Außerdem sind γ- und δ-Formeln jeweils als solche zu markieren. Beachten Sie die Notationsvereinbarungen auf Folie 321.

Aufgabe 4.1

Für jede der folgenden Behauptungen: Finden Sie entweder einen Tableau-Beweis oder geben Sie ein Gegenbeispiel an.

a) Aus $\exists x Q(g(x))$ und $\exists x \forall y\, g(x) = y$ folgt $\forall x(Q(g(x)) \wedge Q(g(g(x))))$.

b) Aus $\exists x\, c = x$, $\forall x \exists y f(x) = f(f(y))$ und $\forall x f(x) = a$ folgt $\exists y(f(y) = c \vee a = c)$

c) $\forall x \exists y[\neg(P(x, y) \supset \forall x \exists z P(x, z))]$ ist unerfüllbar.

Lösung 4.1

a) Folgendes geschlossene Tableau zeigt die Richtigkeit der Konsequenzbehauptung:

(1)	$\mathbf{t} : \exists x\, Q(g(x))$				Annahme, δ-Formel
(2)	$\mathbf{t} : \exists x \forall y\, g(x) = y$				Annahme, δ-Formel
(3)	$\mathbf{f} : \forall x(Q(g(x)) \wedge Q(g(g(x))))$				Annahme, δ-Formel
(4)	$\mathbf{t} : Q(g(a))$				von 1
(5)	$\mathbf{t} : \forall y\, g(b) = y$				von 2, γ-Formel
(6)	$\mathbf{f} : Q(g(c)) \wedge Q(g(g(c)))$				von 3
(7)	$\mathbf{t} : g(b) = g(a)$				von 5
(8)	$\mathbf{t} : Q(g(b))$				$S^{=}$: 7→4
(9)	$\mathbf{f} : Q(g(c))$	von 6	(10)	$\mathbf{f} : Q(g(g(c)))$	von 6
(11)	$\mathbf{t} : g(b) = g(c)$	von 5	(13)	$\mathbf{t} : g(b) = g(g(c))$	von 5
(12)	$\mathbf{f} : Q(g(b))$	$S^{=}$: 11→9	(14)	$\mathbf{f} : Q(g(b))$	$S^{=}$: 13→10
	$\times$	Wid.: 8/12		$\times$	Wid.: 8/14

Kommentar:
Beachten Sie, dass in den Zeilen 4, 5 und 6 jeweils eine neue Konstante einzusetzen ist um die Korrektheit des Beweises sicherzustellen (vgl. Aufgabe 4.3).

b) Die Konsequenzbehauptung ist falsch, wie folgendes Gegenbeispiel zeigt: $\mathcal{I} = \langle \omega, \Phi, \xi \rangle$, mit $\Phi(a) = 0$, $\Phi(c) = 1$, $\Phi(f)(n) = 0$, ξ ist beliebig, da hier nur geschlossene Formeln interpretiert werden.
Die Formel $\exists x\, c = x$ ist in jeder Interpretation wahr. Die zweite Prämisse ist unter $\mathcal{I}$ wahr, da unter dieser Interpretation alle mit f aufgebauten Terme zu 0 auswerten. Aus demselben Grund (und weil $\Phi(a) = 0$) ist auch die dritte Prämisse, $\forall x f(x) = a$, unter $\mathcal{I}$ wahr. Aber die Konklusion $\exists y(f(y) = c \vee a = c)$ drückt unter $\mathcal{I}$ aus, dass die Funktion $\Phi(f)$ für mindestens einen Eingabewert 1 als Ergebnis liefert oder $0 = 1$ gilt, was beides falsch ist.

c) Folgendes geschlossene Tableau (=Tableau-Beweis) zeigt die Unerfüllbarkeit der Formel:

