CS4820, Fall 2021, Lecture 31

Pete Manolios

Nov 29, 2021

Contents

1 Exam 2: Dec 2nd

- Up to material covered to end of November
- Focus on material after exam 1
- Take home option: due midnight on Thursday. Released after class.

2 Presentations

- See the schedule: next week

3 Term Rewrite Systems

3.1 Basic Definitions

- *Rewrite rule*: an equation $l = r$, ofter written $l \to r$ such that
  - l is not a var
  - $\mathit{Vars}(l) \subseteq \mathit{Vars}(r)$
    - book doesn't require this, neither does ACL2s, but standard
- *Term Rewrite System* (TRS)
  - a set of rewrite rules
- *Reduction relation* for Term Rewrite System R, $\to_R$:
  - Pairs (s, t) st. t is s after applying a rewrite rule
  - $\{(s, t) \mid \exists (l, r) \in R$ st. s has subterm $l\sigma$, for some substitution σ and t is s with the subterm replaced by $r\sigma\}$
- We may drop the subscript and write $\to$ instead of $\to_R$
- Above fleshes out how to relate Term Rewriting Systems with Reduction Relations, something we considered last time
- A reduction relation is *canonical* (or *convergent*) iff it is terminating and confluent
- $\to_R$ is canonical iff it is terminating & locally confluent (Newman's lemma)
- If $\to_R$ is canonical, every term has a unique normal form (last time)
- If s has a unique normal form, we write it as $s \downarrow_R$

3.2 Equational Reasoning

3.2.1 Main Question: Validity

- Given E, a set of equalities (eg, TRS), prove $E \models s = t$
- Alternatively, prove $s \leftrightarrow_E^* t$
  - where $\leftrightarrow_E^*$ is the reflexive, symmetric, transitive closure of the reduction relation of E.
  - follows from Birkoff's theorem
- Theorem: if $\rightarrow_E$ is canonical, then $s \leftrightarrow_E^* t$ is decidable
  - Proof Sketch:
    - C1: $\rightarrow_E$ is canonical
    - D1: $s \leftrightarrow_E^* t$ iff $s \downarrow_E = t \downarrow_E$ {C1, Previous Results}
    - D2: $\downarrow_E$ is decidable: given s check if there is a subterm that can we rewrited with $\rightarrow_E$, which requires matching (special case of unification) & substitution, hence decidable; by {C1} we can only do this finitely many times, hence decidable.
    - D3: $s \leftrightarrow_E^* t$ is decidable {D1, D2}

3.3 Motivating Example for Completion

- Consider the rules R
  - $f(f(x, y), z) \rightarrow f(x, f(y, z))$
  - $f(i(x), x) \rightarrow e$
- Can we decide $R \models s = t$ using above theorem (canonicity)?
  - Termination: yes (we won't focus on that here)
  - Confluent?
    - Consider $s = f(f(i(x), x), z)$
    - Apply rule 1 to s: $f(i(x), f(x, z))$
    - Apply rule 2 to s: $f(e, z)$
    - Notice that the new terms are irreducible (in normal form)
    - So, not confluent
    - We found an s which can be rewritten to non-joinable terms

- But, we now have a proof that $f(i(x), f(x,z)) = f(e,z)$
- So, add rule 3, to define R_1
  - $f(f(x,y)z) \to f(x, f(y,z))$
  - $f(i(x), x) \to e$
  - $f(i(x), f(x,z)) \to f(e,z)$
- Note that $\leftrightarrow^*$ has not changed
- But, we can now use the above theorem
  - Termination holds
  - So does confluence
    * But how do we prove that?
    * Do we have to prove confluence directly? (Painful)
    * We can prove local confluence (Newman's Lemma)
    * We can do better
- Theorem: A TRS is locally confluent iff all of its critical pairs are joinable.
  - So, enough to consider a subset of all terms, using the idea of critical pairs.
  - For a finite TRS, there are finitely many critical pairs and checking joinability is decidable due to termination: keep applying rewrite rules until you reach a normal form.
- Completion Algorithm (due to Knuth-Bendix):
  - Start with a finite, terminating TRS and check local confluence using critical pairs.
  - If all critical pairs are joinable, done (confluent).
  - Reduce, orient non-joinable critical pairs.
    * If resulting TRS is still terminating, add new rules and recur
- What can go wrong?
  - Rules generated lead to non-termination
  - Algorithm never terminates (keeps generating critical pairs)

