Concurrency Theory

Winter Semester 2015/16

Lecture 5: Fixed-Point Theory

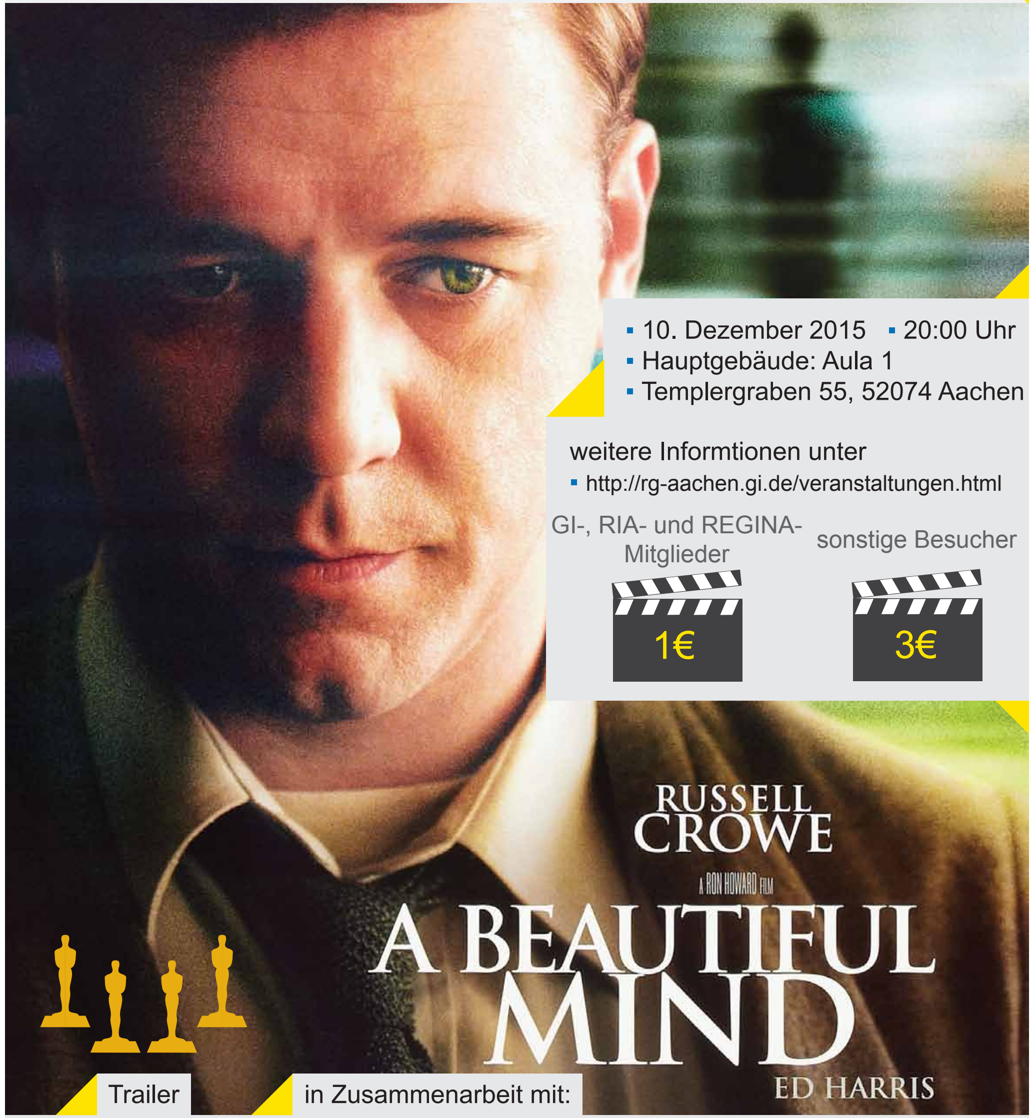
Joost-Pieter Katoen and Thomas Noll
Software Modeling and Verification Group
RWTH Aachen University

http://moves.rwth-aachen.de/teaching/ws-1516/ct/

Software Modeling and Verification Chair

RWTH AACHEN UNIVERSITY

GI - Filmaufführungen



- 10. Dezember 2015
- 20:00 Uhr
- Hauptgebäude: Aula 1
- Templergraben 55, 52074 Aachen

weitere Informtionen unter

- http://rg-aachen.gi.de/veranstaltungen.html

GI-, RIA- und REGINA-Mitglieder	sonstige Besucher
1€	3€

Trailer

in Zusammenarbeit mit:

