Exercises 5

Exercise 1 (Quantifier Elimination in PA)**.** Apply quantifier elimination as seen in the Lectures to the following formulas:

- $\exists x, y.\, 2x + 3y < 7 \land x < y$
- $\exists x, y.\, 2x + 3y < 7 \land y < x$
- $\exists x, y.\, 3x + 3y < 8 \land 8 < 3x + 2y$
- $\exists x, y.\, x = 2y \land \exists z.x = 3z$

Solution: *In PA we have that:*

$$\begin{aligned}
&\exists y.\, 2x + 3y < 7 \land x < y \\
\equiv&\exists y.\, 3x < 3y \land 3y < 7 - 2x \\
\equiv&\exists y'.\, 3x < y' \land y' < 7 - 2x \land 3 \mid y' \\
\equiv&\bigvee_{i=1}^{3} 3x + i < 7 - 2x \land 3 \mid 3x + i
\end{aligned}$$

We can then proceed with the second quantifier:

$$\begin{aligned}
&\exists x.\, \bigvee_{i=1}^{3} 3x + i < 7 - 2x \land 3 \mid 3x + i \\
\equiv&\bigvee_{i=1}^{3} \exists x.\, 3x + i < 7 - 2x \land 3 \mid 3x + i \\
\equiv&\bigvee_{i=1}^{3} \exists x.\, 5x < 7 - i \land 3 \mid 3x + i \\
\equiv&\bigvee_{i=1}^{3} \exists x.\, 15x < 21 - 3i \land 15 \mid 15x + 5i \\
\equiv&\bigvee_{i=1}^{3} \exists x'.\, x' < 21 - 3i \land 15 \mid x' + 5i \land 15 \mid x' \\
\equiv&\bigvee_{i=1}^{3} \bigvee_{j=1}^{15} 15 \mid j + 5i \land 15 \mid j
\end{aligned}$$

Similarly we have for the second sentence:

$$\begin{aligned}
&\exists y.\, 2x+3y<7\wedge y<x\\
\equiv&\exists y.\, 3y<7-2x\wedge 3y<3x\\
\equiv&\exists y'.\, y'<7-2x\wedge y'<3x\wedge 3\mid y'\\
\equiv&\bigvee_{i=1}^{3} 3\mid i\equiv \mathit{True}
\end{aligned}$$

We then have:

$$\exists x.\, \bigvee_{i=1}^{3} 3\mid i\equiv \bigvee_{i=1}^{3}\exists x.\, 3\mid i\equiv \bigvee_{i=1}^{3} 3\mid i\equiv \mathit{True}$$

For the third sentence:

$$\begin{aligned}
&\exists y.\, 3x+3y<8\wedge 8<3x+2y\\
\equiv&\exists y.\, 8-3x<2y\wedge 3y<8-3x\\
\equiv&\exists y.\, 24-9x<6y\wedge 6y<16-6x\\
\equiv&\exists y'.\, 24-9x<y'\wedge y'<16-6x\wedge 6\mid y'\\
\equiv&\bigvee_{i=1}^{6} 24-9x+i<16-6x\wedge 6\mid 24-9x+i
\end{aligned}$$

We then have:

$$\begin{aligned}
&\exists x.\, \bigvee_{i=1}^{6} 24-9x+i<16-6x\wedge 6\mid 24-9x+i\\
\equiv&\exists x.\, \bigvee_{i=1}^{6} 8+i<3x\wedge 6\mid 24-9x+i\\
\equiv&\exists x.\, \bigvee_{i=1}^{6} 24+3i<9x\wedge 6\mid 24-9x+i\\
\equiv&\exists x'.\, \bigvee_{i=1}^{6} 24+3i<x'\wedge 6\mid 24-x'+i\wedge 9\mid x'\\
\equiv&\bigvee_{i=1}^{6}\bigvee_{j=1}^{18} 6\mid 24-j+i\wedge 9\mid j\equiv \mathit{True}
\end{aligned}$$

Finally:

$$\begin{aligned}
&\exists x,y.\, x=2y\wedge \exists z.x=3z\\
\equiv&\exists x, 2\mid x\wedge 3\mid x\\
\equiv&\bigvee_{i=1}^{6} 2\mid i\wedge 3\mid i\equiv \mathit{True}
\end{aligned}$$

$\diamondsuit$

Exercise 2 (Satisfiability algorithm for Presburger arithmetic)**.** Consider the formula $F(x)$ given by

$$F(x) = \bigwedge_{i=1} a_i < x \wedge \bigwedge_{j=1} x < b_j \wedge \bigwedge_{i=1} K_i | (x + t_i).$$

Recall that the terms a_i, b_j, t_i may in general contain other variables than x.

