Ludwig-Maximilians-Universität München
Institut für Informatik
Dr. S. Merz

SS 2001
Begleitblatt 12

Temporale Logik

Grundlegende Beweisregeln für Systemeigenschaften

Im folgenden seien A, B, C Zustandsformeln.

Typische Arten von Formeln zur Beschreibung von Systemeigenschaften

Invarianzeigenschaften. $A \rightarrow \Box B$

Präzedenzeigenschaften. $A \rightarrow B$ **atnext** C, $A \rightarrow B$ **unless** C, $A \rightarrow (B$ **atnext** $C)$ **atnext** $C, \ldots$

Response. $A \rightarrow \Diamond B$

Grundlegende Beweisregeln

(inv) $A \rightarrow B, B$ **invof** $\mathcal{A}_\Gamma \vdash A \rightarrow \Box B$ — gültig in jedem MSTS$_{(s)}$ Γ

(inv') $\text{start}_\Gamma \rightarrow A, A$ **invof** $\mathcal{A}_\Gamma \vdash \Box A$ — gültig in jedem MSTS$_s$ Γ

(atnext)
exec $\lambda \wedge A \rightarrow \bigcirc(C \rightarrow B) \wedge \bigcirc(\neg C \rightarrow A)$ für alle $\lambda \in \mathcal{A}_\Gamma$
$\text{nil}_\Gamma \wedge A \rightarrow (C \rightarrow B)$ — gültig in jedem MSTS$_{(s)}$ Γ
$\vdash A \rightarrow B$ **atnext** C

(unless)
exec $\lambda \wedge A \rightarrow \bigcirc C \vee \bigcirc(A \wedge B)$ für alle $\lambda \in \mathcal{A}_\Gamma$
$\text{nil}_\Gamma \wedge A \rightarrow B \vee C$ — gültig in jedem MSTS$_{(s)}$ Γ
$\vdash A \rightarrow B$ **unless** C

(well)
exec $\lambda \wedge H_\lambda \wedge A \rightarrow \bigcirc(B \vee \exists \overline{z}(\overline{z} \prec z \wedge A_z(\overline{z})))$ für alle $\lambda \in \mathcal{A}_\Gamma$
exec $\lambda \wedge \neg H_\lambda \wedge A \rightarrow \bigcirc(B \vee \exists \overline{z}(\overline{z} \preceq z \wedge A_z(\overline{z})))$ für alle $\lambda \in \mathcal{A}_\Gamma$
$\Box A \rightarrow \Diamond(B \vee E)$
$\vdash \exists z\, A \rightarrow B$ (z nicht frei in B) — gültig in jedem FSTS$_{(s)}$ Γ
Dabei: $\mathcal{A}_\Gamma = \{\lambda_1, \ldots, \lambda_m\}$
$H_{\lambda_1}, \ldots, H_{\lambda_m}$ Formeln von $\mathcal{L}_{T\Gamma}$ ohne flexible Symbole
$E \equiv (H_{\lambda_1} \wedge \text{enabled}_{\lambda_1}) \vee \ldots \vee (H_{\lambda_m} \wedge \text{enabled}_{\lambda_m})$

Herleitung von (well): Sei $C \equiv (\text{exec } \lambda_1 \wedge H_{\lambda_1}) \vee \ldots \vee (\text{exec } \lambda_m \wedge H_{\lambda_m})$.

(1) exec $\lambda \wedge H_\lambda \wedge A \rightarrow \bigcirc(B \vee \exists \overline{z}(\overline{z} \prec z \wedge A_z(\overline{z})))$ für alle $\lambda \in \mathcal{A}_\Gamma$ (Ann.)

(2) exec $\lambda \wedge \neg H_\lambda \wedge A \rightarrow \bigcirc(B \vee \exists \overline{z}(\overline{z} \preceq z \wedge A_z(\overline{z})))$ für alle $\lambda \in \mathcal{A}_\Gamma$ (Ann.)