INFORMATIK RWTH AACHEN

Filmstudio an der RWTH Aachen e.V.

Fachschaft Mathematik-Physik-Informatik RWTH Aachen

RIA GI

Regionalgruppe Informatik Aachen der Gesellschaft für Informatik (GI)

„John Nash ist ein genialer Mathematiker mit einer großen Breite (Nash-Gleichgewicht in der Spieltheorie, reelle algebraische Mannigfaltigkeiten, Differentialgeometrie, partielle Differentialgleichungen), ausgebildet und tätig an den Elite-Universitäten im Osten der USA. Er ist aber auch etwas seltsam: Kommunikationsarm, hochnäsig und mit wenig Empathie. Nach seinem steilen Aufstieg zu Ruhm beginnt eine absonderliche Filmgeschichte, die man auf den ersten Blick dem üblichen Hollywood-Klamauk zuordnet...“

Introducing Recursion

Solution: employ recursion!

- $Inv(\langle a\rangle tt) \equiv \langle a\rangle tt \wedge [a]\, Inv(\langle a\rangle tt)$
- $Pos([a]ff) \equiv [a]ff \vee \langle a\rangle\, Pos([a]ff)$

Interpretation: the sets of states $X, Y \subseteq S$ satisfying the respective formula should solve the corresponding equation, i.e.,

- $X = \langle \cdot a \cdot \rangle(S) \cap [\cdot a \cdot](X)$
- $Y = [\cdot a \cdot](\emptyset) \cup \langle \cdot a \cdot \rangle(Y)$

Open questions

- Do such recursive equations (always) have solutions?
- If so, are they unique?
- How can we compute whether a process satisfies a recursive formula?

Recap: Hennessy-Milner Logic with Recursion

Syntax of HML with One Recursive Variable

Initially: only one variable

Later: mutual recursion

Definition (Syntax of HML with one variable)

The set HMF_X of Hennessy-Milner formulae with one variable X over a set of actions Act is defined by the following syntax:

$$
\begin{array}{rlll}
F ::= & X & & \text{(variable)} \\
| & \mathrm{tt} & & \text{(true)} \\
| & \mathrm{ff} & & \text{(false)} \\
| & F_1 \wedge F_2 & & \text{(conjunction)} \\
| & F_1 \vee F_2 & & \text{(disjunction)} \\
| & \langle \alpha \rangle F & & \text{(diamond)} \\
| & [\alpha] F & & \text{(box)}
\end{array}
$$

where $\alpha \in Act$.

Semantics of HML with One Recursive Variable I

So far: $[\![F]\!] \subseteq S$ for $F \in HMF$ and LTS $(S, Act, \longrightarrow)$
Now: semantics of formula depends on states that (are assumed to) satisfy X

Definition (Semantics of HML with one variable)

Let $(S, Act, \longrightarrow)$ be an LTS and $F \in HMF_X$. The semantics of F,

$$[\![F]\!] : 2^S \to 2^S,$$

is defined by

$$\begin{aligned}
[\![X]\!](T) &:= T \\
[\![\mathrm{tt}]\!](T) &:= S \\
[\![\mathrm{ff}]\!](T) &:= \emptyset \\
[\![F_1 \wedge F_2]\!](T) &:= [\![F_1]\!](T) \cap [\![F_2]\!](T) \\
[\![F_1 \vee F_2]\!](T) &:= [\![F_1]\!](T) \cup [\![F_2]\!](T) \\
[\![\langle\alpha\rangle F]\!](T) &:= \langle\cdot\alpha\cdot\rangle([\![F]\!](T)) \\
[\![[\alpha]F]\!](T) &:= [\cdot\alpha\cdot]([\![F]\!](T))
\end{aligned}$$

