Presburger arithmetic and its extensions (Homework)

Instructions.

Prepare a single PDF file with your solutions, with pages of size A4 (portrait) with blank margins at least 2 cm wide all around. At the top of the first page please put your name and the total number of pages in your submission and make it clear whether you are a Master's student, a PhD student, or neither.

Email the file to `d.chistikov@warwick.ac.uk` by **Saturday 27 June 2026, 12:00 UTC (14:00 CEST).** Please ensure that I confirm I have received your solutions.

Problems.

By $\mathbb{N}$ we denote the set of nonnegative integers: $\mathbb{N} = \{0, 1, 2, \ldots\}$.

1. Describe an algorithm which, given as input 9 integers $a_1, a_2, a_3, b_1, b_2, b_3, c_1, c_2, c_3$, determines in polynomial time if the system of three inequalities $a_i x + b_i y \leq c_i$, $i \in \{1, 2, 3\}$, has a solution (x, y) where x and y are integers.

2. Prove that there is no formula $\varphi(x)$ in Presburger arithmetic that defines the set $\{2^n \mid n \in \mathbb{N}\} \cup \{3^n \mid n \in \mathbb{N}\}$. You may use without proof the fact that a subset of $\mathbb{N}$ can be defined by a formula in Presburger arithmetic iff it is a union of finitely many arithmetic progressions.

3. In this problem, a *Presburger assertion* is a formula in the syntax of Presburger arithmetic where all variable occurrences are bound. Describe how to construct in linear time, given a Presburger assertion about structure $\langle \mathbb{Z}; 0, 1, +, \leq \rangle$, a Presburger assertion about structure $\langle \mathbb{N}; 0, 1, +, \leq \rangle$ that has the same truth value.

4. Give, for each $n \geq 1$, a system of linear equalities with coefficients from $\mathbb{Z}$ and variables interpreted over $\mathbb{Z}$, which has bit size bounded from above by a polynomial in n and on which *division-free Gaussian elimination* requires space exponential in n.

5. Prove there is likely no polynomial-time algorithm that determines whether a given conjunction of modulo constraints of the form $t_i \not\equiv r_i \pmod{m_i}$ is satisfiable, where $m_i \geq 2$ and $0 \leq r_i < m_i$ for each i, and each t_i is a linear polynomial. What changes if the constraints have $\equiv$ instead of $\not\equiv$?

6. Consider the following restricted version of *quantified integer programming*. The input is a sentence in Presburger arithmetic where (*i*) all coefficients at all variable occurrences are 0 and ± 1, (*ii*) in each inequality at most two variables appear, and (*iii*) there are no modulo (divisibility) constraints. Moreover, (*iv*) the sentence is in prenex normal form and the quantifier-free part is a conjunction of inequalities. The output is the truth value of the sentence. Can this problem be solved in polynomial space? Give a proof or show this unlikely.

7. By $\mathscr{Pres}\mathscr{E}xp$ we denote Presburger arithmetic extended with the function $x \mapsto 2^{|x|}$, where $|n|$ is the absolute value of $n \in \mathbb{Z}$.

For each of the following sentences, call it Φ, of $\mathscr{Pres}\mathscr{E}\boldsymbol{xp}$, show how to rewrite it into an equivalent sentence Ψ in $\mathscr{Pres}\mathscr{E}\boldsymbol{xp}$ using Semenov-style reasoning such that Ψ has the form $\forall u_1 \ldots \forall u_t\ \psi(u_1, \ldots, u_t)$ for some $t \geq 0$ and some variables $u_1, \ldots, u_t$, where ψ is a quantifier-free formula. The auxiliary function λ should not occur in Ψ.

Show your working. You can assume off-the-shelf procedures are available for the elimination of variables that have linear occurrences only, and for linearising power comparison constraints.

$$\begin{aligned}
\Phi_1 &: \quad \forall x\ \forall y\ \exists z\ (2 \cdot 2^{|x|} - 3 \cdot 2^{|y|} + z = 0) \\
\Phi_2 &: \quad \forall x\ \exists y\ \exists z\ (y = 2^{|x|}) \wedge (z = 2^{|y|}) \\
\Phi_3 &: \quad \forall x\ \exists a\ \exists b\ (2^{|a|} \leq x) \wedge (x < 2^{|b|}) \wedge (a + 1 = b) \\
\Phi_4 &: \quad \forall z\ \exists x\ \exists y\ (2 \cdot 2^{|x|} - 3 \cdot 2^{|y|} + z = 0)
\end{aligned}$$

Comment on the handling of conjunctions of inequalities (for Φ_2 and Φ_3). (The sketch in our Thursday lecture showed a single constraint only.)

References.

D. Chistikov. An introduction to the theory of linear integer arithmetic. *FSTTCS 2024.* DROPS link. *This is a general reference.*

D.C. Cooper. Theorem proving in arithmetic without multiplication. *Machine Intelligence* 7, 91–99, 1972. Edinburgh University Press. link

D.C. Oppen. A $2^{2^{2^{pn}}}$ upper bound on the complexity of Presburger arithmetic. *J. Comput. Syst. Sci.* 16(3), 323–332, 1978. doi link. (Conference version: Elementary bounds for Presburger arithmetic. *STOC 1973.* doi link.)

E.H. Bareiss. Sylvester's identity and multistep integer-preserving Gaussian elimination. *Math. Comput.* 22, 565–578, 1968. doi link.

D. Chistikov, A. Mansutti, M. Starchak. Integer linear-exponential programming in NP by quantifier elimination. *ICALP 2024.* arXiv link. *Section 4 and Appendix B are relevant for Gaussian elimination.*

M. Benedikt, D. Chistikov, A. Mansutti. The complexity of Presburger arithmetic with power or powers. *ICALP 2023.* arXiv link.

Additional reading.

S. Demri. Rudiments of Presburger arithmetic. Lecture notes (MPRI, M2, 2016). HAL link.

C. Haase. A survival guide to Presburger arithmetic. *ACM SIGLOG News* 5(3), 67–82, 2018. link