max planck institut
informatik

Universität
des
Saarlandes
FR Informatik

Uwe Waldmann

June 12, 2014

Tutorials for "Automated Reasoning II"
Exercise sheet 8

Exercise 8.1:
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 $a^n = e$ and if n is the smallest positive integer with this property. 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 either download the prover from `http://www.spass-prover.org/` or use the interactive web interface on that site. (Do not use the file upload form on that site; it is currently broken.)
- 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.
- In SPASS input files, the connectives $\vee$ and $\neg$ are written `or(_,_)` and `not(_)`.

- 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 8.2:
Prove the lifting lemma (Lemma 3.7) for Equality Factoring inferences.

Exercise 8.3:
Suppose that we redefine the literal ordering for ground equational literals in such a way that a positive literal $s \approx t$ is mapped to $(\{s, t\}, 0)$, a negative literal $s \not\approx t$ is mapped to $(\{s, t\}, 1)$, and the literal ordering $\succ_L$ compares these pairs using the lexicographic combination of the multiset extension of $\succ$ and the ordering $>$ on natural numbers. What would go wrong in the refutational completeness proof for superposition?

Exercise 8.4:
Compute the rewrite systems R_C and R_∞ for the set of clauses

$$
\begin{array}{cr}
f(a) \approx d \vee f(a) \approx c & (1) \\
a \not\approx d \vee f(b) \approx f(d) & (2) \\
f(c) \approx f(d) & (3) \\
f(d) \approx d \vee f(d) \approx b & (4) \\
a \approx b & (5) \\
c \approx d & (6)
\end{array}
$$

Use the KBO with $f > a > b > c > d$ and weight 1 for all symbols as term ordering. Which is the smallest clause C such that C is neither productive nor true in R_C?

Exercise 8.5:
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 $g > f > a$.

Bring your solution (or solution attempt) to the tutorial on June 30.