(1)	$\mathbf{t} : \forall x \exists y[\neg(P(x,y) \supset \forall x \exists z P(x,z))]$	Annahme, γ-Formel
(2)	$\mathbf{t} : \exists y[\neg(P(a,y) \supset \forall x \exists z P(x,z))]$	von 1, δ-Formel
(3)	$\mathbf{t} : \neg(P(a,b) \supset \forall x \exists z P(x,z))$	von 2
(4)	$\mathbf{f} : P(a,b) \supset \forall x \exists z P(x,z)$	von 3
(5)	$\mathbf{t} : P(a,b)$	von 4
(6)	$\mathbf{f} : \forall x \exists z P(x,z)$	von 4, δ-Formel
(7)	$\mathbf{f} : \exists z P(c,z)$	von 6, γ-Formel
(8)	$\mathbf{t} : \exists y[\neg(P(c,y) \supset \forall x \exists z P(x,z))]$	von 1, δ-Formel
(9)	$\mathbf{t} : \neg(P(c,d) \supset \forall x \exists z P(x,z))$	von 8
(10)	$\mathbf{f} : P(c,d) \supset \forall x \exists z P(x,z)$	von 9
(11)	$\mathbf{t} : P(c,d)$	von 10
(12)	$\mathbf{f} : \forall x \exists z P(x,z)$	von 10, δ-Formel
(13)	$\mathbf{f} : P(c,d)$	von 7
	$\times$	Widerspruch (11/13)

Beachten Sie, dass die δ-Regel jeweils nach einer neuen Konstante verlangt. Entsprechend muss die γ-Regel — nach Verwendung der δ-Regel in den Zeilen 7 und 9 — nochmals auf die Formel in der Zeile 1 angewendet werden, um ein geschlossenes Tableau zu erhalten.

Aufgabe 4.2

Sind folgende Konsequenzbehauptungen richtig? Im positiven Fall ist ein Tableau-Beweis anzugeben, im negativen Fall ein vollständig spezifiziertes Gegenbeispiel. (Siehe Folie 409 für entsprechende PL-Formeln.)

a) Jede euklidische Relation ist schwach gerichtet.

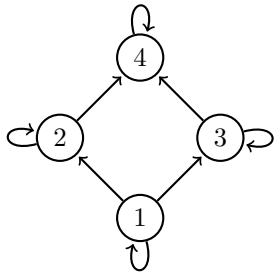
b) Jede schwach gerichtete und reflexive Relation ist euklidisch.

Lösung 4.2

a) Ein Tableau-Beweis dieser Konsequenzbehauptung sieht wie folgt aus:

(1)	$\mathbf{t} : \forall x \forall y \forall z[(R(x,y) \wedge R(x,z)) \supset R(y,z)]$							Ann., γ
(2)	$\mathbf{f} : \forall x \forall y \forall z[(R(x,y) \wedge R(x,z)) \supset \exists u(R(y,u) \wedge R(z,u))]$							Ann., δ
(3)	$\mathbf{f} : \forall y \forall z[(R(a,y) \wedge R(a,z)) \supset \exists u(R(y,u) \wedge R(z,u))]$							von 2, δ
(4)	$\mathbf{f} : \forall z[(R(a,b) \wedge R(a,z)) \supset \exists u(R(b,u) \wedge R(z,u))]$							von 3, δ
(5)	$\mathbf{f} : (R(a,b) \wedge R(a,c)) \supset \exists u(R(b,u) \wedge R(c,u))]$							von 4
(6)	$\mathbf{t} : R(a,b) \wedge R(a,c)$							von 5
(7)	$\mathbf{f} : \exists u(R(b,u) \wedge R(c,u))$							von 5, γ
(8)	$\mathbf{t} : \forall y \forall z[(R(a,y) \wedge R(a,z)) \supset R(y,z)]$							von 1, γ
(9)	$\mathbf{t} : \forall z[(R(a,b) \wedge R(a,z)) \supset R(b,z)]$							von 8, γ
(10)	$\mathbf{t} : (R(a,b) \wedge R(a,c)) \supset R(b,c)$							von 9
(11)	$\mathbf{f} : R(a,b) \wedge R(a,c)$ v. 10 $\times$ (6/11)	(12)	$\mathbf{t} : R(b,c)$					von 10
		(13)	$\mathbf{f} : R(b,c) \wedge R(c,c)$					von 7
		(14) $\mathbf{f} : R(b,c)$ v. 13 $\times$ (12/14)	(15)	$\mathbf{f} : R(c,c)$				von 13
			(16)	$\mathbf{t} : \forall y \forall z[(R(a,y) \wedge R(a,z)) \supset R(y,z)]$				von 1, γ
			(17)	$\mathbf{t} : \forall z[(R(a,c) \wedge R(a,z)) \supset R(c,z)]$				von 16, γ
			(18)	$\mathbf{t} : (R(a,c) \wedge R(a,c)) \supset R(c,c)$				von 17
			(19)	$\mathbf{t} : R(a,b)$				von 6
			(20)	$\mathbf{t} : R(a,c)$				von 6
			(21)	$\mathbf{f} : R(a,c) \wedge R(a,c)$ von 18			(22) $\mathbf{t} : R(c,c)$ $\times$ (15/22)	von 18
			(23)	$\mathbf{f}:R(a,c)$ v. 21 $\times$ (20/23)	(24) $\mathbf{f}:R(a,c)$ v. 21 $\times$ (20/24)			