3.4 Critical Pairs

3.4.1 Definition

- Let $l_i \to r_i, i \in \{1, 2\}$ be two rules, with disjoint variables
  - For disjointness, we have to rename variables
  - l_1, l_2 can be the same rule, with variables renamed
- Let u be a non-variable subterm of l_1 at position p
  - p is like how we dive into a term using the proof builder
    - $f(f(x, y), y)|_{12} = y$
    - $f(f(x, y), y)[w]_{12} = f(f(x, w), y)$: replacement using positions
  - so $l_1|_p = u$
  - p is a sequence of positive integers, possibly ϵ
- Let θ be a mgu of u, l_2
- Starting with $l_1\theta$, we can:
  - Apply rule 1 to get $r_1\theta$
  - Apply rule 2 to get $l_1\theta[r_2\theta]_p$ (replace position p in $l_1\theta$ with $r_2\theta$)

3.4.2 Critical Pairs Example

- Consider the previous rules R
  - $f(f(x, y), z) \to f(x, f(y, z))$
  - $f(i(x), x) \to e$
- What are the critical pairs?
  - CP1
    - Building blocks
      - $l_1 = f(f(x, y), z)$
      - $p = 1$
      - $u = f(x, y)$
      - $l_2 = f(i(u), u)$
      - $\theta = \{(x, i(u)), (y, u)\}$

- $l_1\theta = f(f(i(u), u), z)$
- $r_1\theta = f(i(u), f(u, z))$
- $r_2\theta = e$
- $l_1\theta[r_2\theta]_p = f(e, z)$

* Critical pair
  - $f(i(u), f(u, z))$
  - $f(e, z)$
* Irreducible!

- CP2
  * Building blocks
    - $l_1 = f(f(x, y), z)$
    - $p = 1$
    - $u = f(x, y)$
    - $l_2 = f(f(a, b), c)$
    - $\theta = \{(x, f(a, b)), (y, c)\}$
    - $l_1\theta = f(f(f(a, b), c), z)$
    - $r_1\theta = f(f(a, b), f(c, z))$
    - $r_2\theta = f(a, f(b, c))$
    - $l_1\theta[r_2\theta]_p = f(f(a, f(b, c)), z)$
  * Critical pair
    - $f(f(a, b), f(c, z))$
    - $f(f(a, f(b, c)), z)$
  * Joinable!
    - $f(f(a, b), f(c, z)) \to f(a, f(b, f(c, z)))$
    - $f(f(a, f(b, c)), z) \to f(a, f(f(b, c), z)) \to f(a, f(b, f(c, z)))$

3.4.3 Completion Example

- Orient, add critical pairs to get R_1:
  - $f(f(x, y), z) \to f(x, f(y, z))$
  - $f(i(x), x) \to e$
  - $f(i(u), f(u, z)) \to f(e, z)$ (New rule)
- Recur!
  - But this gives a fixpoint (exercise)

3.5 More Examples

3.5.1 Group Theory Example

1. Axioms of group theory

   - (G_1) $\forall x, y, z : (x \circ y) \circ z = x \circ (y \circ z)$
   - (G_2) $\forall x : e \circ x = x$
   - (G_3) $\forall x : I(x) \circ x = e$

   Notice that this is an equational theory. If we had existential for inverses, we can use Skolemization to get this version!

2. TRS for group theory

   - $G_1 = (x \circ y) \circ z \to x \circ (y \circ z)$
   - $G_2 = e \circ x \to x$
   - $G_3 = I(x) \circ x \to e$
   - $G = \{G_1, G_2, G_3\}$

3. Group Theory Proofs Theorem: $x \circ I(x) = e$

   Proof:

   $$\begin{array}{ll} & x \circ I(x) \\ \leftarrow \{G_2\} & (e \circ x) \circ I(x) \\ \leftarrow \{G_3\} & ((I(I(x)) \circ I(x)) \circ x) \circ I(x) \\ \to \{G_1\} & (I(I(x)) \circ (I(x) \circ x)) \circ I(x) \\ \to \{G_3\} & (I(I(x)) \circ e) \circ I(x) \\ \to \{G_1\} & I(I(x)) \circ (e \circ I(x)) \\ \to \{G_2\} & I(I(x)) \circ I(x) \\ \to \{G_3\} & e \end{array}$$

4. Exercise

   - Run the completion algorithm.

3.6 Commutativity

- Note: $x \circ y = y \circ x$ is non-terminating, no matter what we do
- Boyer-Moore idea: orient the terms this is being applied to; this is what is done in ACL2s

3.7 Conditional Rewriting

- Advanced topic; hard to prove any theorems