Semantics of HML with One Recursive Variable II

- Idea underlying the definition of

$$[\![.]\!] : HMF_X \to (2^S \to 2^S) :$$

  if $T \subseteq S$ gives the set of states that satisfy X, then $[\![F]\!](T)$ will be the set of states that satisfy F
- How to determine this T?
- According to previous discussion: as solution of recursive equation of the form $X = F_X$ where $F_X \in HMF_X$
- But: solution not unique; therefore write:

$$X \overset{min}{=} F_X \qquad \text{or} \qquad X \overset{max}{=} F_X$$

- In the following we will see:
  1. Equation $X = F_X$ always solvable
  2. Least and greatest solutions are unique and can be obtained by fixed-point iteration

Partial Orders

Definition 5.1 (Partial order)

A partial order (PO) $(D, \sqsubseteq)$ consists of a set D, called domain, and of a relation $\sqsubseteq \subseteq D \times D$ such that, for every $d_1, d_2, d_3 \in D$,

reflexivity: $d_1 \sqsubseteq d_1$

transitivity: $d_1 \sqsubseteq d_2$ and $d_2 \sqsubseteq d_3 \implies d_1 \sqsubseteq d_3$

antisymmetry: $d_1 \sqsubseteq d_2$ and $d_2 \sqsubseteq d_1 \implies d_1 = d_2$

It is called total if, in addition, always $d_1 \sqsubseteq d_2$ or $d_2 \sqsubseteq d_1$.

Example 5.2

1. $(\mathbb{N}, \leq)$ is a total partial order
2. $(\mathbb{N}, <)$ is not a partial order (since not reflexive)
3. $(2^{\mathbb{N}}, \subseteq)$ is a (non-total) partial order
4. $(\Sigma^*, \sqsubseteq)$ is a (non-total) partial order, where Σ is some alphabet and $\sqsubseteq$ denotes prefix ordering ($u \sqsubseteq v \iff \exists w \in \Sigma^* : uw = v$)

Upper and Lower Bounds

Definition 5.3 ((Least) upper bounds and (greatest) lower bounds)

Let $(D, \sqsubseteq)$ be a partial order and $T \subseteq D$.

1. An element $d \in D$ is called an upper bound of T if $t \sqsubseteq d$ for every $t \in T$ (notation: $T \sqsubseteq d$). It is called least upper bound (LUB) (or supremum) of T if additionally $d \sqsubseteq d'$ for every upper bound d' of T (notation: $d = \bigsqcup T$).
2. An element $d \in D$ is called an lower bound of T if $d \sqsubseteq t$ for every $t \in T$ (notation: $d \sqsubseteq T$). It is called greatest lower bound (GLB) (or infimum) of T if $d' \sqsubseteq d$ for every lower bound d' of T (notation: $d = \bigsqcap T$).

Example 5.4

1. $T \subseteq \mathbb{N}$ has a LUB/GLB in $(\mathbb{N}, \leq)$ iff it is finite/non-empty
2. In $(2^{\mathbb{N}}, \subseteq)$, every subset $T \subseteq 2^{\mathbb{N}}$ has an LUB and GLB:

$$\bigsqcup T = \bigcup T \qquad \text{and} \qquad \bigsqcap T = \bigcap T$$

Complete Lattices

Definition 5.5 (Complete lattice)

A complete lattice is a partial order $(D, \sqsubseteq)$ such that all subsets of D have LUBs and GLBs. In this case,

$$\bot := \bigsqcup \emptyset \; (= \bigsqcap D) \qquad \text{and} \qquad \top := \bigsqcap \emptyset \; (= \bigsqcup D)$$

respectively denote the least and greatest element of D.