b) Diese Aussage ist falsch. Folgendes Gegenbeispiel ist am leichtesten in graphischer Darstellung zu verstehen. Dabei wird R als die Kanten-Relation des folgenden Graphen interpretiert:



Die Kanten-Relation ist offensichtlich reflexiv und schwach gerichtet, aber nicht euklidisch.

Formaler: $\mathcal{I} = \langle\{1,2,3,4\}, \Phi, \xi\rangle$, wobei $\Phi(R)(x,y) \Leftrightarrow x = y$ oder ($x = 1$ und $y = 2$) oder ($x = 1$ und $y = 3$) oder ($x = 2$ und $y = 4$) oder ($x = 3$ und $y = 4$); ξ ist beliebig.
Alternativ kann man die Relation $\Phi(R)$ als die folgende Menge von Paaren spezifizieren:
$\Phi(R) = \{\langle 1,1\rangle, \langle 2,2\rangle, \langle 3,3\rangle, \langle 4,4\rangle, \langle 1,2\rangle, \langle 1,3\rangle, \langle 2,4\rangle, \langle 3,4\rangle\}$.

Aufgabe 4.3
Untersuchen Sie folgende Varianten der γ- bzw. der δ-Regel für PL-Tableaux.

a) Wenn man bei der γ-Regel nicht berücksichtigt, dass der einzusetzende Term t auch neue Konstanten (Parameter) enthalten kann (anstatt nur aus Konstanten und Funktionssymbolen aufgebaut zu sein, die bereits in den Annahmen vorkommen): Bleibt der Tableau-Kalkül korrekt? Bleibt er vollständig?

b) Wenn man für die δ-Regel nicht verlangt, dass die einzusetzende Konstante bisher nicht im Tableau vorkommen darf: Bleibt der Tableau-Kalkül korrekt? Bleibt er vollständig?

Begründen Sie positive Antworten und geben Sie jeweils ein konkretes Gegenbeispiel bei einer negativen Antwort an. (Gehen Sie davon aus, dass der Tableau-Kalkül, so wie er in der Vorlesung präsentiert wurde, korrekt und vollständig ist.)

Lösung 4.3
a) Jedes Tableau, in dem die eingeschränkte Variante der γ-Regel verwendet wird, bleibt ein regelkonformes Tableau auch gemäß der ursprünglichen Regeln. Insbesondere entstehen durch die Variante keine neuen *geschlossenen* Tableaux. Daher bleibt der Kalkül korrekt.

Allerdings ist der Kalkül nun unvollständig, wie folgendes Beispiel zeigt.
Die Formel $F = \exists x(P(x) \supset P(x))$ ist offensichtlich gültig, aber die entsprechende Signatur Σ enthält gar keine Konstantensymbole. Daher gibt es *keine geschlossene Terme* über Σ. Das bedeutet aber, dass auf $\mathbf{f} : \exists x(P(x) \supset P(x))$ die modifizierte γ-Regel gar nicht anwendbar ist und folglich trotz der Gültigkeit von F kein geschlossenes Tableau für F existiert.

b) Der Kalkül bleibt vollständig, da alle Äste, die in der ursprünglichen Variante des Kalküls geschlossen sind, auch weiterhin geschlossen bleiben. Es gibt also mit der neuen δ-Regel allenfalls zusätzliche Tableau-Beweise.