1. Assume all a_i, b_j, t_i are integer constants. Give an algorithm that, given any formula of the form above, returns:
   - a value for x, if such value exists, and
   - "UNSAT" if no such value exists

   Solution: *Since*

   $$F(x) \equiv \bigvee_{i=1}^{\mathrm{lcm}(\{K_i\}_i)} F(\max_i a_i + i)$$

   The algorithm checks for all i in that range whether $F(\max_i a_i + i)$ holds, and output one of them if it exists. Otherwise it returns UNSAT. $\diamondsuit$

2. Give a recursive algorithm that, given a formula in the above form returns
   - one map from variables to integers for which formula evaluates to true, if such a map exists, and
   - "UNSAT" if no such map exists.

   Solution: *Applying the quantifier elimination procedure gives us a formula of the form*

   $$\bigvee_{i_1=1}^{N_1} \cdots \bigvee_{i_k=1}^{N_k} \varphi$$

   During the procedure, we record for each quantifier $\exists x_j$ the associated term $t_j = \max_i a_i$. The latter allows us to compute the range for each variable. We then try all possible assignments using backtracking on $F(\overline{x})$ to find a suitable one. $\diamondsuit$

Exercise 3 (Quantifier elimination for rationals)**.** In this exercise we will devise a quantifier elimination method for rational numbers. We consider formulas over the signature $(\mathbb{Q}, <, \leq, =, +, -)$, i.e. with constant symbols among $\mathbb{Q}$, interpreted over the standard structure of rational numbers.

1. Show that for any formula F, there exists a formula F_1 such that

$$F \iff Q_1 x_1, \ldots, Q_n x_n, Q_{n+1} y. F_1$$

Where Q_i are either $\exists$ or $\neg\exists$, i.e. existential quantifiers that can be separated by negations and where F_1 is built only from $(\wedge, \vee, \mathbb{Q}, <, =, +, -, k \cdot \_)$. In particular it is quantifier-free and contains no negation!

Solution: *We can find such a formula by applying the following steps.*

   (a) *Pushing all the quantifiers to the beginning of the formula.*

   (b) *Changing $\forall x_i.\, \varphi$ in $\neg\exists x_i.\, \neg\varphi$.*

   (c) *Pushing negations to atomic subformulas, applying De Morgan laws and converting $\neg\, a < b$ into $b \leq a$, $\neg\, a \leq b$ into $b < a$ and $\neg\, a = b$ into $b < a \vee a < b$.*

   (d) *Substituting all occurences of $a \leq b$ by $a < b \vee a = b$.*

$\diamondsuit$

2. Do we need to add the divisibility relation as in the PA case? Why?

Solution: *No, because in this case, variables are rationals and not integers anymore, so they can be divided by an arbitrary integer.* $\diamondsuit$

3. Show that there exist a formula F_2 such that $F_1 \iff F_2$ and every atom of F_2 is of the form:

$$t < y$$

or

$$y < t$$

or

$$t = y$$

for some term t

Solution: *In each atom, we can move around all the varibles expect y in order to end up with atoms of the form $k \cdot y < t$, $t < k \cdot y$ or $t = k \cdot y$. By multiplying both sides by $1/k$ we obtain the desired result.* $\diamondsuit$

4. Show that there exists a formula F_3 that is quantifier-free such that

$$(\exists y. F_2) \iff F_3$$

Solution: *There are several ways to tackle this problem. We present* *here the most similar to Presburger Arithmetic quantifier elimination. We start by converting F_2 in DNF and distribute the existential quantifier over the disjunction afterwards. We therefore end up with subformulas of the form:*

$$\exists y.\ \bigwedge_{i\in I} t_i < y \wedge \bigwedge_{j\in J} y < t_j \wedge \bigwedge_{k\in K} t_k = y$$

If $K \neq \emptyset$, we can just replace every occurence of y by one of the t_k. Otherwise we eliminate the quantifier by reducing each conjuction to:

$$\bigwedge_{i\in I} \bigwedge_{j\in J} t_i < t_j$$

$\Diamond$

Exercise 4 (PA without divisibility)**.** Show that Presburger Arithmetic without the divisibility relationship does not admit quantifier elimination with the following steps:

1. Find a quantified formula of one free variable $F(y)$ such that $F(y)$ is true for infinitely many positive integers and false for infinitely many positive integers. I.e., $S_F = \{n \in \mathbb{N} | F(n)\}$ is infinite and $\mathbb{N} \setminus S_F$ is infinite.

