Technical University of Munich
Chair for Logic and Verification

Prof. Tobias Nipkow
Kevin Kappelmann

SS 2022 — Exercise Sheet 13 — 22.07.2022

No tutorial on 29.07. Final Q&A and exam preparation tutorial will take place on 01.08, 02.08, or 03.08. Exact place and time will be decided and announced on Zulip.

Exercise 13.1. **[Ferrante–Rackoff Elimination]**
Apply the Ferrante–Rackoff Elimination to check the validity of the following sentence:

$$\exists x(\exists y(x = 2 \cdot y) \rightarrow (2 \cdot x \geq 0 \vee 3 \cdot x < 2))$$

Solution:

$$
\begin{aligned}
& \exists x(\exists y(x = 2 \cdot y) \rightarrow (2 \cdot x \geq 0 \vee 3 \cdot x < 2)) \\
\Longleftrightarrow_{R_+} \quad & \exists x(\exists y(y = \frac{1}{2}x) \rightarrow (2 \cdot x \geq 0 \vee 3 \cdot x < 2)) \\
\Longleftrightarrow_{R_+} \quad & \exists x \left(\bot \vee \bot \vee \frac{1}{2}x = \frac{1}{2}x \vee \bot \rightarrow (2 \cdot x \geq 0 \vee 3 \cdot x < 2)\right) \\
\Longleftrightarrow \quad & \exists x \left(\left(\top \wedge \top \wedge \neg\left(\frac{1}{2}x = \frac{1}{2}x\right) \wedge \top\right) \vee (2 \cdot x \geq 0 \vee 3 \cdot x < 2)\right) \\
\Longleftrightarrow_{R_+} \quad & \exists x \left(\left(\top \wedge \top \wedge \left(\frac{1}{2}x < \frac{1}{2}x\right) \wedge \top\right) \vee (2 \cdot x \geq 0 \vee 3 \cdot x < 2)\right) \\
\Longleftrightarrow_{R_+} \quad & \exists x \left((\top \wedge \top \wedge \bot \wedge \top) \vee \left(0 < x \vee x = 0 \vee x < \frac{2}{3}\right)\right) \\
\Longleftrightarrow_{R_+} \quad & \bigvee_{t \in \{-\infty, \infty, 0, 1/3\}} \left((\top \wedge \top \wedge \bot \wedge \top) \vee \left(0 < x \vee x = 0 \vee x < \frac{2}{3}\right)\right)[t/x] \\
\Longleftrightarrow \quad & (\cdots \vee (\bot \vee \bot \vee \top)) \vee (\cdots \vee (\top \vee \bot \vee \bot)) \vee \left(\cdots \vee \left(0 < 0 \vee 0 = 0 \vee 0 < \frac{2}{3}\right)\right) \\
& \vee \left(\cdots \vee \left(0 < \frac{1}{3} \vee \frac{1}{3} = 0 \vee \frac{1}{3} < \frac{2}{3}\right)\right) \\
\Longleftrightarrow \quad & \top \qquad \text{(optional step; not part of QEP)}
\end{aligned}
$$

Exercise 13.2. [Presburger Arithmetic]
Eliminate the quantifiers from the following formulas according to Presburger arithmetic:

1. $\forall y(3 < x + 2y \vee 2x + y < 3)$
2. $\forall x(2 \mid x \rightarrow (2x \geq 0 \vee 3x < 2))$

Solution:

$$
\begin{aligned}
& \forall y(3 < x + 2y \vee 2x + y < 3) \\
\iff\; & \neg\exists y \neg(3 < x + 2y \vee 2x + y < 3) \\
\iff_{\mathcal{P}}\; & \neg\exists y(3 \geq x + 2y \wedge 2x + y \geq 3) \\
\iff_{\mathcal{P}}\; & \neg\exists y(0 \leq 3 - x - 2y \wedge 0 \leq 2x + y - 3) \\
\iff_{\mathcal{P}}\; & \neg\exists y(0 \leq 3 - x - 2y \wedge 0 \leq 4x + 2y - 6) \\
\iff_{\mathcal{P}}\; & \neg\exists z(0 \leq 3 - x - z \wedge 0 \leq 4x + z - 6 \wedge 2 \mid z) \\
\iff_{\mathcal{P}}\; & \neg\Big((0 \leq 3 - x - (6 - 4x) \wedge 0 \leq 4x + (6 - 4x) - 6 \wedge 2 \mid 6 - 4x) \\
& \quad \vee (0 \leq 3 - x - (6 - 4x + 1) \wedge 0 \leq 4x + (6 - 4x + 1) - 6 \wedge 2 \mid 6 - 4x + 1)\Big)
\end{aligned}
$$