Folgendes Beispiel zeigt, dass der Kalkül nicht mehr korrekt ist: Die Formel $G = \exists x P(x) \supset P(a)$ ist offensichtlich nicht gültig, da wir beispielsweise über dem Gegenstandsbereich der natürlichen Zahlen $\Phi(P) =$ "ist gerade" und $\Phi(a) = 1$ interpretieren können. Jedes Tableau für G muss wie folgt beginnen:

(1)	$\mathbf{f} : \exists x P(x) \supset P(a)$	Annahme
(2)	$\mathbf{t} : \exists x P(x)$	δ-Formel
(3)	$\mathbf{f} : P(a)$	

Wenn wir nun bei der Elimination des Existenzquantors in (2) a anstatt eines neuen Parameters für x einsetzen, so erhalten wir in der nächsten Zeile

$$(4) \quad \mathbf{t} : P(a)$$

und folglich ein geschlossenes Tableau im Gegensatz zur Tatsache, dass G nicht gültig ist.

Aufgabe 4.4
Verwenden Sie die Definition von partieller bzw. totaler Korrektheit um festzustellen, für welche Programme π die folgenden Korrektheitsaussagen wahr sind.

a) $\{\top\}\,\pi\,\{\top\}$

b) $\{\top\}\,\pi\,\{\bot\}$

c) $\{\bot\}\,\pi\,\{\top\}$

d) $\{\bot\}\,\pi\,\{\bot\}$

Das sind in Summe acht Fragen (vier verschiedene Kombinationen von Vor- und Nachbedingungen, jeweils untersucht hinsichtlich partieller und totaler Korrektheit), die sich aber gemeinsam mit nur wenigen Fallunterscheidungen beantworten lassen.

Es sind nicht konkrete Programme gefragt, die die Korrektheitsaussagen wahr werden lassen, sondern die notwendigen und hinreichenden Eigenschaften, die ein Programm erfüllen muss, sodass die Aussagen wahr sind.

Lösung 4.4
Partielle Korrektheit: Eine Korrektheitsaussage $\{F\}\,\pi\,\{G\}$ ist wahr bzgl. partieller Korrektheit, wenn gilt:

> Für alle $I \in ENV$ gilt:
> Wenn $\mathcal{M}(I, F) = \mathbf{t}$ zutrifft und $I' = \mathcal{M}(I, \pi)$ definiert ist,
> dann trifft $\mathcal{M}(I', G) = \mathbf{t}$ zu.

Für $F = \bot$ oder $G = \top$ ist die Implikation unabhängig von der Wahl von π immer erfüllt, da entweder die Prämisse immer falsch oder die Konklusion immer wahr ist. Anders gesagt ist die Korrektheitsaussage in diesen Fällen für beliebige Programme π wahr.

Betrachten wir den vierten Fall, $F = \top$ und $G = \bot$. Gibt es auch nur eine einzige Variablenbelegung I, sodass $I' = \mathcal{M}(I, \pi)$ definiert ist, dann ist die Korrektheitsaussage falsch. Die Belegung I stellt dann nämlich ein Gegenbeispiel zur All-Behauptung dar, da die Implikation falsch liefert:

$$\text{Wenn } \underbrace{\mathcal{M}(I, \top) = \mathbf{t}}_{\text{gilt}} \text{ und } \underbrace{I' = \mathcal{M}(I, \pi)}_{\text{ist definiert}} \text{ definiert, dann } \underbrace{\mathcal{M}(I', \bot) = \mathbf{t}}_{\text{gilt nicht}}.$$

Somit ist die Aussage in diesem Fall ausschließlich für jene Programme π partiell korrekt, die für keine Eingabe terminieren.

Totale Korrektheit: Eine Korrektheitsaussage $\{F\}\,\pi\,\{G\}$ ist wahr bzgl. totaler Korrektheit, wenn gilt:

> Für alle $I \in ENV$ gilt:
> Wenn $\mathcal{M}(I, F) = \mathbf{t}$ zutrifft,
> dann ist $I' = \mathcal{M}(I, \pi)$ definiert und es trifft $\mathcal{M}(I', G) = \mathbf{t}$ zu.

