Discrete Structures II

Ulf Nilsson
TCSLAB, IDA, LiU

LiU expanding reality

Fixed points

LiU expanding reality

Fixed points

Definition Consider an operation $f\colon A \to A$. An element $a \in A$ is called a *fixed point* of f iff $f(a) = a$.

Some questions

- When does f have a fixed point?
- Which are the preferable fixed point(s), when more than one?
- How can we compute fixed points?

Properties of functions

Definition Let $(A, \leq)$ be a poset. A function $f\colon A \to A$ is said to be

- *monotone* (order-preserving) iff $f(x) \leq f(y)$ whenever $x \leq y$.
- *antimonotone* iff $f(x) \geq f(y)$ whenever $x \leq y$.
- *inflationary* iff $x \leq f(x)$ for all $x \in A$.
- *idempotent* iff $f(f(x)) = f(x)$ for all $x \in A$.

Continuous maps

Definition A function $f\colon A \to A$ is *continuous* if it preserves existing least upper bounds; i.e. if $B \subseteq A$ and $\bigvee B$ exists, then $\bigvee \{f(x) \mid x \in B\}$ exists and equals $f(\bigvee B)$.

Definition Let $(A, \leq)$ be a cpo. A function $f\colon A \to A$ is called (chain-) *continuous* if

$$f(\bigvee\{x_0, x_1, x_2, \ldots\}) = \bigvee\{f(x_0), f(x_1), f(x_2), \ldots\}$$

for every ascending chain $x_0 < x_1 < x_2 < \ldots$ in A.

Continuous maps II

Definition Let $(A, \leq)$ be a complete lattice. A function $f\colon A \to A$ is *continuous* if

$$f(\bigvee B) = \bigvee\{f(x) \mid x \in B\}$$

for every $B \subseteq A$.

Theorem Every continuous map is monotonic.

Theorem If $f\colon A \to A$ is monotone and A is finite, then f must be continuous.

Pre- and post-fixed points

Definition Let $(A, \leq)$ be a poset and consider a map $f\colon A \to A$. An $x \in A$ such that $f(x) \leq x$ is called a *pre-fixed point* of f. Similarly $x \in A$ is called a *post-fixed point* of f iff $x \leq f(x)$.

Knaster-Tarski's theorem

Theorem Let $(A, \leq)$ be a complete lattice and $f\colon A \to A$ monotone. Then $\bigwedge\{x \in A \mid f(x) \leq x\}$ is the least fixed point of f, and $\bigvee\{x \in A \mid x \leq f(x)\}$ is the greatest fixed point of f.

Theorem Let $(A, \leq)$ be a cpo and $f\colon A \to A$ monotone. Then f has a least fixed point.

Notation

The least fixed point of f is denoted $\text{LFP}(f)$. Alternatively

$$\mu x.f(x)$$

with reading: the least x such that $f(x) = x$.

The greatest fixed point of f is denoted $\text{GFP}(f)$, alternatively

$$\nu x.f(x).$$

Kleene's fixed point theorem

Theorem Let $(A, \leq)$ be a cpo (or a complete lattice) and assume that $f\colon A \to A$ is continuous. Then $f^\omega(\bot)$ is the least fixed point of f.

Note that

$$f^\omega(\bot) = \bigvee_{n<\omega} f^n(\bot).$$

That is, $\text{LFP}(f)$ is the least upper bound of the Kleene sequence,

$$\bot, f(\bot), f^2(\bot), \ldots, f^n(\bot), \ldots$$

Finite automata on infinite words

Automata based verification

Input:

- A set of all possible system behaviors, modeled by a set of ω-words (typically encoded as a Büchi automaton);
- A set of allowed behaviors, expressed in a temporal logic (typically LTL, Linear time logic) which translates into a Büchi automaton;

Automata based verification II

Aim:

- To check if allowed behaviors contain system behavior; i.e. if $\mathcal{L}(\mathit{System}) \subseteq \mathcal{L}(\mathit{Spec})$

Alternatively:

- Check (non-)emptiness of $\mathcal{L}(\mathit{System}) \cap \overline{\mathcal{L}(\mathit{Spec})}$

Finite languages

- A a finite alphabet
- A^* the set of finite strings over A
- Notation: $u, v, w \in A^*$ and $U, V, W \subseteq A^*$
- Concatenation: $U.V$
- Union: $U + V$
- Finite iteration: U^*

Infinite languages

- A a finite alphabet
- A^ω the set of (countably) infinite words over A (so called ω-words)
- Notation: $\alpha, \beta, \gamma \in A^\omega$ and $L \subseteq A^\omega$
- Infinite iteration:

$$U^\omega = \{\alpha \in A^\omega \mid \exists w_1 w_2 \ldots \in U, \alpha = w_1 w_2 \ldots\}.$$

Büchi automata

Definition A Büchi automaton $\mathcal{B}$ over an alphabet A is a tuple (Q, q_0, Δ, F) where Q is a finite set of *states*, $q_0 \in Q$ an *initial state*, $\Delta \subseteq Q \times A \times Q$ a *transition relation* and $F \subseteq Q$ a set of *accepting*, or *final*, states.