   Solution: *$\exists x.\, 2x = y$ is such formula as it is true for all even numbers and false for odd ones.* $\Diamond$

2. Show that for any quantifier-free formula of one free variable $G(y)$, either S_G is finite or $\mathbb{N} \setminus S_G$ is finite.

   Solution: *Since:*

   - *$x = y$ can be written as $y - 1 < x < y + 1$;*
   - *we can push negations down to atomic formula;*
   - *we can distribute ANDs over ORs;*

   any quantifie-free formula is equivalent to

   $$\bigwedge_i ai < n_i \cdot y \wedge \bigwedge_j n'_j \cdot y < b_j$$

   which is itself equivalent

   $$\bigwedge_i ai \cdot \left(\frac{N}{n_i}\right) < N \cdot y \wedge \bigwedge_j N \cdot y < b_j \cdot \left(\frac{N}{n'_j}\right)$$

   where $N = \operatorname{lcm}(\{a_i\}_i, \{b_j\}_j)$.

When $\{a_i\}_i$ is not empty we can merge all the bounds to a single one ending up with:

$$\max_i \left(ai \cdot \left(\frac{N}{n_i} \right) \right) < N \cdot y$$

Similarly if $\{b_j\}_j$ is not empty we have:

$$N \cdot y < \min_j \left(b_j \cdot \left(\frac{N}{n'_j} \right) \right)$$

We end up with 3 possibilities:

- *either $\{b_i\}_i = \emptyset$, in which case* $S_G = \left\{ y \in \mathbb{N} \;\middle|\; y > \left\lceil \frac{\max_i \left(a_i \cdot \left(\frac{N}{n_i} \right) \right)}{N} \right\rceil \right\}$, *which is a cofinite set;*
- *either $\{a_i\}_i = \emptyset$, in which case* $S_G = \left\{ y \in \mathbb{N} \;\middle|\; y < \left\lfloor \frac{\max_j \left(b_j \cdot \left(\frac{N}{n'_i} \right) \right)}{N} \right\rfloor \right\}$, *which is a finite set;*
- *either both are non empty in which case S_G is the intersection of the two sets above and is therefore finite as well.*

$\Diamond$

3. Conclude.

   Solution: *This shows that we cannot find for any formula F, an equivalent quantifier-free formula G that is equivalent to it. Indeed, our quantifier elimination procedure produces formulas with subformulas of the form $k \mid f(\overline{x})$ which admit an existential quantifier under the hood.* $\Diamond$

Exercise 5 (Structure of sets)**.** Consider the structure $(\mathcal{P}(\mathbb{N}), \subseteq, = \cap, \cup, \_^c)$ whose base set is the set of all sets of natural numbers and where $\_^c$ denotes complement. Is it possible to eliminate quantifiers from arbitrary first order formulas on this structure? For example, $\exists B. A \subseteq B \wedge B \subseteq C$ is equivalent to $A \subseteq C$. Show a quantifier elimination procedure, or give an example of a quantified first-order logic formula that has no equivalent formula without quantifiers, and prove it.

Solution:

Quantifier elimination is not possible as there exist formulas that have no quantifier-free equivalent. For example we can express $\exists Y. X \cap Y^c \neq \emptyset \wedge$

$X \cap Y \neq \emptyset$, which is satisfied for all X containing at least two elements. However, without quantifiers we can only express $X = \emptyset$, $X = \mathbb{N}$ or boolean combinations of both.

$\Diamond$

Exercise 6 (A rational arithmetic formula)**.** Consider the following formula $G(x, z)$ where the variables range over rational numbers $\mathbb{Q}$:

$$\forall y.((x < y \land y < z) \longrightarrow \forall u.(x \neq u + u + u))$$

Find a quantifier-free formula equivalent to $G(x, z)$.

Solution:

$$\begin{aligned}
&\forall y.((x < y \land y < z) \longrightarrow \forall u.(x \neq u + u + u)) \\
\equiv&\neg\exists y.(x < y \land y < z \land \exists u.(x = u + u + u)) \\
\equiv&\neg\exists y.(x < y \land y < z) \\
\equiv&\neg(x < z)
\end{aligned}$$

$\Diamond$