6. Bisimulationsäquivalenz und Simulationsordnung

Ziel: · Untersuche Beziehung zwischen dem konkreten und dem abstrakten Transitionssystem.

· Wann ist der Schluss $C_A \models \varphi \Rightarrow C_C \models \varphi$ gültig?

Technisch: Zwei grundlegende Relationen zwischen Kripke-Strukturen (zustandsbeschrifteten Transitionssystemen).

Bisimulationsäquivalenz ($K_C \approx K_A$):

Die Kripke-Strukturen K_C und K_A zeigen dasselbe Transitionsverhalten (inklusive Branching).

Gut: $K_C \approx K_A$ gdw. $\forall \varphi \in CTL^*: K_C \models \varphi$ gdw. $K_A \models \varphi$.

Schlecht: · Mit diesem starken Zusammenhang enthält K_A ähnlich viel Information wie K_C.

· Deshalb unterscheidet sich die Größe kaum.

Simulationsordnung ($K_C \leq K_A$):

Die abstrakte Kripke-Struktur K_A kann das Transitionsverhalten von K_C nachahmen.

Schlechter: $\forall \varphi \in ACTL^*: K_A \models \varphi \Rightarrow K_C \models \varphi$.

$\forall \varphi \in ECTL^*: K_C \models \varphi \Rightarrow K_A \models \varphi$.

Gut: Mit diesem schwächeren Zusammenhang benötigt K_A oft deutlich weniger Zustände als K_C.

6.1 Bisimulationsäquivalenz:

Ziele: Speicherverwaltung, Entscheidbarkeit, Minimierung.

Definition (Kripke-Struktur):

Eine Kripke-Struktur ist ein Tupel $K = (AP, S, S_0, \rightarrow, \ell)$

mit · AP Menge atomarer Formeln,

· S Menge an Zuständen mit initialen Zuständen $S_0 \subseteq S$,

· $\rightarrow \subseteq S \times S$ Transitionsrelation.

- $l: S \to \mathcal{P}(AP)$ <u>Beschriftung</u>.
- Es wird <u>Deadlock-Freiheit</u> angenommen: $\forall s \in S\ \exists s' \in S: s \to s'$.
- Eine Kripke-Struktur heißt <u>endlich</u>, falls AP und S endlich sind.
- Die <u>Menge aller Kripke-Strukturen</u> ist $\mathcal{K}$.

<u>Definition (Bisimulation und Bisimulationsäquivalenz):</u>

Seien $K = (AP, S, S_0, \to, l)$ und $K' = (AP, S', S_0', \to', l')$ Kripke-Strukturen über AP.
Eine Relation $R \subseteq S \times S'$ heißt <u>Bisimulation</u> zwischen K und K', falls für alle $(s, s') \in R$ gilt:

(1) $l(s) = l(s')$

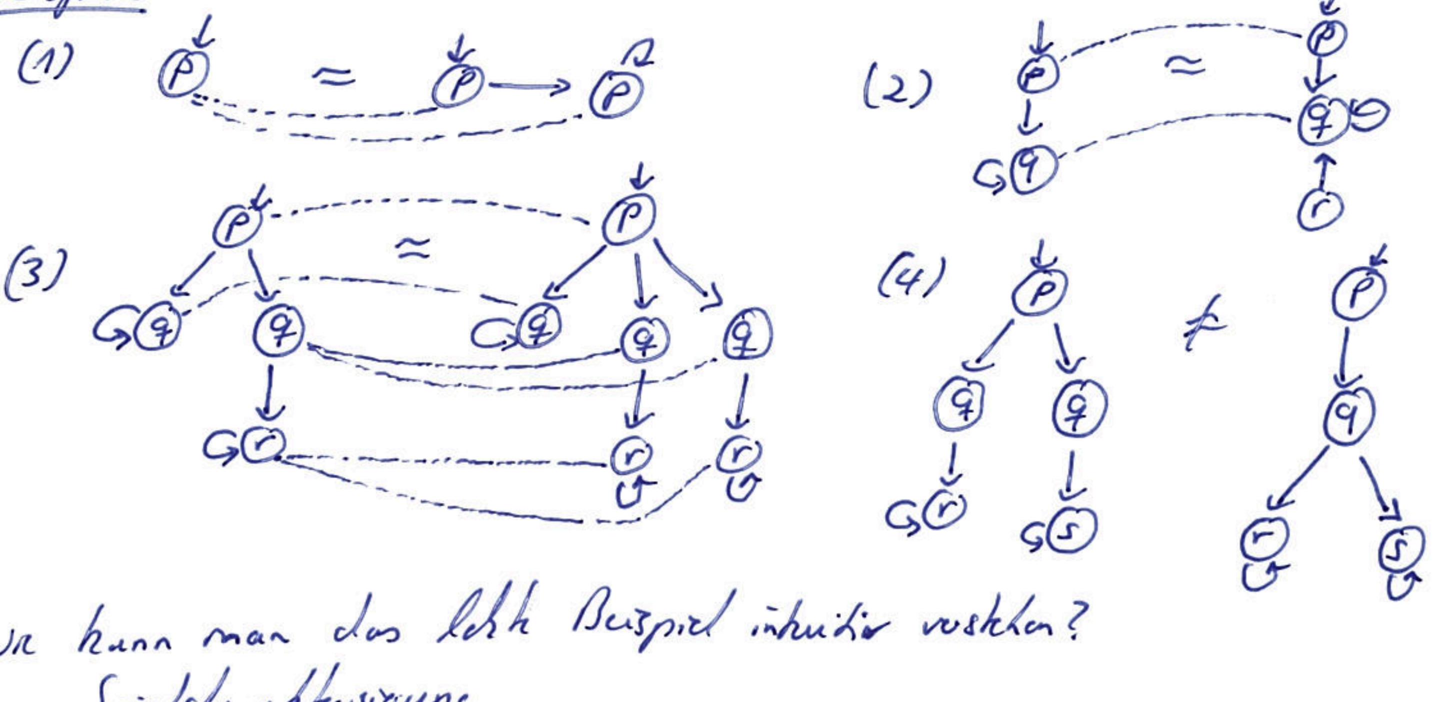
(2) $\forall t \in S: s \to t \Rightarrow \exists t' \in S': s' \to t' \wedge (t, t') \in R$.

(3) $\forall t' \in S': s' \to t' \Rightarrow \exists t \in S: s \to t \wedge (t, t') \in R$.

Die Kripke-Strukturen heißen <u>bisimulationsäquivalent</u>, $K \approx K'$, falls <u>es</u> eine Bisimulation $R \subseteq S \times S'$ <u>gibt</u>, die die initialen Zustände verbindet:

$$\forall s_0 \in S_0\ \exists s_0' \in S_0': (s_0, s_0') \in R$$
und
$$\forall s_0' \in S_0'\ \exists s_0 \in S_0: (s_0, s_0') \in R.$$

<u>Beispiel:</u>



Wie kann man das letzte Beispiel intuitiv verstehen?
Spielcharakterisierung.

Lemma:

Bisimulationsäquivalenz $\approx \subseteq \mathcal{K} \times \mathcal{K}$

ist eine Äquivalenzrelation.

Beweis:

Seien $K^i = (AP, S^i, S_0^i, \rightarrow^i, \ell^i)$ mit $i = 1, 2, 3$.

Transitivität:

Gelte $K^1 \approx K^2$ mittels R und $K^2 \approx K^3$ mittels R'.

Dann folgt

$$K^1 \approx K^3 \text{ mittels } R' \circ R = \{ (s, s'') \in S^1 \times S^3 \mid \exists s' \in S^2 : (s, s') \in R \wedge (s', s'') \in R' \}$$

Reflexivität und Symmetrie sind Übung. $\square$

6.1.1 Spielcharakterisierung

- Es gibt zwei Spieler: Attacker und Defender
- Eine Partie ist eine Folge

  $$(s_0, s_0') \rightarrow (s_1, s_1') \rightarrow (s_2, s_2') \rightarrow \ldots$$

  von Konfigurationen der Form $(s, s') \in S \times S'$.
- Die Partie verläuft in Runden,

  die jeweils in einer Konfiguration (s, s') starten

  und nach folgenden Regeln gespielt werden.

  ↳ Zunächst wählt Attacker die rechte oder linke Seite

  der aktuellen Konfiguration, zum Beispiel s.

  Dann macht er einen Zug, zum Beispiel $s \rightarrow t$.

  ↳ Defender muss nun mit einem passenden Zug

  von der anderen Seite der Konfiguration antworten,

  zum Beispiel $s' \rightarrow t'$.

  Passend heißt dabei, dass $\ell(t) = \ell'(t')$ gelten muss.

  ↳ Die Konfiguration der nächsten Runde lautet (t, t').