Definition A *run* of a Büchi automaton $\mathcal{B} = (Q, q_0, \Delta, F)$ on an ω-word α is an infinite word of states $\sigma \in Q^\omega$ such that $\sigma(0) = q_0$ and $(\sigma(i), \alpha(i), \sigma(i+1)) \in \Delta$ for all $i \geq 0$.

Büchi automata (cont)

- Let $\inf(\sigma)$ be the set of all states that occur infinitely often in the ω-word σ.
- An ω-word α is *accepted* by a Büchi automaton $\mathcal{B}$ iff there is a run σ on α such that $F \cap \inf(\sigma) \neq \emptyset$.
- The ω-language of a Büchi automaton $\mathcal{B}$,

$$\mathcal{L}(\mathcal{B}) = \{\alpha \mid \mathcal{B} \text{ accepts } \alpha\}.$$

- An ω-language definable by some Büchi automaton is said to be Büchi recognizable.

Closure properties

Theorem If $L_1, L_2 \subseteq A^\omega$ are Büchi recognizable languages, then so are $L_1 \cup L_2$ and $L_1 \cap L_2$.

Proposition If $U \subseteq A^*$ is regular, then U^ω is Büchi recognizable.

Proposition If $U \subseteq A^*$ is regular and $L \subseteq A^\omega$ is Büchi recognizable then so is $U.L$.

ω-regular languages

Theorem An ω-language L is Büchi recognizable iff there is some $n \geq 0$ and regular languages of finite words, U_i and V_i where $1 \leq i \leq n$, such that

$$L = \bigcup_{i=1}^{n} U_i.(V_i)^\omega.$$

Such languages are called ω-regular languages.

Emptiness and containment

Theorem The nonemptiness problem for Büchi automata is decidable and solvable in O(m+n) time, where m is the number of states, and n the number of transitions.

Note that

$$L_1 \subseteq L_2 \text{ iff } L_1 \cap \overline{L_2} = \emptyset.$$

Complementation of Büchi automata

Büchi automata *are* closed under complementation.

Theorem If L is Büchi recognizable, then so is $A^\omega \setminus L$.

- Relatively easy to complement deterministic Büchi (but the result is non-deterministic Büchi).
- Complementing non-deterministic Büchi is *very* complicated!

More on complementation

Let $W \subseteq A^*$ be a regular language and let

$$\lim W = \{\alpha \in A^\omega \mid \forall m \geq 0\ \exists n > m \text{ s.t. } \alpha(0)\ldots\alpha(n) \in W\}.$$

Then

Theorem An ω-language L is deterministically Büchi recognizable iff there is some regular language $W \subseteq A^*$ such that $L = \lim W$.

Theorem The language $(a+b)^* b^\omega$ is not deterministically Büchi recognizable.

Muller automata

Definition A Muller automaton $\mathcal{B}$ over an alphabet A is a tuple (Q, q_0, Δ, F) where Q is a finite set of *states*, $q_0 \in Q$ an *initial state*, $\Delta \subseteq Q \times A \times Q$ a *transition relation* and $F \subseteq 2^Q$ a set of sets of *accepting states*.

Definition An ω-word α is accepted by a Muller automaton $\mathcal{B}$ iff there exists a run σ on α such that $\inf(\sigma) \in F$.

McNaughton's theorem

Theorem If L is deterministically Muller recognizable, then L is (non-deterministically) Büchi recognizable.

General idea:

- "Guess" when we enter a set F_j of accepting states,
- Make sure that we never leave F_j,
- Make sure that all states in F_j are visited infinitely often.

McNaughton's theorem (Part 2)

Theorem If L is (nondeterministically) Büchi recognizable, then L is deterministically Muller recognizable.

A Safra tree over Q is a finite, ordered tree with nodes from the set $\{1, 2, \ldots, 2 \cdot |Q|\}$ where

- Each node is labeled by some $R \subseteq Q$,
- Siblings have disjoint labels,
- The union of all siblings is a proper subset of the parent.

Some nodes may be marked as final.

Safra's construction

Let $B = (Q, q_0, \Delta, F)$ be a Büchi automaton, and let $M = (Q', q'_0, \Delta', F')$ be a Muller automaton where

- Q' is the set of Safra trees over Q
- q'_0 is the Safra tree consisting of a node labeled $\{q_0\}$ (marked as final if $q_0 \in F$),
- A set S of Safra trees is in F' iff some node name appears in each $t \in S$, and in some $t \in S$ this node name is marked as final,
- and $\Delta'(q, a) = \ldots$

Safra's construction (cont.)

...and $\Delta'(q, a) = \ldots$

1. For each node n (labeled S_n) in q, apply the powerset construction on input a. Mark n as non-final.
2. For each node in this tree whose label contains a final state, branch off a new son containing the final states (pick a free name in $\{1, 2, \ldots, 2 \cdot |Q|\}$). Mark the new node as final.
3. Remove a state q from a node (and all its descendants) if q appears in a left sibling. Remove all nodes labeled by empty set (apart from the root).
4. For each node n, remove all descendants if their union equals the label of n. If so, mark n as final.

Complementation of Muller automata

Theorem If (Q, q_0, Δ, F) is a deterministic Muller automaton accepting $L \subseteq A^\omega$, then $(Q, q_0, \Delta, 2^Q \setminus F)$ accepts $A^\omega \setminus L$, i.e. the complement of L.

Problem is subject to active research...