Unité Mixte de Recherche 5104 CNRS - INPG - UJF
Centre Equation
2, avenue de VIGNATE
F-38610 GIERES
tel : +33 456 52 03 40
fax : +33 456 52 03 50
http://www-verimag.imag.fr

On Decidability within the Arithmetic of Addition and Divisibility

Marius Bozga and Radu Iosif

Report n^o TR-2004-18

January 6, 2005

On Decidability within the Arithmetic of Addition and Divisibility

Marius Bozga and Radu Iosif

January 6, 2005

Abstract

The arithmetic of natural numbers with addition and divisibility has been shown undecidable as a consequence of the fact that multiplication of natural numbers can be interpreted into this theory, as shown by J. Robinson [Rob49]. The most important decidable subsets of the arithmetic of addition and divisibility are the arithmetic of addition, proved by M. Presburger [Pre29], and the purely existential subset, proved by L. Lipshitz [Lip76]. In this paper we define a new decidable fragment of the form $QzQ_1x_1 \ldots Q_nx_n\varphi(\vec{x}, z)$ where the only variable allowed to occur to the left of the divisibility sign is z. For this form, called $\mathcal{L}_|^{(1)}$ in the paper, we show the existence of a quantifier elimination procedure which always leads to formulas of Presburger arithmetic. We generalize the $\mathcal{L}_|^{(1)}$ form to $\exists z_1, \ldots \exists z_m Q_1x_1 \ldots Q_nx_n\varphi(\vec{x}, \vec{z})$, where the only variables appearing on the left of divisibility are $z_1, \ldots, z_m$. For this form, called $\exists\mathcal{L}_|^{(*)}$, we show decidability of the positive fragment, namely by reduction to the existential theory of the arithmetic with addition and divisibility. The $\mathcal{L}_|^{(1)}$, $\exists\mathcal{L}_|^{(*)}$ fragments were inspired by a real application in the field of program verification. We considered the satisfiability problem for a program logic used for quantitative reasoning about memory shapes, in the case where each record has at most one pointer field. The reduction of this problem to the positive subset of $\exists\mathcal{L}_|^{(*)}$ is sketched in the end of the paper.

Keywords: arithmetic theories, decidability, quantifier elimination, quantitative analysis

Reviewers:

Notes:

How to cite this report:

```
@techreport { ,
title = { On Decidability within the Arithmetic of Addition and Divisibility},
authors = { Marius Bozga and Radu Iosif},
institution = { Verimag Technical Report },
number = {TR-2004-18},
year = { },
note = { }
}
```

1 Introduction

The undecidability of first-order arithmetic of natural numbers occurs as a consequence of Gödel's Incompleteness Theorem [G3̈1]. The basic result has been discovered by A. Church [Chu36], and the essential undecidability (undecidability of its every consistent extension) by B. Rosser [Ros36], both as early as 1936. Consequences of this result are the undecidability of the theory of natural numbers with *multiplication and successor function* and with *divisibility and successor function*, both discovered by J. Robinson in [Rob49]. To complete the picture, the existential fragment of the full arithmetic i.e., *Hilbert's Tenth Problem* was proved undecidable by Y. Matiyasevich [Mat70]. The interested reader is further pointed to [B0́2] for an excellent survey of the (un)decidability results in arithmetic.

On the positive side, the decidability of the arithmetic of natural numbers with addition and successor function has been shown by M. Presburger [Pre29], result which has found many applications in modern computer science, especially in the field of automated reasoning. Another important result is the decidability of the *existential* theory of addition and divisibility, proved independently by A. P. Beltyukov [Bel76] and L. Lipshitz [Lip76]. Namely, it is shown that formulas of the form $\exists x_1, \ldots \exists x_n \bigwedge_{i=1}^{K} f_i(\vec{x})|g_i(\vec{x})$ are decidable, where f_i, g_i are linear functions over $x_1, \ldots x_n$ and the symbol $|$ means that each f_i is an integer divisor of g_i when both are interpreted over $\mathbb{N}^n$. The decidability of formulas of the form $\exists x_1, \ldots \exists x_n \varphi(\vec{x})$, where φ is an open formula in the language $\langle +, |, 0, 1\rangle$, is stated as a corollary in [Lip76].