- Attacker gewinnt eine Partie,
  falls Defender nicht mehr auf einen Zug antworten kann.
- Verläuft die Partie unendlich lange,
  gewinnt Defender die Partie.
- Man ist nicht am Gewinn einer Partie interessiert,
  sondern am Gewinn des (Bisimulations)spiels
  Hier gewinnt Attacker / Defender,
  wenn er eine Gewinnstrategie hat:
  Egal welche Züge der Gegner macht,
  der Spieler gewinnt jede Partie,
  in der er entsprechend der Strategie spielt.

Bisimulationsspiele sind determiniert:
gegeben eine Startkonfiguration $(s,s') \in S \times S'$ mit $\ell(s) = \ell'(s')$
gewinnt einer der beiden Spieler das Bisimulationsspiel, und nicht beide.

Satz:
Betrachte Zustände $s \in S$ und $s' \in S'$.
Es gibt eine Bisimulationsrelation $R \subseteq S \times S'$ mit $(s,s') \in R$
gdw. Defender eine Gewinnstrategie von dieser Startkonfiguration hat.

6.1.2 Entscheidbarkeit

Problem: Wie entscheidet man, ob endliche Kripke-Strukturen $K, K' \in \mathcal{K}$
bisimulationsäquivalent sind.

Lemma:
$K \approx K'$ gdw. die größte Bisimulationsrelation R
die Startzustände verbindet.

Dabei ist
$$R := \bigcup_{\substack{R' \subseteq S \times S' \\ R' \text{ Bisimulation}}} R'.$$

Wie berechnet man die größte Bisimulationsrelation?

Idee:

↳ Zunächst ist die volle Relation $S \times S'$ Kandidat für eine Bisimulation.

↳ Dann werden Paare $(s, s') \in S \times S'$ entfernt, bei denen Beschriftungen oder Nachfolger nicht passen.

⇒ Fixpunkt.

Definition:

Seien $K = (AP, S, S_0, \rightarrow, l)$ und $K' = (AP, S', S_0', \rightarrow', l')$ Kripke-Strukturen.

Die Funktion

$$f_{\approx} : \mathbb{P}(S \times S') \rightarrow \mathbb{P}(S \times S')$$

ist definiert durch $(Q \subseteq S \times S')$:

$$f_{\approx}(Q) := \{ (s, s') \in Q \mid l(s) = l'(s') \}$$
$$\cap \{ (s, s') \in Q \mid \forall t : s \rightarrow t \Rightarrow \exists t' \in S' : (s' \rightarrow t' \wedge (t, t') \in Q) \}$$
$$\cap \{ (s, s') \in Q \mid \forall t' : s' \rightarrow t' \Rightarrow \exists t \in S : (s \rightarrow t \wedge (t, t') \in Q) \}$$

Lemma:

$f_{\approx}$ ist monoton.

- Da $f_{\approx}$ monoton ist, ist die Kette
$$S \times S' \supseteq f_{\approx}(S \times S') \supseteq f_{\approx}(f_{\approx}(S \times S')) \supseteq \dots$$ absteigend.

Sie konvergiert gegen den größten Fixpunkt (Satz von Kleene):
$$gfp(f_{\approx}) = f_{\approx}^{k}(S \times S') \quad \text{mit} \quad f_{\approx}^{k}(S \times S') = f_{\approx}^{k+1}(S \times S').$$

- Es bleibt zu zeigen, dass der größte Fixpunkt mit der größten Bisimulation übereinstimmt.

Dann lässt sich $gfp(f_{\approx})$ zur Entscheidung der Bisimulationsäquivalenz nutzen.

Lemma:

(1) Jeder Fixpunkt von $f_\approx$ ist eine Bisimulation.

(2) Jede Bisimulation $R' \subseteq S \times S'$ ist ein Fixpunkt von $f_\approx$.

Satz:

$gfp(f_\approx)$ ist die größte (bzgl. $\subseteq$) Bisimulation R.

Beweis:

- Mit obigem Lemma, Teil (1) gilt

$$gfp(f_\approx) \subseteq \bigcup_{\substack{R' \subseteq S \times S' \\ R' \text{ Bisimulation}}} R' = R.$$

- Umgekehrt ist R mit Teil (2) des Lemmas ein Fixpunkt von $f_\approx$.
  Mit dem Satz von Knaster & Tarski bilden die Fixpunkte wieder einen vollständigen Verband, dessen Top-Element $gfp(f_\approx)$ ist.
  Damit folgt

$$R \subseteq gfp(f_\approx).$$

- Zusammen gilt

$$R = gfp(f_\approx).$$

$\square$

Korollar:

$K \approx K'$ gdw. $gfp(f_\approx)$ die Startzustände der Kripke-Strukturen verbindet.