Technische Universität München
Institut für Informatik
Prof. Tobias Nipkow, Ph.D.
Alexander Krauss, Sascha Böhme

WS 2008/09
30. 01. 2009

Logic

Exercise Sheet 12

Exercise 12.1 Quantifier Elimination for Presburger Arithmetic

a) $\forall y.\ 3 < x + 2y \vee 2x + y < 3$

b) $\forall x.\ (\exists y.\ x = 2y) \Rightarrow 2x \geq 0 \vee 3x < 2$

Solution

a)

$$\begin{aligned}
&\forall y.\ 3 < x + 2y \vee 2x + y < 3 \\
\equiv\ &\neg(\exists y.\ 3 \geq x + 2y \wedge 2x + y \geq 3) \\
\equiv\ &\neg(\exists y.\ 3 - 2x \leq y \wedge 2y \leq 3 - x) \\
\equiv\ &\neg(\exists y.\ 6 - 4x \leq 2y \wedge 2y \leq 3 - x) \\
\equiv\ &\neg(\exists z.\ 6 - 4x \leq z \wedge z \leq 3 - x \wedge 2 \mid z) \\
\equiv\ &\neg(6 - 4x \leq 3 - x \wedge 2 \mid (6 - 4x) \vee 6 - 4x + 1 \leq 3 - x \wedge 2 \mid (6 - 4x + 1))
\end{aligned}$$

b)

$$\begin{aligned}
&\forall x.\ (\exists y.\ x = 2y) \Rightarrow 2x \geq 0 \vee 3x < 2 \\
\equiv\ &\forall x.\ (\exists y.\ x \leq 2y \wedge x \geq 2y) \Rightarrow 2x \geq 0 \vee 3x < 2 \\
\equiv\ &\forall x.\ (\exists z.\ x \leq z \wedge x \geq z \wedge 2 \mid z) \Rightarrow 2x \geq 0 \vee 3x < 2 \\
\equiv\ &\forall x.\ 2 \mid x \Rightarrow 2x \geq 0 \vee 3x < 2 \\
\equiv\ &\neg(\exists x.\ 2 \mid x \wedge 2x \leq 0 \wedge 3x \geq 2) \\
\equiv\ &\neg(\exists x.\ 2 \mid x \wedge 6x \leq 0 \wedge 6x \geq 4) \\
\equiv\ &\neg(\exists z.\ 2 \mid z \wedge z \leq 0 \wedge z \geq 4 \wedge 6 \mid z) \\
\equiv\ &\neg(2 \mid 4 \wedge 4 \leq 0 \wedge 6 \mid 4)
\end{aligned}$$

Exercise 12.2 Quantifier Elimination for Linear Real Arithmetic

a) $\exists xy.\ 2x + 3y = 7 \wedge x < y \wedge 0 < x$

b) $\exists xy.\ 3x + 3y < 8 \wedge 8 < 3x + 2y$

Solution

a)

$$\begin{aligned}
&\exists xy.\ 2x + 3y = 7 \wedge x < y \wedge 0 < x \\
\equiv\ &\exists x.\ \exists y.\ y = \frac{7}{3} - \frac{2}{3}x \wedge x < y \wedge 0 < x \\
\equiv\ &\exists x.\ x < \frac{7}{3} - \frac{2}{3}x \wedge 0 < x \\
\equiv\ &\exists x.\ 0 < x \wedge \frac{5}{3}x < \frac{7}{3} \\
\equiv\ &0 < \frac{7}{3}
\end{aligned}$$

b)

$$\begin{aligned}
&\exists xy.\ 3x + 3y < 8 \wedge 8 < 3x + 2y \\
\equiv\ &\exists x.\ \exists y.\ y < \frac{8}{3} - x \wedge 4 - \frac{3}{2}x < y \\
\equiv\ &\exists x.\ 4 - \frac{3}{2}x < \frac{8}{3} - x \\
\equiv\ &\exists x.\ \frac{8}{3} < x \\
\equiv\ &\top
\end{aligned}$$

Exercise 12.3 Definable Sets

A set $D \subseteq \mathbb{Z}$ is said to be *eventually periodic* iff there are positive numbers n and k such that for all $x \geq n$, we have $x \in D \Leftrightarrow x + k \in D$.