In this paper we work within the theory of natural numbers with addition and divisibility, our results being also applicable to integers. We start from an observation encountered in [Lip76], namely that an atomic proposition $f(\vec{x}, y)|g(\vec{x}, y)$ where y occurs in f with a non-zero coefficient, can be replaced by an equivalent formula $\varphi(\vec{x}, y)$ of Presburger arithmetic, under the assumption $y \geq x_i$, for all $x_i \in \vec{x}$. An immediate consequence is that any formula of $\langle \mathbb{N}, +, |, 0, 1\rangle$, such that for any atomic proposition $f(\vec{x})|g(\vec{y})$ we have $\vec{y} \subseteq \vec{x}$, $\vec{x}$ denoting the set of variables that occurs in f with a non-null coefficient, can be directly defined in Presburger arithmetic. This simple fact motivates the search for more expressive decidable subsets of $\langle \mathbb{N}, +, |, 0, 1\rangle$, in which at least one variable that occurs on the right side of the divisibility sign does not occur simultaneously on the left.

Our main result is the decidability of formulas of the form $QzQ_1x_1 \ldots Q_nx_n\varphi(\vec{x}, z)$ where $Q, Q_1 \ldots Q_n \in \{\exists, \forall\}$, φ is quantifier-free, and all divisibility propositions are of the form $f(z)|g(\vec{x}, z)$, with f, g linear functions. This form is called $\mathcal{L}_|^{(1)}$, as there is only one variable that appears on the left of $|$. We show that any formula in this fragment can be evaluated by applying quantifier elimination to the open formula $Q_1x_1 \ldots Q_nx_n\varphi(\vec{x}, z)$, the result being a Presburger formula in which z occurs free. This fact is somewhat surprising, since the $\mathcal{L}_|^{(1)}$fragment allows to encode queries apparently beyond the scope of Presburger arithmetic such as: given a Presburger formula φ with n free variables, is it true that all values $v_1, \ldots, v_n$ which satisfy φ, are altogether *relatively prime*?

Second, a generalization is made by allowing multiple existentially quantified variables occur to the left of the divisibility sign that is, formulas of the form $\exists z_1 \ldots \exists z_n Q_1x_1 \ldots Q_mx_m\varphi(\vec{x}, \vec{z})$, for quantifier-free φ, where the only divisibility propositions are of the form $f(\vec{z})|g(\vec{x}, \vec{z})$. Using essentially the same method as in the case of $n = 1$, we show decidability of the *positive* form of the $\exists\mathcal{L}_|^{(*)}$subset i.e., in which no divisibility proposition occurs under negation. However the result of quantifier elimination for the positive $\exists\mathcal{L}_|^{(*)}$fragment cannot be expressed in Presburger arithmetic, but in the existential fragment of $\langle\mathbb{N}, +, |, 0, 1\rangle$. This result is also the best possible in the sense that, if negation of divisibility propositions is allowed, the $\exists\mathcal{L}_|^{(*)}$fragment is undecidable. The worst-case complexity of the quantifier elimination method is non-elementary and the decision complexity for the alternation-free fragments of $\mathcal{L}_|^{(1)}$, $\exists\mathcal{L}_|^{(*)+}$are bounded by a triple exponential.

We applied the decidability result for the positive $\exists\mathcal{L}_|^{(*)}$fragment to a concrete problem in the field of program verification. More precisely, we consider a specification logic used to reason about the shape of the recursive data structures generated by imperative programs that handle pointers. This logic, called *alias logic with counters* [BIL04] is interpreted over deterministic labeled graphs. It allows to express linear arithmetic relations between the lengths of certain paths within a graph. The satisfiability problem has been shown undecidable over unrestricted dag, and implicitly, graph models, but decidability can be shown over tree models. We complete the picture by showing decidability of this logic over structures composed of an arbitrary finite number of lists. The difficulty w.r.t trees consists in the fact that lists may have loops, which introduce divisibility constraints. However, as it is shown, the problem remains within the bounds of the positive $\exists\mathcal{L}_|^{(*)}$ fragment of $\langle\mathbb{N}, +, |, 0, 1\rangle$. Despite its catastrophic complexity upper bound, this result enables, in principle, the automatic verification of quantitative properties for an important class of programs that manipulate list structures only.