Example 5.6

1. $(\mathbb{N}, \leq)$ is not a complete lattice as, e.g., $\mathbb{N}$ does not have a LUB
2. $(\mathbb{N} \cup \{\infty\}, \leq)$ with $n \leq \infty$ for all $n \in \mathbb{N}$ is a complete lattice
3. $(2^{\mathbb{N}}, \subseteq)$ is a complete lattice

Application to HML with Recursion

Lemma 5.7

Let $(S, Act, \longrightarrow)$ *be an LTS. Then* $(2^S, \subseteq)$ *is a complete lattice with*

- $\bigsqcup \mathcal{T} = \bigcup \mathcal{T} = \bigcup_{T \in \mathcal{T}} T$ *for all* $\mathcal{T} \subseteq 2^S$
- $\bigsqcap \mathcal{T} = \bigcap \mathcal{T} = \bigcap_{T \in \mathcal{T}} T$ *for all* $\mathcal{T} \subseteq 2^S$
- $\bot = \bigsqcup \emptyset = \bigsqcap 2^S = \emptyset$
- $\top = \bigsqcap \emptyset = \bigsqcup 2^S = S$

Proof.

omitted □

Fixed Points

Definition 5.8 (Fixed point)

Let D be some domain, $d \in D$, and $f : D \to D$. If

$$f(d) = d$$

then d is called a fixed point of f.

Example 5.9

1. The (only) fixed points of $f_1 : \mathbb{N} \to \mathbb{N} : n \mapsto n^2$ are 0 and 1
2. A subset $T \subseteq \mathbb{N}$ is a fixed point of $f_2 : 2^{\mathbb{N}} \to 2^{\mathbb{N}} : T \mapsto T \cup \{1, 2\}$ iff $\{1, 2\} \subseteq T$

Monotonicity of Functions

Definition 5.10 (Monotonicity)

Let $(D, \sqsubseteq)$ and $(D', \sqsubseteq')$ be partial orders. A function $f : D \to D'$ is called monotonic (w.r.t. $(D, \sqsubseteq)$ and $(D', \sqsubseteq')$) if, for every $d_1, d_2 \in D$,

$$d_1 \sqsubseteq d_2 \implies f(d_1) \sqsubseteq' f(d_2).$$

Example 5.11

1. $f_1 : \mathbb{N} \to \mathbb{N} : n \mapsto n^2$ is monotonic w.r.t. $(\mathbb{N}, \leq)$
2. $f_2 : 2^{\mathbb{N}} \to 2^{\mathbb{N}} : T \mapsto T \cup \{1, 2\}$ is monotonic w.r.t. $(2^{\mathbb{N}}, \subseteq)$
3. Let $\mathcal{T} := \{T \subseteq \mathbb{N} \mid T \text{ finite}\}$. Then $f_3 : \mathcal{T} \to \mathbb{N} : T \mapsto \sum_{n \in T} n$ is monotonic w.r.t. $(2^{\mathbb{N}}, \subseteq)$ and $(\mathbb{N}, \leq)$.
4. $f_4 : 2^{\mathbb{N}} \to 2^{\mathbb{N}} : T \mapsto \mathbb{N} \setminus T$ is not monotonic w.r.t. $(2^{\mathbb{N}}, \subseteq)$ (since, e.g., $\emptyset \subseteq \mathbb{N}$ but $f_4(\emptyset) = \mathbb{N} \not\subseteq f_4(\mathbb{N}) = \emptyset$).