(3) $\Box A \rightarrow \Diamond(B \vee E)$ (Ann.)

(4) $A \rightarrow \exists \overline{z}(\overline{z} \preceq z \wedge A_z(\overline{z}))$ (pred)

(5) exec $\lambda \wedge \exists \overline{z}(\overline{z} \preceq z \wedge A_z(\overline{z})) \wedge \Box\neg B \rightarrow \bigcirc(\exists \overline{z}(\overline{z} \preceq z \wedge A_z(\overline{z})) \wedge \Box\neg B)$ für alle $\lambda \in \mathcal{A}_\Gamma$ (1)(2)

(6) $\exists \overline{z}(\overline{z} \preceq z \wedge A_z(\overline{z})) \wedge \Box\neg B \rightarrow \Box(\exists \overline{z}(\overline{z} \preceq z \wedge A_z(\overline{z})) \wedge \Box\neg B)$ (inv)(5)

(7) $A \wedge \Box\neg B \rightarrow \Box\exists \overline{z}(\overline{z} \preceq z \wedge A_z(\overline{z}))$ (4)(6)

(8) $A \wedge \Box\neg B \wedge \Box\neg\exists \overline{z}(\overline{z} \prec z \wedge A_z(\overline{z})) \rightarrow \Box A \wedge \Box\neg B$ (7)

(9) $\Box A \rightarrow \Box\Diamond(B \vee E)$ (3)(T30)

(10) $\Box A \rightarrow \Box\Diamond B \vee \Box\Diamond E$ (9)(T32)

(11) $\Box\Diamond E \rightarrow \Box\Diamond(H_{\lambda_1} \wedge \text{enabled}_{\lambda_1}) \vee \ldots \vee \Box\Diamond(H_{\lambda_m} \wedge \text{enabled}_{\lambda_m})$ (T32)

(12) $\Box\Diamond\text{enabled}_\lambda \rightarrow \Diamond\text{exec}\ \lambda$ für alle $\lambda \in \mathcal{A}_\Gamma$ (fair)

(13) $H_\lambda \rightarrow \Box H_\lambda$ für alle $\lambda \in \mathcal{A}_\Gamma$ (ltl6)(ind1)

(14) $\Box\Diamond E \rightarrow \Diamond C$ (11)(12)(13)

(15) $A \wedge \Box\neg B \wedge \Box\neg\exists\,\overline{z}(\overline{z} \prec z \wedge A_z(\overline{z})) \rightarrow \Diamond C \wedge \Box A \wedge \Box\neg B$ (8)(10)(14)

(16) $\Box A \wedge \Box\neg B \rightarrow (\Diamond C \rightarrow \Diamond(C \wedge A \wedge \Box\neg B))$ (T10)(T17)(T29)

(17) $A \wedge \Box\neg B \wedge \Box\neg\exists\,\overline{z}(\overline{z} \prec z \wedge A_z(\overline{z})) \rightarrow \Diamond(C \wedge A \wedge \Box\neg B)$ (15)(16)

(18) $\text{exec}\ \lambda \wedge H_\lambda \wedge A \wedge \Box\neg B \rightarrow \bigcirc\exists\,\overline{z}(\overline{z} \prec z \wedge A_z(\overline{z}))$ für alle $\lambda \in \mathcal{A}_\Gamma$ (1)

(19) $A \wedge \Box\neg B \wedge \Box\neg\exists\,\overline{z}(\overline{z} \prec z \wedge A_z(\overline{z})) \rightarrow \Diamond\exists\,\overline{z}(\overline{z} \prec z \wedge A_z(\overline{z}))$ (17)(18)

(20) $A \rightarrow \Diamond(B \vee \exists\,\overline{z}(\overline{z} \prec z \wedge A_z(\overline{z})))$ (19)

(21) $\exists\, z\ A \rightarrow \Diamond B$ (wfo)(20)

Anwendungsbeispiele

1. Türme von Hanoi (als MSTS$_s$)

   Zusätzliche Axiome:

   (TH1) $\text{exec}\ \lambda_{12}$ **exor** $\text{exec}\ \lambda_{13}$ **exor** $\text{exec}\ \lambda_{21}$ **exor** $\text{exec}\ \lambda_{23}$ **exor** $\text{exec}\ \lambda_{31}$ **exor** $\text{exec}\ \lambda_{32}$

   (TH2) $\text{exec}\ \lambda_{ij} \rightarrow p_i \neq \mathit{empty} \wedge (p_j \neq \mathit{empty} \rightarrow \mathit{top}(p_i) < \mathit{top}(p_j))$ für alle λ_{ij}

   (TH3) $\text{exec}\ \lambda_{ij} \rightarrow p_i' = \mathit{pop}(p_i) \wedge p_j' = \mathit{push}(p_j, \mathit{top}(p_i)) \wedge p_k' = p_k$ für alle λ_{ij}, $k \neq i$, $k \neq j$

   Behauptung: $\text{start}_\Gamma \rightarrow \Box B$ mit $B \equiv AG(p_1) \wedge AG(p_2) \wedge AG(p_3)$

   (1) $\text{start}_\Gamma \rightarrow B$ (data)

   (2) $\text{exec}\ \lambda_{12} \wedge B \rightarrow \bigcirc B$ (TH2)(TH3)(data)

   (3) $\text{exec}\ \lambda_{13} \wedge B \rightarrow \bigcirc B$ (TH2)(TH3)(data)

   $\vdots$

   (7) $\text{exec}\ \lambda_{32} \wedge B \rightarrow \bigcirc B$ (TH2)(TH3)(data)

   (8) B **invof** $\mathcal{A}_\Gamma$ (2)–(7)

   (9) $\text{start}_\Gamma \rightarrow \Box B$ (inv)(1)(8)

2. Berechnung der Fakultät (als FSTS$_s$)

   Zusätzliches Axiom:

   (F) $\text{exec}\ \alpha \rightarrow i > 0 \wedge i' = i - 1 \wedge \mathit{erg}' = \mathit{erg} * i$

   Behauptung: $\text{start}_\Gamma \wedge i = n \rightarrow \Diamond(\text{nil}_\Gamma \wedge \mathit{erg} = n!)$ $(n \in \mathcal{X})$

   Sei $A \equiv i = z \wedge \mathit{erg} = \frac{n!}{z!}$, $B \equiv i = 0 \wedge \mathit{erg} = n!$, $H_\alpha \equiv$ **true**.

   (1) $\text{exec}\ \alpha \wedge A \rightarrow \bigcirc(i = z - 1 \wedge \mathit{erg} = \frac{n!}{z!} * z)$ (F)

   (2) $\text{exec}\ \alpha \wedge H_\alpha \wedge A \rightarrow \bigcirc(B \vee \exists\,\overline{z}(\overline{z} < z \wedge A_z(\overline{z})))$ (1)(data)

   (3) $\text{exec}\ \alpha \wedge \neg H_\alpha \wedge A \rightarrow \bigcirc(B \vee \exists\,\overline{z}(\overline{z} \leq z \wedge A_z(\overline{z})))$ (prop)

   (4) $A \rightarrow (i = 0 \wedge \mathit{erg} = n!) \vee i > 0$ (data)

   (5) $\Box A \rightarrow \Diamond(B \vee (H_\alpha \wedge \text{enabled}_\alpha))$ (4)(ltl3)(T5)

   (6) $\exists\, z\ A \rightarrow \Diamond B$ (well)(2)(3)(5)

   (7) $\text{start}_\Gamma \wedge i = n \rightarrow \exists\, z\ A$ (data)

   (8) $B \rightarrow \neg\text{exec}\ \alpha \wedge \mathit{erg} = n!$ (F)(prop)

   (9) $\text{start}_\Gamma \wedge i = n \rightarrow \Diamond(\text{nil}_\Gamma \wedge \mathit{erg} = n!)$ (6)(7)(8)(T5)