2 Preliminaries

In this paper we work with first-order logic over the language $\langle +, |, 0, 1\rangle$. A formula in this language is interpreted over $\mathbb{N}$ in the standard way: $+$ denotes the addition of natural numbers, $|$ is the divisibility relation, and $0, 1$ are the constants zero and one. In particular, we consider that $0|0$, $0 \not| n$ and $n|0$, for all $n \in \mathbb{N} \setminus \{0\}$. In the following we will intentionally use the same notation for a mathematical constant symbol and its interpretation, as we believe, no confusion will arise from that.

The results in this paper rely on two theorems from elementary number theory. The first one is the well-known Chinese Remainder Theorem (CRT) [DPS99] and the second one is a (prized) conjecture proposed by P. Erdös in 1963 and proved by R. Crittenden and C. Vanden Eynden in 1969 [CE69]. The CRT says that: $\exists x \bigwedge_{i=1}^{K} m_i|(x - r_i) \leftrightarrow \bigwedge_{1\le i,j\le K}(m_i, m_j)|(r_i - r_j)$, where $m_i \in \mathbb{N}, r_i \in \mathbb{Z}$ and (a, b) denotes the greatest common divisor of a and b [1]. The CRT can be slightly generalized as follows:

[1]The second part of the Theorem, expressing the solutions x to the system of linear congruences on the left hand of the equivalence is not used in this paper.

Corollary 1 *For any integers $m_i \in \mathbb{N}$ and $a_i \in \mathbb{Z} \setminus \{0\}, r_i \in \mathbb{Z}$ with $1 \leq i \leq K$ we have:*

$$\exists x \bigwedge_{i=1}^{K} m_i|(a_i x - r_i) \leftrightarrow \bigwedge_{1 \leq i,j \leq K} (a_i m_j, a_j m_i)|(a_i r_j - a_j r_i) \wedge \bigwedge_{i=1}^{K} (a_i, m_i)|r_i$$

Proof: Let $A = \Pi_{i=1}^{K} a_i$ and $A_i = \frac{A}{a_i}$.

$$\begin{aligned}
\exists x \bigwedge_{i=1}^{K} m_i|(a_i x - r_i) \quad &\longleftrightarrow \quad \exists x \bigwedge_{i=1}^{K} A_i m_i|(Ax - A_i r_i) \longleftrightarrow \exists y \bigwedge_{i=1}^{K} A_i m_i|(y - A_i r_i) \wedge A|y \\
&\overset{CRT}{\longleftrightarrow} \quad \bigwedge_{1 \leq i < j \leq K} (A_i m_i, A_j m_j)|(A_i r_i - A_j r_j) \wedge \bigwedge_{1 \leq i \leq K} (A_i m_i, A)|A_i r_i \\
&\longleftrightarrow \quad \bigwedge_{1 \leq i,j \leq K} (a_i m_j, a_j m_i)|(a_i r_j - a_j r_i) \wedge \bigwedge_{i=1}^{K} (a_i, m_i)|r_i
\end{aligned}$$

$\square$

Usually the CRT is used as a means of solving systems of linear congruences. A linear congruence equation is an equation of the form $ax \equiv b \mod m$, for some $a, b \in \mathbb{Z}$ and $m \in \mathbb{N} \setminus \{0\}$. Such an equation is solvable if and only if $(a, m)|b$. If the equation admits one solution y, then the solutions are given by the arithmetic progression $\{x \equiv y \mod \frac{m}{(a,m)}\}$. The second Theorem, stated as a conjecture by Erdös, is the following:

Theorem 1 ([CE69]) *Let $a_1, \ldots, a_n \in \mathbb{Z}, b_1, \ldots, b_n \in \mathbb{N} \setminus \{0\}$. Suppose there exists an integer x_0 satisfying none of the congruences: $\{x \equiv a_i \mod b_i\}_{i=1}^{n}$. Then there is such an x_0 among $1, 2, 3, \ldots, 2^n$.*

We shall use this theorem rather in its positive form i.e., n arithmetic progressions $\{a_i + b_i\mathbb{Z}\}_{i=1}^{n}$ cover $\mathbb{Z}$ if and only if they cover the set $1, 2, 3, \ldots, 2^n$.