Für $F = \bot$ ist die Implikation unabhängig von der Wahl von π immer erfüllt, da die Prämisse falsch ist. Für $F = \top$ und $G = \bot$ ist die Implikation unabhängig von der Wahl von π immer falsch, da die Prämisse wahr und die Konklusion falsch ist:

$$\text{Wenn } \underbrace{\mathcal{M}(I, \top) = \mathbf{t}}_{\text{gilt}}, \text{ dann } \underbrace{I' = \mathcal{M}(I, \pi)}_{\text{beliebig}} \text{ definiert und } \underbrace{\mathcal{M}(I', \bot) = \mathbf{t}}_{\text{gilt nicht}}.$$

Betrachten wir den vierten Fall, $F = \top$ und $G = \top$. Gibt es auch nur eine einzige Variablenbelegung I, sodass $I' = \mathcal{M}(I, \pi)$ nicht definiert ist, dann ist die Korrektheitsaussage falsch. Die Belegung I stellt dann nämlich ein Gegenbeispiel zur All-Behauptung dar, da die Implikation falsch liefert:

$$\text{Wenn } \underbrace{\mathcal{M}(I, \top) = \mathbf{t}}_{\text{gilt}}, \text{ dann } \underbrace{I' = \mathcal{M}(I, \pi)}_{\text{nicht definiert}} \text{ definiert und } \underbrace{\mathcal{M}(I', \top) = \mathbf{t}}_{\text{gilt}}.$$

Somit ist die Aussage ausschließlich für jene Programme π total korrekt, die für jede Eingabe terminieren.

Zusammenfassend stellen wir fest:

a) $\{\top\}\,\pi\,\{\top\}$ ist partiell korrekt für alle Programme, aber total korrekt nur für Programme, die immer terminieren.

b) $\{\top\}\,\pi\,\{\bot\}$ ist partiell korrekt nur für Programme, die nie terminieren, und total korrekt für kein Programm.

c) $\{\bot\}\,\pi\,\{\top\}$ ist partiell und total korrekt für alle Programme.

d) $\{\bot\}\,\pi\,\{\bot\}$ ist partiell und total korrekt für alle Programme.

Aufgabe 4.5

Verwenden Sie die Regeln des Hoare-Kalküls, am besten in Form der Annotationsregeln, um zu zeigen, dass die folgende Aussage total korrekt, d.h., wahr hinsichtlich totaler Korrektheit ist. Verwenden Sie die Formel

$$m^2 \leq k < n^2 \wedge 0 \leq m < n \leq k + 1$$

als Invariante und den Ausdruck $n - m$ als Terminationsfunktion (Variante). Argumentieren Sie, warum die auftretenden Formeln gültig sind.

Welche Funktion berechnet das Programm, wenn man k als Eingabe und m als Ausgabe betrachtet? Zur Beantwortung dieser Frage reicht es, die Nachbedingung geeignet umzuformen.

$\{\, F\colon k \geq 0 \,\}$
```
begin
  begin
    m ← 0;
    n ← k + 1
  end;
  while m + 1 ≠ n do
    begin
      l ← (m + n)/2;
      if l² ≤ k then
        m ← l
      else
        n ← l
    end
end
```
$\{\, G\colon m^2 \leq k < (m+1)^2 \,\}$

Lösung 4.5

Im Folgenden kürzen wir die Invariante mit *Inv* und die Variante mit t ab. Im ersten Schritt annotieren wir das Programm mit den Bedingungen, die sich aus dem Hoare-Kalkül ergeben. Wir nummerieren die Formeln in jener Reihenfolge, in der wir sie hinzufügen.

