Algorithmic aspects of arithmetic theories with division

Advisor: Alessio Mansutti (*email:* alessio.mansutti@imdea.org)
Location: IMDEA Software Institute, Madrid, Spain

October 9, 2024

1 Context

Arithmetic theories are first-order logics about number systems, such as the integers or the real numbers. They represent a fundamental branch in mathematical logic, and play a pivotal role in various areas of computer science, encompassing both theoretical and practical applications:

- Arithmetic theories are extensively used in formal methods to verify the correctness of software and hardware systems. In the last decade this field has grown at an unprecedented rate, especially thanks to several algorithmic improvements in the fields of static analysis and Satisfiability Modulo Theory (SMT) solvers [BT18].
- Arithmetic theories are fundamental in the field of optimization: several networks, planning and scheduling problems can be represented using systems of inequalities, and solved using, e.g., Integer Linear Programming (ILP) algorithms [Sch99]. ILP corresponds to the conjunctive queries of Linear Integer Arithmetic (LIA, a.k.a. Presburger arithmetic).
- Connections between arithmetic theories and automata theory led to many surprising results. As an example, from the seminal work of Büchi we know that finite automata can be encoded into an extension of LIA known as Büchi arithmetic [BHMV94]. The vice-versa also holds: each formula of Büchi arithmetic corresponds to a finite automaton. Hundreds of results and open problems in combinatorics on words, number theory and other areas of discrete mathematics have been automatically proven using this connection [Sha22].

In the above areas of computer science, a significant attention has been reserved to three arithmetic theories: LIA, Linear Real Arithmetic (LRA) and Non-linear Real Arithmetic (NRA). LIA and LRA are the first-order theories of the integers and the reals numbers, respectively, together with the addition function and the order relation. In both these theories, the atomic formulae are given by linear inequalities. NRA extends LRA by introducing the multiplication function, thus allowing for multivariate polynomials of degree greater than one. The emphasis computer scientists place on these three theories is rooted in profound limits of computation:

- It is not possible to extend LIA with the multiplication function and have a complete procedure deciding the resulting theory. This is due to the celebrated proof by Matiyasevich, Robinson, Davis, and Putnam, demonstrating the undecidability of determining whether a system of polynomials over the integers has a solution (a.k.a. Hilbert's 10th problem).
- When it comes to extensions of NRA with further mathematical functions, one quickly reaches the limits of our current mathematical understanding. For instance, the extension of NRA

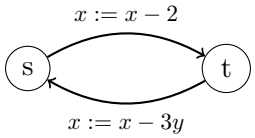
with the exponential function (NRAE) is only known to admit a decidable satisfiability problem subject to Schanuel's conjecture, a number theory conjecture that is widely believed to be true but completely out of reach for current mathematics.

Nonetheless, modern applications often demand to go beyond the three aforementioned theories, wandering near these limits of computation. To this end, several interesting theories of arithmetic have been very recently investigated. The following is a non-exhaustive list of works in this direction, limited to the last two years: [RHK23, BCM23, Sta23, DHMP24, DHM24, CMS24, BKN$^+$24, KLN$^+$24]. *The internship is placed in this context of investigating expressive theories of arithmetic.*

Before we continue. Below, I illustrate one possible research topic that can be tackled during the internship, but further topics in arithmetic theories are available; ranging from purely theoretical to practical ones. In case you are interested in the general subject of arithmetic theories and SMT solvers, but not on the specific topic below, do reach out!

2 Integer Linear Programming with divisibility constraints

Consider the following counter system having two states s and t and two integer variables x and y:



The system updates x by means of the two transitions between the two states; one transition decrements x by 2, the second transition decrements x by $3y$. Given a convex polyhedron $P \subseteq \mathbb{N}^2$, we are asked if there are $(u, v) \in P$ for which, starting from the state s and the initial assignment $(x = u, y = v)$, the counter system reaches the state t with the assignment $(x = 0, y = v)$.