If we interpret a linear congruence over $\mathbb{Z}$ instead of $\mathbb{N}$ we obtain that the solutions form an infinite progression containing both positive and negative numbers. In other words, $ax \equiv b \mod m$ has a solution in $\mathbb{N}$ if and only if it has a solution in $\mathbb{Z}$. The same reasoning applies to the CRT, since the solution of a system of linear congruences is the intersection of a finite number of progressions, hence a progression itself. As for Erdös' Conjecture, we can see that it is true for positive integers only (Corollary 3 in Appendix A) . In conclusion, the above theorems hold for $\mathbb{Z}$ as well as they do for $\mathbb{N}$. In general, all results in this paper apply the same to integer and natural numbers, therefore we will not make the distinction unless necessary[2].

[2]For instance, it is not clear whether one can define the order relation in the existential fragment of $\langle \mathbb{Z}, +, |, 0, 1\rangle$, hence we will work with $\langle \mathbb{Z}, +, |, \leq, 0, 1\rangle$ instead of it, whenever needed.

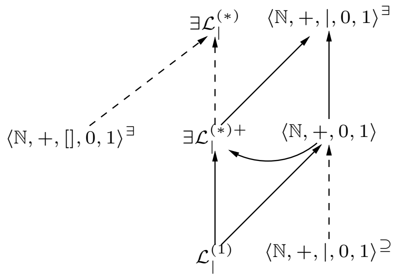


Figure 1:

3 Setting up the Scene

The discussion of this section is intended to motivate formally our definitions of decidable subsets of $\langle \mathbb{N}, +, |, 0, 1\rangle$, by establishing relations between our results and the existing ones [Pre29], [Lip76].

For the purposes of this discussion, we consider two different relations between theories: definability and reducibility. Let T_1 and T_2 be two theories interpreted over the same universe. On one hand, we say that T_1 is *definable* in T_2 if, for every relation symbol $R(x_1, \ldots, x_n)$ in the language of T_1 there exists an open formula $\phi_R(x_1, \ldots, x_n)$, with free variables $x_1, \ldots, x_n$, in the language of T_2 such that, for any interpretation of $x_1, \ldots, x_n$, R holds in T_1 if and only if ϕ_R holds in T_2. On the other hand, we say that T_1 is *reducible* to T_2 if there exists a Turing machine that transforms every formula $\phi_1(x_1, \ldots, x_n)$ in the language of T_1 into a formula $\phi_2(x_1, \ldots, x_n)$ in the language of T_2, such that, for any interpretation of $x_1, \ldots, x_n$, ϕ_1 holds in T_1 if and only if ϕ_2 holds in T_2. Obviously, definability implies reducibility, but not viceversa. For instance, any formula of Presburger arithmetic can be transformed into a system of linear equations and congruences using quantifier elimination, however the method is non-trivial [Pre29], [FR74]. Our search for decidable theories is pointed towards theories that are not trivially definable in a well-known decidable theory. As it will turn out, our results are however reducible to known theories.

Figure 1 describes the contributions of this paper. The dotted arrows represent definability relations, while the solid ones stand for reducibility relations. All theories presented here are interpreted over $\mathbb{N}$, but the relations transfer to $\mathbb{Z}$ without difficulty. We denote by $\langle \mathbb{N}, +, |, 0, 1\rangle^{\supseteq}$ the fragment of $\langle \mathbb{N}, +, |, 0, 1\rangle$, obtained by applying the restriction that each divisibility proposition is of the form $f(\vec{x})|g(\vec{y})$, where $\vec{x} \supseteq \vec{y}$ and moreover, each $y \in \vec{y}$ is bound to occur in f with a non-null coefficient. By $\langle \mathbb{N}, +, 0, 1\rangle$ we denote the Presburger arithmetic and $\langle \mathbb{N}, +, |, 0, 1\rangle^{\exists}$ stands for the purely existential subset of $\langle \mathbb{N}, +, |, 0, 1\rangle$. By $\langle \mathbb{N}, +, [], 0, 1\rangle^{\exists}$ we denote the existential fragment of the arithmetic with addition and the least common multiple relation, denoted as $[x, y] = z$.