$\{\, F\colon k \geq 0 \,\}$
begin
  begin
    $\{\, F_6\colon \mathit{Inv}\left[\begin{smallmatrix} k+1 \\ n \end{smallmatrix}\right]\left[\begin{smallmatrix} 0 \\ m \end{smallmatrix}\right] \,\}$
    $m \leftarrow 0;$
    $\{\, F_5\colon \mathit{Inv}\left[\begin{smallmatrix} k+1 \\ n \end{smallmatrix}\right] \,\}$
    $n \leftarrow k+1$
  end;
  $\{\, F_1\colon \mathit{Inv} \,\}$
  while $m+1 \neq n$ **do**
    $\{\, F_2\colon \mathit{Inv} \wedge m+1 \neq n \wedge t = t_0 \,\}$
    begin
      $l \leftarrow (m+n)/2;$
      $\{\, F_7\colon \mathit{Inv} \wedge m+1 \neq n \wedge t = t_0 \wedge l = (m+n)/2 \,\}$
      if $l^2 \leq k$ **then**
        $\{\, F_8\colon \mathit{Inv} \wedge m+1 \neq n \wedge t = t_0 \wedge l = (m+n)/2 \wedge l^2 \leq k \,\}$
        $\{\, F_{12}\colon (\mathit{Inv} \wedge 0 \leq t < t_0)\left[\begin{smallmatrix} l \\ m \end{smallmatrix}\right] \,\}$
        $m \leftarrow l$
        $\{\, F_{10}\colon \mathit{Inv} \wedge 0 \leq t < t_0 \,\}$
      else
        $\{\, F_9\colon \mathit{Inv} \wedge m+1 \neq n \wedge t = t_0 \wedge l = (m+n)/2 \wedge l^2 > k \,\}$
        $\{\, F_{13}\colon (\mathit{Inv} \wedge 0 \leq t < t_0)\left[\begin{smallmatrix} l \\ n \end{smallmatrix}\right] \,\}$
        $n \leftarrow l$
        $\{\, F_{11}\colon \mathit{Inv} \wedge 0 \leq t < t_0 \,\}$
    end
    $\{\, F_3\colon \mathit{Inv} \wedge 0 \leq t < t_0 \,\}$
  $\{\, F_4\colon \mathit{Inv} \wedge m+1 = n \,\}$
end
$\{\, G\colon m^2 \leq k < (m+1)^2 \,\}$

Beweis der Implikationen: Überall dort, wo wir zwei Bedingungen erhalten haben (eine beim Annotieren von oben nach unten, eine beim Annotieren von unten nach oben), müssen wir zeigen, dass die obere Bedingung die untere impliziert (Implikationsregel).

$F \supset F_6$

$$k \geq 0 \supset \mathit{Inv}\left[\begin{smallmatrix} k+1 \\ n \end{smallmatrix}\right]\left[\begin{smallmatrix} 0 \\ m \end{smallmatrix}\right]$$
$$k \geq 0 \supset 0^2 \leq k < (k+1)^2 \wedge 0 \leq 0 < k+1 \leq k+1$$

Konklusion	gültig, weil ...
$0^2 \leq k$	äquivalent zur Prämisse $k \geq 0$
$k < (k+1)^2$	wahr für beliebiges k
$0 \leq 0$	wahr (Eigenschaft der Relation $\leq$)
$0 < k+1$	äquivalent zur Prämisse $k \geq 0$
$k+1 \leq k+1$	wahr für beliebiges k (Eigenschaft der Relation $\leq$)

$F_4 \supset G$

$$\mathit{Inv} \wedge m+1 = n \supset m^2 \leq k < (m+1)^2$$
$$m^2 \leq k < n^2 \wedge 0 \leq m < n \leq k+1 \wedge m+1 = n \supset m^2 \leq k < (m+1)^2$$

Konklusion	gültig, weil ...
$m^2 \leq k$	ist eine der Prämissen
$k < (m+1)^2$	folgt aus den Prämissen $k < n^2$ und $m+1 = n$

$F_8 \supset F_{12}$

$$(Inv \wedge m+1 \neq n \wedge t = t_0 \wedge l = (m+n)/2 \wedge l^2 \leq k)$$
$$\supset (Inv \wedge 0 \leq t < t_0)\left[\begin{smallmatrix} l \\ m \end{smallmatrix}\right]$$

$$(m^2 \leq k < n^2 \wedge 0 \leq m < n \leq k+1 \wedge m+1 \neq n \wedge n-m = t_0 \wedge l = (m+n)/2 \wedge l^2 \leq k)$$
$$\supset l^2 \leq k < n^2 \wedge 0 \leq l < n \leq k+1 \wedge 0 \leq n-l < t_0$$