How would you solve the above toy problem? A general way goes as follows. We first characterize the values of x that can be obtained by iterating the cycle $s \to t \to s$. Clearly, at every iteration of this cycle the variable x is decremented by $3y + 2$, and thus after z iterations the new value x' of the variable x corresponds to $x' = x - z \cdot (3y + 2)$. Our toy problem can then be formalized as follows. Are there $(x, y) \in \mathbb{Z}^2$ satisfying

$$(x, y) \in P \wedge \exists z \exists x' \exists x'' \in \mathbb{N} : x' = x - z \cdot (3y + 2) \wedge x'' = x' - 3y \wedge x'' = 0 \quad ?$$

Above, the variable x'' corresponds to the value of x after performing one last time the update $x := x - 3y$ following z iterations of the cycle $s \to t \to s$. We now see an issue: the constraint $x' = x - z \cdot (3y + 2)$ is quadratic, and this makes our problem out of reach for linear integer arithmetic solvers. We should not despair however: in this case, the variable z is simply encoding the fact that $x - x'$ must be divisible by $3y + 2$. Hence, the previous formula can be rewritten as

$$(x, y) \in P \wedge \exists x' \exists x'' \in \mathbb{N} : (3y + 2) \mid x - x' \wedge x' \leq x \wedge x'' = x' - 3y \wedge x'' = 0\,,$$

where $(3y + 2) \mid x - x'$ is a divisibility constraint that holds for integer values of y, x and x' such that $3y + 2$ divides $x - x'$; and the inequality $x' \leq x$ is added to force the quotient of the division (previously, the variable z) to be positive. This is an instance of IP-DIV.

Definition 1 (IP-DIV) *A* Integer linear program with divisibility constraints *(*IP-DIV*) is a system of constraints $\varphi(\boldsymbol{x})$ of the form*

$$\begin{gathered} A \cdot \boldsymbol{x} \leq \boldsymbol{b} \\ f_1(\boldsymbol{x}) \mid f_2(\boldsymbol{x}) \\ \cdots \\ f_{2n-1}(\boldsymbol{x}) \mid f_{2n}(\boldsymbol{x}) \,, \end{gathered}$$

where $\boldsymbol{x}$ is the vector of variables occurring in the system, A and $\boldsymbol{b}$ are an integer matrix and an integer vector, respectively, and each f_i is an integer linear polynomial in variables $\boldsymbol{x}$. The IP-DIV feasibility problem *asks for an input IP-DIV $\varphi(\boldsymbol{x})$ whether there is an integer assignment to the variables $\boldsymbol{x}$ making φ true.*

Regarding our toy problem, this is good news! It turns out that there is an algorithm to decide the IP-DIV feasibility problem.

Theorem 1 ([Lip78, Lip81, LOW15]) *The* IP-DIV *feasibility problem is* NP*-hard an in* NEXPTIME*. It is already* NP*-hard for 2 variables, 2 divisibility constraints and 4 inequalities.*

Over the years, the decidability of the IP-DIV feasibility problem turned out to be fundamental for many applications. Briefly, this problem found its first applications in the nineties, where it was used to solve bit-vector equations [MR98] and unification problems [Vor99]. Very recently, algorithms for IP-DIV have been used as black-boxes to solve word equations with length constraints [LM21] and to synthesize parameters in one-counter automata [PR22]. The algorithm for solving IP-DIV instances has been improved several times [Lip78, LOW15, DHM24]. Currently, the asymptotically best-known procedure is from myself, Rémy Défossez (ex-student of MPRI), Christoph Haase (Oxford University) and Guillermo A. Pérez (Antwerp University) [DHMP24].

Goal. Despite the very recent progress on algorithms for solving IP-DIV instances, the complexity of this problem is still poorly understood, as depicted by the gap in Theorem 1. The overall goal of the internship is to improve our understanding on this gap, by performing the first study on the geometry of the solutions of IP-DIV systems. The procedure from [DHMP24] has a clear bottleneck that may be explainable or avoidable by looking at issue. If "explainable", chances are we will be able to improve the current NP-hardness lower bound. If "avoidable", we will most probably be able to improve the NEXPTIME upper bound.

Want to know more about the problem? I have recently given an tutorial on this subject; the slides are here: alessiomansutti.github.io/slides/24tiat.pdf. Otherwise, you can look at the paper by Lechner, Ouaknine and Worrell [LOW15] (skipping Section 3).

3 On the advisor

I am an Assistant Professor at the IMDEA Software Institute. Prior to joining IMDEA, I was a Research Associate in the Automated Verification Group of the University of Oxford, working with Christoph Haase in arithmetic theories. I hold a PhD degree in Computer Science from ENS Paris-Saclay, where I was a student of Stéphane Demri and Étienne Lozes in the Laboratoire Spécification et Vérification (it is now the Laboratoire Méthodes Formelles — LMF).

4 On the internship

The internship will take place in Madrid (Spain) where IMDEA Software is situated. The internship position can be fully funded. The working language at the institute is English. Knowledge of Spanish is not required.

