max planck institut
informatik

Universität
des
Saarlandes
FR Informatik

Uwe Waldmann July 9, 2024

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 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 E 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 the latest version of E from `https://www.eprover.org/`.
- A sample E 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. Use `eprover --auto --proof-object group.p | less` to run E on it.
- 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 first-order theorem provers.)

Exercise 8.2:

Compute minimal complete sets of unifiers for the following equality problems. (There is no need to construct and solve diophantine equation systems; the solutions are relatively obvious.)

(1) $\{ x + y \approx a + b \}$ w. r. t. ACU.

(2) $\{ x + y \approx a + b \}$ w. r. t. AC.

(3) $\{ x + y \approx x \}$ w. r. t. ACU.

(4) $\{ x + y \approx x \}$ w. r. t. AC.

(5) $\{ x + y + a \approx z + b \}$ w. r. t. ACU.

(6) $\{ x + y + a \approx z + z \}$ w. r. t. ACU.

(7) $\{ a + x + x \approx y + b \}$ w. r. t. A.

Bring your solution (or solution attempt) to the tutorial on July 16.