$$
\begin{aligned}
& \forall x(2 \mid x \rightarrow (2x \geq 0 \vee 3x < 2)) \\
\iff\; & \neg\exists x \neg(2 \mid x \rightarrow (2x \geq 0 \vee 3x < 2)) \\
\iff\; & \neg\exists x(2 \mid x \wedge \neg(2x \geq 0 \vee 3x < 2)) \\
\iff_{\mathcal{P}}\; & \neg\exists x(2 \mid x \wedge 2x < 0 \wedge 3x \geq 2) \\
\iff_{\mathcal{P}}\; & \neg\exists x(2 \mid x \wedge 2x \leq -1 \wedge 2 \leq 3x) \\
\iff_{\mathcal{P}}\; & \neg\exists x(2 \mid x \wedge 0 \leq -1 - 2x \wedge 0 \leq 3x - 2) \\
\iff_{\mathcal{P}}\; & \neg\exists x(12 \mid 6x \wedge 0 \leq -3 - 6x \wedge 0 \leq 6x - 4) \\
\iff_{\mathcal{P}}\; & \neg\exists z(12 \mid z \wedge 0 \leq -3 - z \wedge 0 \leq z - 4 \wedge 6 \mid z) \\
\iff_{\mathcal{P}}\; & \neg \bigvee_{4 \leq t \leq 15} (12 \mid t \wedge 0 \leq -3 - t \wedge 0 \leq t - 4 \wedge 6 \mid t) \\
\iff_{\mathcal{P}}\; & \neg \bigvee_{4 \leq t \leq 15} (12 \mid t \wedge \bot \wedge \cdots) \quad \iff_{\mathcal{P}} \quad \top \qquad \text{(optional steps; not part of QEP)}
\end{aligned}
$$

Exercise 13.3. [Quantifier Elimination for $Th(\mathbb{N}, 0, S, =)$]
Give a quantifier-elimination procedure for $Th(\mathbb{N}, 0, S, =)$ where S is the successor operation on natural numbers, i.e. $S(n) = n + 1$.

Hint: $a = b$ iff $S^k(a) = S^k(b)$ for any $a, b, k \in \mathbb{N}$.

Solution:
We assume $F = \exists x(A_1 \wedge \ldots \wedge A_n)$ where x occurs in all A_i and each A_i is of the form

$$S^k(x) = S^m(t) \text{ or } S^k(x) \neq S^m(t)$$

where t is 0 or a variable (using symmetry of $=$).

If x occurs on both sides of an atom A_i, we can compare the number of successors and replace it with $\bot$ or $\top$, i.e. $Th(\mathbb{N}, 0, S) \models (S^k(x) = S^l(x)) \iff k = l$. Hence, we can assume that $x \neq t$.

We have to distinguish two cases:

1. All A_i only use $\neq$, but not $=$: We can return $\top$ because x can always be chosen to be different from finitely many natural numbers.
2. There is at least one A_i of the form $S^m(x) = t$ where $x \neq t$.

   We replace A_i as follows:
   - If $m > 0$, we add the constraints $t \neq 0 \wedge \ldots \wedge t \neq S^{m-1}(0)$ to ensure that the solution for x is non-negative.
   - Otherwise, replace it with $\top$.

   The other A_j $(i \neq j)$ can be replaced as follows: Let A_j be $S^k(x) = u$. Using the hint, first increment both sides by m: $S^{k+m}(x) = S^m(u)$. Then, substitute A_i, resulting in $S^k(t) = S^m(u)$.

   This works similarly for inequality, resulting in $S^k(t) \neq S^m(u)$.

For optimization purposes, we could also assume that either side of the equalities/inequalities contains no successor application. If they do, we can decrement until at least one side is 0 or a variable.

Homework 13.1. [Under Presburger] (++)

Perform Presburger arithmetic quantifier elimination for the following formula:

$$\forall x(\exists y(x = 2y \land 2 \mid y) \to 4 \mid x)$$

You may additionally simplify ground atoms during the process.

Solution:

$$\begin{aligned}
& \forall x(\exists y(x = 2y \land 2 \mid y) \to 4 \mid x) \\
\Longleftrightarrow_{\mathcal{P}} \quad & \forall x(\exists y(0 \le 2y - x \land 0 \le -2y + x \land 4 \mid 2y) \to 4 \mid x) \\
\Longleftrightarrow_{\mathcal{P}} \quad & \forall x(\exists z(0 \le z - x \land 0 \le -z + x \land 4 \mid z \land 2 \mid z) \to 4 \mid x) \\
\Longleftrightarrow_{\mathcal{P}} \quad & \forall x\Big(((0 \le x - x \land 0 \le -x + x \land 4 \mid x \land 2 \mid x) \\
& \quad \lor (0 \le x + 1 - x \land 0 \le -(x+1) + x \land 4 \mid x + 1 \land 2 \mid x + 1) \\
& \quad \lor (0 \le x + 2 - x \land 0 \le -(x+2) + x \land 4 \mid x + 2 \land 2 \mid x + 2) \\
& \quad \lor (0 \le x + 3 - x \land 0 \le -(x+3) + x \land 4 \mid x + 3 \land 2 \mid x + 3)\big) \to 4 \mid x\Big) \\
\Longleftrightarrow_{\mathcal{P}} \quad & \forall x\Big(((\top \land \top \land 4 \mid x \land 2 \mid x) \\
& \quad \lor (\top \land \bot \land 4 \mid x + 1 \land 2 \mid x + 1) \\
& \quad \lor (\top \land \bot \land 4 \mid x + 2 \land 2 \mid x + 2) \\
& \quad \lor (\top \land \bot \land 4 \mid x + 3 \land 2 \mid x + 3)\big) \to 4 \mid x\Big) \\
\Longleftrightarrow \quad & \forall x\Big(\big((4 \mid x \land 2 \mid x) \lor \bot \lor \bot \lor \bot\big) \to 4 \mid x\Big) \\
\Longleftrightarrow \quad & \forall x\Big((4 \mid x \land 2 \mid x) \to 4 \mid x\Big) \\
\Longleftrightarrow \quad & \neg\exists x\Big(4 \mid x \land 2 \mid x \land \neg(4 \mid x)\Big) \\
\Longleftrightarrow_{\mathcal{P}} \quad & \neg \bigvee_{i=1}^{3} \exists x(4 \mid x \land 2 \mid x \land 4 \mid x + i) \\
\Longleftrightarrow_{\mathcal{P}} \quad & \neg \bigvee_{i=1}^{3} \bigvee_{j=0}^{3} (4 \mid j \land 2 \mid j \land 4 \mid j + i) \\
\Longleftrightarrow_{\mathcal{P}} \quad & \neg \bigvee_{i=1}^{3} \bigvee_{j=0}^{3} (\bot \land \cdots) \quad \Longleftrightarrow \quad \top \qquad \text{(optional step; not part of QEP)}
\end{aligned}$$

Homework 13.2. **[Quantifier Elimination for $Th(\mathbb{Z}, 0, S, P, =, <)$]** (+++)
Give a quantifier-elimination procedure for $Th(\mathbb{Z}, 0, S, P, =, <)$ where S is the successor and P the predecessor operation on integers, i.e. $S(n) = n + 1$ and $P(n) = n - 1$. Do not use Presburger arithmetic; give a direct algorithm.

Solution:
At any point, we normalise any term t such that it might contain S or P but not both:

1. If $t = S^k(P^m(u))$, replace t by $P^{m-k}(u)$ if $k \leq m$ and $S^{k-m}(u)$ otherwise.
2. Case $t = P^k(S^m(u))$: analogous.

Moreover, we apply the following transformations:

1. Replace $\neg(t < u)$ by $t = u \lor u < t$.
2. Replace $t = u$ by $t < S(u) \land u < S(t)$.
3. Replace $t \neq u$ by $t < u \lor u < t$.

We can then assume that we have some $F = \exists x(A_1 \land \ldots \land A_n)$ where x occurs in all A_i and each A_i is of the form

$$f^k(x) < g^m(t) \text{ or } f^k(t) < g^m(x)$$

where t is 0 or a variable and $f, g \in \{S, P\}$. First consider the case $t = x$:

1. Replace $S^k(x) < S^m(x)$ by $\top$ if $k < m$ and $\bot$ otherwise.
2. Replace $P^k(x) < P^m(x)$ by $\top$ if $k > m$ and $\bot$ otherwise.
3. Replace $P^k(x) < S^m(x)$ by $\top$.
4. Replace $S^k(x) < P^m(x)$ by $\bot$.

Let F_x be the conjunction of all these atoms. We then bring all remaining A_i into canonical form for x:

1. Replace $S^k(x) < g^m(t)$ by $x < P^k(g^m(t))$
2. Replace $P^k(x) < g^m(t)$ by $x < S^k(g^m(t))$
3. Replace $f^k(t) < S^m(x)$ by $P^m(f^k(t)) < x$
4. Replace $f^k(t) < P^m(x)$ by $S^m(f^k(t)) < x$

Let U be the set of these atoms. We then replace F by

$$F_x \land \bigwedge_{(l<x)\in U} \bigwedge_{(x<u)\in U} S(l) < u.$$

> It is always easy to be logical.
> It is almost impossible to be logical to the bitter end.
>
> — Albert Camus