The Fixed-Point Theorem I

Alfred Tarski (1901–1983)

Theorem 5.12 (Tarski's fixed-point theorem)

Let $(D, \sqsubseteq)$ be a complete lattice and $f : D \to D$ monotonic. Then f has a least fixed point $\mathrm{fix}(f)$ and a greatest fixed point $\mathrm{FIX}(f)$ given by

$$\mathrm{fix}(f) = \bigsqcap\{d \in D \mid f(d) \sqsubseteq d\} \qquad \textit{(GLB of all pre-fixed points of } f\textit{)}$$

$$\mathrm{FIX}(f) = \bigsqcup\{d \in D \mid d \sqsubseteq f(d)\} \qquad \textit{(LUB of all post-fixed points of } f\textit{)}$$

Proof.

on the board □

The Fixed-Point Theorem II

Example 5.13 (cf. Example 5.9)

- Let $f : 2^{\mathbb{N}} \to 2^{\mathbb{N}} : T \mapsto T \cup \{1,2\}$
- As seen before: $f(T) = T$ iff $\{1,2\} \subseteq T$
- Theorem 5.12 for fix:

$$\begin{aligned}\mathrm{fix}(f) &= \bigsqcap\{d \in D \mid f(d) \sqsubseteq d\}\\ &= \bigcap\{T \subseteq \mathbb{N} \mid f(T) \subseteq T\}\\ &= \bigcap\{T \subseteq \mathbb{N} \mid T \cup \{1,2\} \subseteq T\}\\ &= \bigcap\{T \subseteq \mathbb{N} \mid \{1,2\} \subseteq T\}\\ &= \{1,2\}\end{aligned}$$

- Theorem 5.12 for FIX:

$$\begin{aligned}\mathrm{FIX}(f) &= \bigsqcup\{d \in D \mid d \sqsubseteq f(d)\}\\ &= \bigcup\{T \subseteq \mathbb{N} \mid T \subseteq f(T)\}\\ &= \bigcup\{T \subseteq \mathbb{N} \mid T \subseteq T \cup \{1,2\}\}\\ &= \bigcup 2^{\mathbb{N}}\\ &= \mathbb{N}\end{aligned}$$

The Fixed-Point Theorem for Finite Lattices

Theorem 5.14 (Fixed-point theorem for finite lattices)

Let $(D, \sqsubseteq)$ *be a finite complete lattice and* $f : D \to D$ *monotonic. Then*

$$\text{fix}(f) = f^m(\bot) \quad \textit{and} \quad \text{FIX}(f) = f^M(\top)$$

for some $m, M \in \mathbb{N}$ *where* $f^0(d) := d \quad \textit{and} \quad f^{k+1}(d) := f(f^k(d))$.

Proof.

on the board □

Example 5.15

- Let $f : 2^{\{0,1\}} \to 2^{\{0,1\}} : T \mapsto T \cup \{0\}$
- $f^0(\bot) = \emptyset$, $f^1(\bot) = \{0\}$, $f^2(\bot) = \{0\} = f^1(\bot)$
  $\implies \text{fix}(f) = \{0\}$ for $m = 2$
- $f^0(\top) = \{0, 1\}$, $f^1(\top) = \{0, 1\} = f^0(\top)$
  $\implies \text{FIX}(f) = \{0, 1\}$ for $M = 1$

Application to HML with Recursion

Lemma 5.16

Let $(S, Act, \longrightarrow)$ be an LTS and $F \in HMF_X$. Then

1. $[\![F]\!] : 2^S \to 2^S$ *is monotonic w.r.t.* $(2^S, \subseteq)$
2. $\text{fix}([\![F]\!]) = \bigcap\{T \subseteq S \mid [\![F]\!](T) \subseteq T\}$
3. $\text{FIX}([\![F]\!]) = \bigcup\{T \subseteq S \mid T \subseteq [\![F]\!](T)\}$

If, in addition, S is finite, then

4. $\text{fix}([\![F]\!]) = [\![F]\!]^m(\emptyset)$ *for some* $m \in \mathbb{N}$
5. $\text{FIX}([\![F]\!]) = [\![F]\!]^M(S)$ *for some* $M \in \mathbb{N}$

Proof.

1. by induction on the structure of F (details omitted)
2. by Lemma 5.7 and Theorem 5.12
3. by Lemma 5.7 and Theorem 5.12
4. by Lemma 5.7 and Theorem 5.14
5. by Lemma 5.7 and Theorem 5.14 □