

$$1.1) u_1 \models \Sigma_{\text{Act}} \langle \langle a \rangle \# \rangle$$

$$\langle u_1, \langle a \rangle \# \vee \langle \langle Act \rangle \# \wedge [Act] X \rangle \rangle \rightarrow \langle u_1, \langle Act \rangle \# \wedge [Act] X \rangle \rightarrow \langle u_3, X \rangle$$

$$\langle u_1, \langle Act \rangle \# \wedge [Act] X \rangle \rightarrow \langle u_3, \langle a \rangle \# \vee \langle \langle Act \rangle \# \wedge [Act] X \rangle \rangle$$

$$\rightarrow \langle u_3, \langle Act \rangle \# \wedge [Act] X \rangle \rightarrow \langle u_3, \langle Act \rangle \# \rangle$$

4.19 Definition
Sei $T = (\text{Proc}, \text{Act}, \text{Tran})$ mit S_0 definiert über Act.
Wichtigste Formeln sind gegeben wie folgt:

- $\text{Init}(t) : X \models F \wedge ActX$
- $\text{Act}(t) : X \models F \wedge ActX$
- $\text{In}(t) : X \models F \wedge (Act \vee ActX)$
- $\text{Even}(t) : X \models F \wedge (Act \wedge ActX)$
- $\text{Odd}(t) : X \models F \wedge (Act \wedge ActX)$
- $\text{GPF}(t) : X \models F \wedge (Act \wedge ActX)$

$$1.c) t_1 \models \text{Inv}(\langle a \rangle \#)$$

$$x = \langle a \rangle \# \wedge [\langle a, b \rangle] X$$

$$\langle t_1, \langle a \rangle \# \wedge [\langle a, b \rangle] X \rangle$$

$$\downarrow$$

$$\langle t_1, [\langle a, b \rangle] X \rangle$$

$$\downarrow$$

$$\langle t_2, X \rangle$$

$$\downarrow$$

$$\langle t_2, \langle a \rangle \# \wedge [\langle a, b \rangle] X \rangle$$

$$\downarrow$$

$$\langle t_2, [\langle a, b \rangle] X \rangle$$

$$\downarrow$$

$$\langle t_3, X \rangle$$

$$\downarrow$$

$$\langle t_3, \langle a \rangle \# \wedge [\langle a, b \rangle] X \rangle$$

$$\downarrow$$

$$\langle t_3, \langle a \rangle \# \rangle$$

Angreifer gewinnt

$$a) \langle s_2, \langle b \rangle \# \wedge [b] X \rangle$$

$$\downarrow$$

$$\langle s_2, \langle b \rangle \# \rangle$$

$$b) \langle s_1, \langle b \rangle \# \vee \langle \{a, b\} \rangle Y \rangle$$

$$\downarrow$$

$$\langle s_1, \langle \{a, b\} \rangle Y \rangle$$

$$\downarrow$$

$$\langle s_3, \langle b \rangle \# \vee \langle \{a, b\} \rangle Y \rangle$$

$$\downarrow$$

$$\langle s_3, \langle b \rangle \# \rangle$$

Aufgabe 1: Model-Checking

Gegeben sei folgendes LTS:



Gib an, ob die folgenden Prozesse die angegebenen Formeln erfüllen. Wenn ja, gib eine universelle Verteidigungsstrategie an. Wenn nein, gib eine universelle Angriffsstrategie an.

- 1.a) $s_2 \models X$ mit $X \equiv \langle b \rangle \# \wedge [b] X$
- 1.b) $s_1 \models Y$ mit $Y \equiv \langle b \rangle \# \vee \langle \{a, b\} \rangle Y$
- 1.c) $t_1 \models \text{Inv}(\langle a \rangle \#)$
- 1.d) $u_1 \models \text{Even}(\langle a \rangle \#)$
- 1.e) $u_1 \models [a] \text{Inv}(\langle a \rangle \#)$

6.25 Definition (Spielbewertung)

Sei $T = (\text{Proc}, \text{Act}, \text{Tran})$.

Sei $X \equiv F_X$ für $m \in \{\text{max}, \text{min}\}$.

Unendliche MC-Spiele h in T gewinnt

- die Verteidigungsseite, falls $m = \text{max}$;
- der Angriffsseite, falls $m = \text{min}$.

Endliche MC-Spiele h in T gewinnt

- die Verteidigungsseite, falls $h(z_h) \in H_a$.
- der Angriffsseite, falls $h(z_h) \in H_d$.

4.22 Definition (Spielwert)

Sei $T = (\text{Proc}, \text{Act}, \text{Tran})$.