Konklusion	gültig, weil ...
$l^2 \leq k$	Prämisse
$k < n^2$	Prämisse
$0 \leq l$	Wegen der Prämisse $l = (m+n)/2$ müssen wir $(m+n)/2 \geq 0$ zeigen. Das gilt, da sowohl m als auch n nicht-negativ sind (Prämisse $0 \leq m < n$).
$l < n$	Aus den Prämissen $l = (m+n)/2$ und $m < n$ erhalten wir $(m+n)/2 < (n+n)/2 = n$.
$n \leq k+1$	Prämisse
$0 \leq n-l$	Wir haben bereits gezeigt, dass aus den Prämissen $l < n$ folgt (siehe oben). Das ist gleichbedeutend mit $0 < n-l$, woraus wir $0 \leq n-l$ erhalten.
$n-l < t_0$	Wegen der Prämissen $l = (m+n)/2$ und $n-m = t_0$ lässt sich die Ungleichung schreiben als $m < (m+n)/2$. Aus den Prämissen $m < n$ und $m+1 \neq n$ erhalten wir $m+2 \leq n$, daher gilt $(m+n)/2 \geq (m+m+2)/2 = m+1 > m$, was wir zeigen wollten. Die Voraussetzung $m+1 \neq n$ wird tatsächlich benötigt, da andernfalls $(m+m+1)/2$ nicht strikt größer als m sein müsste.

$F_9 \supset F_{13}$

$$(Inv \wedge m+1 \neq n \wedge t = t_0 \wedge l = (m+n)/2 \wedge l^2 > k)$$
$$\supset (Inv \wedge 0 \leq t < t_0)\left[\begin{smallmatrix} l \\ n \end{smallmatrix}\right]$$

$$(m^2 \leq k < n^2 \wedge 0 \leq m < n \leq k+1 \wedge m+1 \neq n \wedge n-m = t_0 \wedge l = (m+n)/2 \wedge l^2 > k)$$
$$\supset m^2 \leq k < l^2 \wedge 0 \leq m < l \leq k+1 \wedge 0 \leq l-m < t_0$$

Konklusion	gültig, weil ...
$m^2 \leq k$	Prämisse
$k < l^2$	Prämisse
$0 \leq m$	Prämisse
$m < l$	Wegen der Prämisse $l = (m+n)/2$ müssen wir $m < (m+n)/2$ zeigen. Die Prämissen $m < n$ und $m+1 \neq n$ implizieren zusammen $m+2 \leq n$, wir erhalten daher $(m+n)/2 \geq (m+m+2)/2 = m+1 > m$. Die Voraussetzung $m+1 \neq n$ wird tatsächlich benötigt, da $(m+m+1)/2$ andernfalls nicht zwingend größer als m sein muss.
$l \leq k+1$	Wegen der Prämisse $m < n \leq k+1$ gilt $m < k+1$ und $n \leq k+1$, woraus wir $l = (m+n)/2 \leq k < k+1$ erhalten.
$l < n$	Aus den Prämissen $l = (m+n)/2$ und $m < n$ folgt $(m+n)/2 < (n+n)/2 = n$.
$0 \leq l-m$	Wir haben bereits ein paar Zeilen weiter oben gezeigt, dass aus den Prämissen $m < l$ folgt. Das ist gleichbedeutend mit $0 < l-m$, woraus $0 \leq l-m$ folgt.
$l-m < t_0$	Wegen der Prämisse $n-m = t_0$ ist dies gleichbedeutend mit $l < n$, was aber aus den Prämissen folgt (siehe ein paar Zeilen weiter oben).

Die durch das Programm berechnete Funktion erhält man durch Auflösen der Nachbedingung nach m.

$$\begin{aligned} & m^2 \leq k < (m+1)^2 && \left|\sqrt{\ }\right. \\ & m \leq \sqrt{k} < m+1 && \left| \text{ Definition der Floor-Funktion}\right. \\ & m = \lfloor \sqrt{k} \rfloor \end{aligned}$$

Das heißt, das Programm berechnet die ganzzahlige Quadratwurzel aus k.