The contribution of this paper is the definition and study of the $\mathcal{L}_{|}^{(*)}$ fragment of $\langle \mathbb{N}, +, |, 0, 1\rangle$. In general, $\mathcal{L}_{|}^{(n)}$ denotes the class of formulas where only the first n variables (in prenex form) appear to the left of the divisibility sign in an atomic proposition. Formally, $\mathcal{L}_{|}^{(n)}$ is the set of formulas $Q_1 z_1 \ldots Q_n z_n R_1 x_1 \ldots R_m x_m \varphi(\vec{x}, z)$ where $Q_i, R_j \in \{\exists, \forall\}$ and the only divisibility propositions are $f(\vec{z})|g(\vec{x},\vec{z})$, with f and g linear functions. The set $\mathcal{L}_|^{(*)}$is the union of all $\mathcal{L}_|^{(n)}$, for $n \geq 1$. We denote by $\exists\mathcal{L}_|^{(*)}$the subset of $\mathcal{L}_|^{(*)}$obtained by setting, in each $\mathcal{L}_|^{(n)}$, $Q_i \equiv \exists$, for all $1 \leq i \leq n$ and, by $\exists\mathcal{L}_|^{(*)+}$, the set of all formulas of $\exists\mathcal{L}_|^{(*)}$in which no divisibility proposition occurs within the scope of a logical negation.

The definability of $\langle \mathbb{N}, +, |, 0, 1\rangle^{\supseteq}$ into $\langle \mathbb{N}, +, 0, 1\rangle$ occurs as a consequence of the following simple lemma:

Lemma 1 ([Lip76]) *Let f and g be linear functions with positive coefficients, $f(\vec{x}, y) = ay + h(\vec{x})$, $a \neq 0$ and $g(\vec{x}, y) = b_0 + \Sigma_{i=1}^{p-1} b_j x_j + b_p y$. Under the assumption $\bigwedge_{i=1}^{n} y \geq x_i$, we have that $f(\vec{x}, y)|g(\vec{x}, y) \leftrightarrow \bigvee_{k=1}^{\Sigma_{j=0}^{p} b_j} kf(\vec{x}, y) = g(\vec{x}, y)$.*

Proof: Since $y \geq x_i$ we have $y\Sigma_{j=0}^{p} b_j \geq g(\vec{x}, y) = kf(\vec{x}, y) = k(ay + h(\vec{x}))$. Now $a > 0$ implies $y\Sigma_{j=0}^{p} b_j \geq ky$, hence $k \leq \Sigma_{j=0}^{p} b_j$. $\Box$ Let $\phi(\vec{x})$ be an open formula of $\langle \mathbb{N}, +, |, 0, 1\rangle^{\supseteq}$, to which we adjoin the valid formula $\bigvee_{1 \leq i_1, \ldots, i_n \leq n} x_{i_1} \leq x_{i_2} \wedge \ldots \wedge x_{i_{n-1}} \leq x_{i_n}$. If there are negative coefficients in ϕ, we can write ϕ as a finite union of formulas with positive coefficients only, using the method from [Lip76]. Now return to disjunctive normal form and apply Lemma 1 to replace each divisibility proposition by a Presburger formula. This is possible due the assumption that each $y \in \vec{y}$ occurs in f under a non-null coefficient.