We say that a set $D \subseteq \mathbb{Z}$ is *definable in Presburger arithmetic*, if $D = \{x \mid p\}$ where p is a formula in Presburger arithmetic whose only free variable is x.

a) Show that a set of integers is definable in the language of Presburger arithmetic if and only if it is eventually periodic.

b) Show that there is no formula $p(x, y, z)$ in Presburger arithmetic such that for all $m, n, k \in \mathbb{Z}$,

$$mn = k \quad \text{iff} \quad \mathbb{Z} \vDash p(m, n, k)$$

Hint: Consider the set $\{x^2 \mid x \in \mathbb{Z}\}$.

Solution

a) We first show that a set definable in Presburger arithmetic is eventually periodic (e.p.). Consider a Presburger formula p. We can eliminate all quantifiers in p to make it quantifier-free. We also put it in NNF, which means that p then consists of primitive formulas of

the forms $x < c$, $x \leq c$, $x = c$, $c \leq x$, and $c < x$, where c is a constant. These primitive formulas are combined using conjunctions and disjunctions.

By induction on the structure of the formula, we show that the corresponding set is e.p.:

- For $p = x < c$, the set is e.p. with $n = c$ and $k = 1$.
- For $p = (x = c)$, the set is e.p. with $n = c + 1$ and $k = 1$.
- For $p = x \geq c$, the set is e.p. with $n = c$ and $k = 1$.
- the other base cases are similar.
- For $p = p_1 \wedge p_2$ we know by induction hypothesis that D_{p_1} and D_{p_2} are e.p., hence there exist n_1, k_1, n_2, k_2 satisfying the condition above. Now, $D_p = D_{p_1} \cap D_{p_2}$ is e.p. as well, with $n = \max(n_1, n_2)$ and $k = k_1 k_2$ (or alternatively, $k = \mathrm{lcm}(k_1, k_2)$).
- the case for disjunction is similar.

For the other direction, our claim is slightly flawed, since the definition of "eventually periodic" places no restriction on the behaviour of D for very small values. We must either change the definition of "eventually periodic" to require that $|x| > n$ implies $x \in D \Leftrightarrow x + k \in D$ (note the $|\cdot|$), or we simply restrict our claim to $\mathbb{N}$ instead of $\mathbb{Z}$, which we do in the following:

So let $D \subseteq \mathbb{N}$ be a set that is e.p., and n and k are the corresponding constants. We show that D can be defined in Presburger arithmetic. D consists of a finite prefix $\{a_1, \ldots, a_m\} \subseteq \{0, \ldots, n-1\}$ and a finite set $\{b_1, \ldots, b_\ell\} \subseteq \{n, \ldots, n+k-1\}$, which contains the pattern that is repeated periodically. We define

$$D = \{x \mid x = a_1 \vee \cdots \vee x = a_m \vee (\exists y.\ k|y \wedge (x = b_1 + y \vee \cdots \vee x = b_\ell + y))\}$$

b) If there were such a formula, then we could use it to define the set of squares as $S := \{x \mid \exists y.\, p(y, y, x)\}$. However, S is not e.p.: Assume for contradiction that it is, with the constants n,k. Then take $m := \max(n, k)$. Then $m^2 \in S$, which implies that $m^2 + k \in S$, too. However, the next square is $(m+1)^2 = m^2 + 2m + 1 > m^2 + k$, which implies that $m^2 + k \notin S$.

Exercise 12.4 Characterizing the real numbers

a) Find a complete axiomatization of the theory of the real numbers with addition, i.e., a set of axioms Σ, such that $\mathrm{Cn}(\Sigma) = \mathrm{Th}(\mathbb{R}, <, +, -, 0)$.

b) Give a sketch of the proof that your axiomatization is complete.

Solution

The idea of this exercise was to see that the quantifier elimination procedure for real linear arithmetic gives us a complete theory: Since we can reduce any sentence to $\top$ or $\bot$ by eliminating quantifiers, the theory contains either p or $\neg p$ for any sentence.

Finding a complete set of axioms now merely involves collecting all the properties that are used in the quantifier elimination.

However, the problem is that the quantifier elimination procedure uses multiplication and division by constants to express the intermediate steps, and the rules that are used here cannot be expressed with $<, +, -, 0$ alone. Hence we must extend the language at least with multiplication and division by constants to express all the axioms that are used.