Die Menge der MC-Spiele in T ist definiert als

- MC-Spiele $\langle X, Y \rangle$ mit $X \equiv F_X$ und $Y \equiv F_Y$ für $m \in \{\text{max}, \text{min}\}$.
- MC-Verteidigungsstrategie $\sigma \in \Sigma_{\text{Act}}$ mit $\sigma \models X$ und $\sigma \models Y$.
- MC-Angriffsstrategie $\tau \in \Sigma_{\text{Act}}$ mit $\tau \models X$ und $\tau \models Y$.

1.e)

$$\langle u_1, \langle a \rangle \# \vee \langle [\langle a \rangle] \# \wedge [Act] X \wedge \langle Act \rangle \# \rangle \rangle$$

$$\downarrow$$

$$\langle u_1, [\langle a \rangle] \# \wedge [Act] X \wedge \langle Act \rangle \# \rangle$$

$$\downarrow$$

$$\langle u_1, [Act] X \rangle$$

$$\downarrow$$

$$\langle u_3, X \rangle$$

$$\downarrow$$

$$\langle u_3, \langle a \rangle \# \vee \langle [\langle a \rangle] \# \wedge [Act] X \wedge \langle Act \rangle \# \rangle \rangle$$

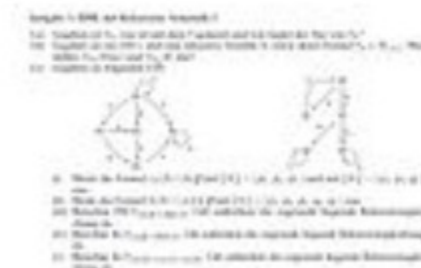
$$\downarrow$$

$$\langle u_3, [\langle a \rangle] \# \wedge [Act] X \wedge \langle Act \rangle \# \rangle$$

$$\downarrow$$

$$\langle u_3, \langle Act \rangle \# \rangle$$

Angreifer gewinnt



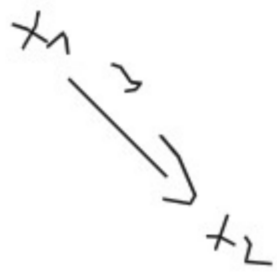
Regel 1: Eindeutigkeit der Nachfolger
 Sei A eine Aussage. Angenommen zwei Nachfolger X und Y existieren.
 (1) X ist ein Nachfolger von A .
 (2) Y ist ein Nachfolger von A .
 (3) X ist ein Nachfolger von Y .
 (4) Y ist ein Nachfolger von X .
 (5) X und Y sind äquivalent.

$$(A \Rightarrow B) \equiv \neg A \vee B$$

Entweder es gibt gar keinen Nachfolger oder es gibt einen Nachfolger, der die Eigenschaft wieder hat

2a) $X \stackrel{\text{max}}{=} Y \wedge [A \Rightarrow] X$
 $Y = [a] \text{ff} \vee \langle A \Rightarrow \rangle Y$

2b) $X \stackrel{\text{min}}{=} Y \vee \langle A \Rightarrow \rangle X$
 $Y \stackrel{\text{min}}{=} [b] \text{ff} \wedge (\langle A \Rightarrow \rangle Y \vee [A \Rightarrow] \text{ff})$



Implikationseliminierung

$$A \Rightarrow B \equiv \neg A \vee B$$

Regel 1: Eindeutigkeit der Nachfolger
 Sei A eine Aussage. Angenommen zwei Nachfolger X und Y existieren.
 (1) X ist ein Nachfolger von A .
 (2) Y ist ein Nachfolger von A .
 (3) X ist ein Nachfolger von Y .
 (4) Y ist ein Nachfolger von X .
 (5) X und Y sind äquivalent.

Regel 2: Implikationseliminierung
 Sei A, B, C Aussagen. Sei X ein Nachfolger von A .
 (1) X ist ein Nachfolger von B .
 (2) X ist ein Nachfolger von C .
 (3) X ist ein Nachfolger von $B \wedge C$.
 (4) X ist ein Nachfolger von $B \vee C$.
 (5) X ist ein Nachfolger von $B \Rightarrow C$.
 (6) X ist ein Nachfolger von $\neg B \vee C$.



1a) $X \stackrel{\text{max}}{=} [A \Rightarrow] X \wedge \langle A \Rightarrow \rangle \text{ff}$

1b) $[a] \langle b \rangle \text{ff}$

1c) $X \stackrel{\text{min}}{=} [a] \text{ff} \vee \langle [b, c] \rangle X$

1d) $X \stackrel{\text{max}}{=} [b] \langle c \rangle X \vee [a] \text{ff}$