IMDEA Software is a public research institute. It was funded in 2006 with the objective of advancing the scientific and technological foundations that allow the cost-efficient development of software characterized by sophisticated functionality and high quality, in terms of safety, reliability, and efficiency. Researchers at the institute cover mostly three areas: (1) Security and Privacy, (2) Program Analysis and Verification, and (3) Languages, Compilers, and Systems.

References

[BCM23] Michael Benedikt, Dmitry Chistikov, and Alessio Mansutti. The complexity of presburger arithmetic with power or powers. In *ICALP*, volume 261 of *LIPIcs*, pages 112:1–112:18. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2023.

[BHMV94] Véronique Bruyère, Georges Hansel, Christian Michaux, and Roger Villemaire. Logic and p-recognizable sets of integers. *Bulletin of the Belgian Mathematical Society - Simon Stevin*, 1(2):191 – 238, 1994.

[BKN+24] Valérie Berthé, Toghrul Karimov, Joris Nieuwveld, Joël Ouaknine, Mihir Vahanwala, and James Worrell. On the decidability of monadic second-order logic with arithmetic predicates. In *LICS*, pages 11:1–11:14. ACM, 2024.

[BT18] Clark Barrett and Cesare Tinelli. *Satisfiability Modulo Theories*, pages 305–343. Springer International Publishing, 2018.

[CMS24] Dmitry Chistikov, Alessio Mansutti, and Mikhail R. Starchak. Integer linear-exponential programming in NP by quantifier elimination. In *ICALP*, volume 297 of *LIPIcs*, pages 132:1–132:20. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2024.

[DHM24] Andrei Draghici, Christoph Haase, and Florin Manea. Semënov arithmetic, affine {VASS}, and string constraints. In *STACS*, volume 289 of *LIPIcs*, pages 29:1–29:19. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2024.

[DHMP24] Rémy Défossez, Christoph Haase, Alessio Mansutti, and Guillermo A. Pérez. Integer programming with GCD constraints. In *SODA*, pages 3605–3658. SIAM, 2024.

[KLN+24] Toghrul Karimov, Florian Luca, Joris Nieuwveld, Joël Ouaknine, and James Worrell. On the decidability of presburger arithmetic expanded with powers. *CoRR*, abs/2407.05191, 2024.

[Lip78] Leonard Lipshitz. The Diophantine problem for addition and divisibility. *Trans. Am. Math. Soc*, pages 271–283, 1978.

[Lip81] Leonard Lipshitz. Some remarks on the Diophantine problem for addition and divisibility. *Bull. Soc. Math. Belg. Sér. B*, 33(1):41–52, 1981.

[LM21] Anthony W. Lin and Rupak Majumdar. Quadratic word equations with length constraints, counter systems, and Presburger arithmetic with divisibility. *Log. Methods Comput. Sci.*, 17(4), 2021.

[LOW15] Antonia Lechner, Joël Ouaknine, and James Worrell. On the complexity of linear arithmetic with divisibility. In *Proc. Symposium on Logic in Computer Science, LICS*, pages 667–676, 2015.

[MR98] M. Oliver Möller and Harald Rueß. Solving bit-vector equations. In *FMCAD*, volume 1522 of *Lecture Notes in Computer Science*, pages 36–48. Springer, 1998.

[PR22] Guillermo A. Pérez and Ritam Raha. Revisiting parameter synthesis for one-counter automata. In *CSL*, volume 216 of *LIPIcs*, pages 33:1–33:18. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022.

[RHK23] Rodrigo Raya, Jad Hamza, and Viktor Kuncak. On the complexity of convex and reverse convex prequadratic constraints. In *LPAR*, volume 94 of *EPiC Series in Computing*, pages 350–368. EasyChair, 2023.

[Sch99] Alexander Schrijver. *Theory of linear and integer programming.* Wiley-Interscience series in discrete mathematics and optimization. Wiley, 1999.

[Sha22] Jeffrey Shallit. *The Logical Approach to Automatic Sequences: Exploring Combinatorics on Words with Walnut.* London Mathematical Society Lecture Note Series. Cambridge University Press, 2022.

[Sta23] Mikhail R. Starchak. On the existential arithmetics with addition and bitwise minimum. In *FoSSaCS*, volume 13992 of *Lecture Notes in Computer Science*, pages 176–195. Springer, 2023.

[Vor99] Andrei Voronkov. Simultaneous rigid e-unification and other decision problems related to the herbrand theorem. *Theor. Comput. Sci.*, 224(1-2):319–352, 1999.