max planck institut
informatik

Universität
des
Saarlandes
FR Informatik

Uwe Waldmann

June 27, 2016

Tutorials for "Automated Reasoning II"
Exercise sheet 7

Exercise 7.1:
A group is a set G with a binary function $\cdot : G \times G \to G$, a unary function $\_^{-1} : G \to G$, and an element $e \in G$ that satisfy the axioms

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$
$$a \cdot e = a$$
$$a \cdot a^{-1} = e$$

for all $a, b, c \in G$. (It is sufficient to assert that e is a right identity and that $\_^{-1}$ is a right inverse. One can prove from these axioms that e is also a left identity and that $\_^{-1}$ is also a left inverse.)

For a group element $a \in G$ and a positive integer n, we define a^n recursively by $a^1 = a$ and $a^{n+1} = a \cdot (a^n)$. We say that $a \in G$ has order n if n is the smallest positive integer such that $a^n = e$. We say that $a \in G$ has order ∞ if there is no positive integer n such that $a^n = e$. (Note that every group has exactly one element with order 1, namely e itself.)

We say that some $a \in G$ commutes with some $b \in G$ if $a \cdot b = b \cdot a$. The center of a group G is the set of all elements $a \in G$ that commute with every $b \in G$.

Formalize the following problem in unsorted first-order logic with equality and use the theorem prover SPASS to prove it: If a group G has exactly one element with order 2, then this element is in the center of G.

Notes:

- You can download SPASS from `http://www.spass-prover.org/`; use either version 3.9, 3.7, or 3.5.
- A sample SPASS input file containing the definition of a group and the conjecture that the right identity element in a group is also a left identity is available from the tutorial web page.
- Even though the presentation above refers to integer numbers, you should formalize the problem without referring to integer numbers.
- It is advisable to formalize the problem without defining auxiliary predicates like `commutes(_)` or `center(_)`. (With auxiliary predicates, the problem becomes noticably harder for SPASS.)

Exercise 7.2:
Compute R_∞ for the clause set $\{f(x) \approx a\}$ and the signature $\Sigma = (\{f/1,\ g/1,\ a/0\}, \emptyset)$; use the LPO with $g > f > a$.

Exercise 7.3:
Prove Lemma 3.14: For every run $N_0 \vdash N_1 \vdash N_2 \vdash \ldots$ of the superposition calculus, $\mathit{Red}(N_i) \subseteq \mathit{Red}(N_\infty)$ and $\mathit{Red}(N_i) \subseteq \mathit{Red}(N_*)$.

Exercise 7.4:
Find an unsatisfiable clause set consisting of two unit clauses $s \approx t$ and $u \not\approx v$ and a term ordering $\succ$ such that the only inference that neither violates the ordering restrictions of the superposition calculus nor yields a tautology is a positive superposition inference in which the left-hand side of $s \approx t$ is unified with the right-hand side of a renamed copy of $s \approx t$.

Bring your solution (or solution attempt) to the tutorial on July 4.