CS4820, Fall 2021, Lecture 27

Pete Manolios

Nov 15, 2021

Contents

1 Review Schedule for paper presentations

Elided

2 Rewriting

Rewriting is a powerful theorem proving technique and we have already seen it in action in ACL2s, so we won't say much in terms of motivation initially. Term rewriting is essential in understanding lambda calculus.

2.1 Basic Definitions

- *Abstract Reduction relation*: Binary relation, R on a set X
  - we may write $x \to y$ instead of $R(x, y)$
  - typically derived from set of equalities ($l = r$) via instantiation, but can be any relation
- Closures

- *transitive closure* of $\rightarrow$: $\rightarrow^+$ (Kleene notation)
- *reflexive, transitive closure* of $\rightarrow$: $\rightarrow^*$ (Kleene notation)

- *Normal form*: x is in normal form iff there is no y s.t. $x \rightarrow y$
- *Terminating, Strongly normalizing, Noetherian* (all mean same thing)
  - There is no infinite sequence $x_0 \rightarrow \cdots \rightarrow x_n \rightarrow \cdots$
- *Reverse relation*: Define $x < y$ to be $y \rightarrow x$; now notice
  - x is in normal form iff it is minimal wrt $<$
  - $\rightarrow$ is terminating if $<$ is well-founded (no infinite decreasing sequences)
- Relation to ACL2s, concepts such as termination, induction, etc.
  - In ACL2s, we reason about functions: termination, induction
  - In ACL2s, we don't (typically) reason about rewrite rules
  - But, we could and the same techniques for termination, induction can be used

2.2 Confluence

- $\rightarrow$ has the *diamond property*:
  - if $x \rightarrow y$ and $x \rightarrow y'$, $\exists z$ s.t. $y \rightarrow z$ and $y' \rightarrow z$
- $\rightarrow$ is *confluent*: $\rightarrow^*$ has the diamond property
  - if $x \rightarrow^* y$ and $x \rightarrow^* y'$, $\exists z$ s.t. $y \rightarrow^* z$ and $y' \rightarrow^* z$
- $\rightarrow$ is *weakly confluent*:
  - if $x \rightarrow y$ and $x \rightarrow y'$, $\exists z$ s.t. $y \rightarrow^* z$ and $y' \rightarrow^* z$
- $x \downarrow y$ (x and y are *joinable*): $\exists z$ s.t. $x \rightarrow^* z$ and $y \rightarrow^* z$
  - $\rightarrow$ is confluent: if $x \rightarrow^* y$ and $x \rightarrow^* y'$, then $y \downarrow y'$
  - $\rightarrow$ is weakly confluent: if $x \rightarrow y$ and $x \rightarrow y'$, then $y \downarrow y'$
- Theorem if $\rightarrow$ has the diamond property, it is weakly confluent
  - Proof: trivial, as $y \rightarrow z$ implies $y \rightarrow^* z$

- Theorem if $\to$ has the diamond property, it is confluent
  - Proof: double induction on length of $x \to^* y$ and $x \to^* y'$, picture (see book) makes it clear
- Theorem: if $\to$ is confluent, it is weakly confluent
  - Proof: trivial, as $x \to y$ implies $x \to^* y$
- Weak confluence does not imply confluence; consider
  - Define $\to$ as follows
    * $b \to a$
    * $b \to c$
    * $c \to b$
    * $c \to d$
  - Note that $\to$ is weakly confluent
  - but not confluent: $c \to^* a$ and $c \to^* d$, but $a \not\downarrow d$

2.3 Newman's Lemma (1942)

- If $\to$ is terminating and weakly confluent, then it is confluent
- Proof: By well-founded induction on $P(x) = \forall y, z : x \to^* y \wedge x \to^* z : y \downarrow z$
  - C1 (Context): $\to$ is terminating (hyp)
  - C2: $\to$ is weakly confluent (hyp)
  - C3: $\forall u : x \to^+ u : P(u)$ (IH)
  - C4: $x \to^* y \wedge x \to^* z$ (hyp of confluence)
  - D1: $x = y$ or $x = z$, then $y \downarrow z$ (C1, so no steps taken)
  - D2: $x \neq y$, $x \neq z$, (D1, PL)
  - D3: $\exists y_1, z_1 : x \to y_1 \to^* y$ and $x \to z_1 \to^* z$ (C4, D2)
  - D4: $\exists u : y_1 \to^* u$ and $z_1 \to^* u$ (C2, D3)
  - D5: $\exists v : u \to^* v$ and $y \to^* v$ ($P(y_1)$: C3, $x \to y_1$: D3, $y_1 \to^* y$: D3, $y_1 \to^* u$: D4)
  - D6: $\exists w : v \to^* w$ and $z \to^* w$ ($P(z_1)$: C3, $x \to z_1$, D3 ($z_1 \to^* z$), D4,D5 ($z_1 \to^* u \to^* v$))
  - D7: $y \downarrow z$ ($y \to *v \to^* w$: D5,D6, $z \to^* w$: D6)

2.4 Church-Rosser

- $\leftrightarrow^*$ is the reflexive, symmetric, transitive closure of $\rightarrow$
- $\rightarrow$ is *Church-Rosser*: if $x \leftrightarrow^* y$ then $x \downarrow y$
- Theorem: Church-Rosser is equivalent to confluence
- Proof:
  - Pong: Confluence is special case of Church-Rosser, since if $x \rightarrow^* y$ and $x \rightarrow^* y'$ then $y \leftrightarrow^* y'$
  - Ping: See book