So an essential ingredient of non-trivial subtheories of $\langle \mathbb{N}, +, |, 0, 1\rangle$ is the occurrence of variables exclusively to the right of the divisibility sign. In the definition of $\mathcal{L}_|^{(*)}$we take this fact into account, allowing unrestricted quantification over these variables. On the other hand, in $\exists\mathcal{L}_|^{(*)}$, all variables on the left of the divisibility sign are existentially quantified. The latter assumption is motivated by the fact that one can e.g., define primeness of x as $\forall t\ t|x \rightarrow t = 1 \vee t = x$ and use it to further define multiplication[3].

The remaining relations from Figure 1, namely the reductions from $\mathcal{L}_|^{(1)}$to Presburger arithmetic and from $\exists\mathcal{L}_|^{(*)+}$to $\langle \mathbb{N}, +, |, 0, 1\rangle^{\exists}$ are the topics of Sections 4 and 5. The undecidability of $\exists\mathcal{L}_|^{(*)}$ is a consequence of the fact that $\langle \mathbb{N}, +, [], 0, 1\rangle^{\exists}$ can be defined into it and the latter is undecidable, as it will be shown in the end of Section 5. Presburger arithmetic can be reduced to $\exists\mathcal{L}_|^{(*)+}$and $\langle \mathbb{N}, +, |, 0, 1\rangle^{\exists}$ due to the fact that it has quantifier elimination [Pre29].

4 Decidability of $\mathcal{L}_|^{(1)}$

In this section we show that the $\mathcal{L}_|^{(1)}$class can be effectively reduced to the $\langle \mathbb{N}, +, 0, 1\rangle$ theory. Mostly for clarity, we will work first with a simplified form, in which each divisibility atomic proposition is of the form $z|f(\vec{x}, z)$, and then we generalize to propositions of the form

[3]The undecidability proof of $\langle \mathbb{N}, +, |, 0, 1\rangle$ given in [Woo81] uses the fact that each number can be written as sum of at most 7 primes and that the product of two distinct primes is their least common multiple.

$h(z)|f(\vec{x},z)$, with f,h linear functions. Hence we start explaining the reduction of formulas of the following simple form:

$$Q_1x_1\dots Q_nx_n \bigvee_{i=1}^{N}\Big(\bigwedge_{j=1}^{M_i} z|f_{ij}(\vec{x},z)\wedge\bigwedge_{j=1}^{P_i} z\not| g_{ij}(\vec{x},z)\wedge\varphi_i(\vec{x},z)\Big) \tag{1}$$

where f_{ij} and g_{ij} are linear functions with integer coefficients and φ_i, are Presburger formulas with $\vec{x}$ and z free.

The general form (1) is not yet suitable for quantifier elimination due to the following inconvenient: the same variable x_k, for some $1\le k\le n$, might appear both in a divisibility proposition and in a Presburger formula $\varphi_i(\vec{x},z)$. This precludes the application of the CRT in the given form (Corollary 1). To overcome this problem, we eliminate first the φ_i subformulas from (1) as described in the following.

As Presburger arithmetic has quantifier elimination [Pre29], we can assume w.l.o.g. that $\varphi_i(\vec{x},z)\equiv\bigvee_k\bigwedge_l\exists t_{kl}\ t_{kl}\ge 0\ \wedge\ h_{kl}(\vec{x},z)+t_{kl}=0\ \wedge\ \bigwedge_l c_{kl}|h'_{kl}(\vec{x},z)$, with h_{kl},h'_{kl} linear functions with integer coefficients, and c_{kl} positive integer constants. Suppose now that x_m, for some $1\le m\le n$, appears in some $h_{kl}(\vec{x})=a_{kl}x_m+b_{kl}(\vec{x},z)$ with coefficient $a_{kl}\neq 0$. We multiply through with a_{kl} by replacing all formulas of the form $h(\vec{x},z)+t=0$ with $a_{kl}h(\vec{x},z)+a_{kl}t=0$, $c|h'(\vec{x},z)$ with $a_{kl}c|a_{kl}h'(\vec{x},z)$, and $z|f(\vec{x},z)$ with $a_{kl}z|a_{kl}f(\vec{x},z)$. Then we eliminate $a_{kl}x_m$ by substituting it with $-b_{kl}(\vec{x},z)-t_{kl}$, which does not contain x_m. The CRT can be applied a number of times to eliminate the t_{kl} variables[4]. We repeat the above steps until all x variables occurring within linear equations have been eliminated. The resulting formula is of the form:

$$Q_1x_1\dots Q_nx_n \bigvee_{i=1}^{N}\Big(\bigwedge_{j=1}^{M_i} z_{ij}|f_{ij}(\vec{x},z)\wedge\bigwedge_{j=1}^{P_i} z_{ij}\not| g_{ij}(\vec{x},z)\wedge\psi_i(z)\Big) \tag{2}$$

where each z_{ij} is either $a_{ij}z$, $a_{ij}\in\mathbb{N}\setminus\{0\}$, or a constant $c_{ij}\in\mathbb{N}$ and $\psi_i(z)$ are Presburger formulas in which z occurs free. In the rest of the section we show how to reduce an arbitrary formula of the form (2) to an equivalent Presburger formula in two phases: first, we successively eliminate the quantifiers $Q_1x_1,\dots,Q_nx_n$ and second, we define the resulting solved form into Presburger arithmetic.

Quantifier Elimination

We consider three cases, based on the type of the last quantifier Q_n ($\exists,\forall$) and the sign of the divisibility propositions occurring in the formula (positive, negative). Namely, we treat the cases existential positive, universal positive and universal mixed. The remaining case (existential mixed) can be dealt with by first negating and then applying the universal mixed case.

[4] Notice that the constraint $t_{kl}\ge 0$ is trivially satisfied if we work with $\mathbb{N}$, otherwise, for $\mathbb{Z}$, we can use the fact that the solutions to a linear congruence system form a progression that contains infinitely many positive and negative numbers.

The Existential Positive Case In this case the formula (2) becomes:

$$\bigvee_{i=1}^{N} \exists x_n \bigwedge_{j=1}^{M_i} z_{ij}|f_{ij}(\vec{x}, z) \wedge \psi_i(z) \tag{3}$$

W.l.o.g. we can assume that $M_i \neq 0$ for all $1 \leq i \leq N$, and that $f_{ij}(\vec{x}, z) = a_{ij}x_n + g_{ij}(\vec{x'}, z)$, where $\vec{x'} = \vec{x} \setminus \{x_n\}$, and with all coefficients $a_{ij} \neq 0$. Applying Corollary 1 to the i-th disjunct, we obtain (the original i subscript has been omitted): $\bigwedge_{1\leq k,l\leq M}(a_k z_l, a_l z_k)|(a_k g_l - a_l g_k) \wedge \bigwedge_{1\leq k\leq M}(a_k, z_k)|g_k \wedge \psi(z)$. In the resulting formula we have three types of divisibility propositions, which we can write equivalently as:

- $(a_i a' z, a_j a'' z)|(a_i g_j - a_j g_i) \ : \ (a_i a', a_j a'')z|(a_i g_j - a_j g_i)$
- $(a_i, az)|g_i \ : \ \bigvee_{r=0}^{a_i - 1}(az \equiv r) \mod a_i \wedge (a_i, r)|g_i$
- $(a_i c_j, a_j c_i)|(a_i g_j - a_j g_i)$ and $(a_i, c_i)|g_i$ are left untouched.

We have used the equivalence $(az, c)|f \leftrightarrow \bigvee_{r=0}^{c-1} az \equiv r \mod c \wedge (r, c)|f$. Now $az \equiv r \mod c$ is a Presburger formula with z free. The formula can now be easily written back in the form (3), with $n - 1$ variables of type x_i, instead of n. The size of the resulting formula (in DNF) is at most quadratic in the size of the input.

The Universal Positive Case It is now convenient to consider the matrix of (2) in conjunctive normal form. In this case the formula (2) becomes:

$$\bigwedge_{i=1}^{P} \forall x_n \bigvee_{j=1}^{Q_i} z_{ij}|f_{ij}(\vec{x}, z) \vee \psi_i(z) \tag{4}$$

W.l.o.g. we can assume that $f_{ij}(\vec{x}, z) = a_{ij}x_n + b_{ij}(\vec{x'}, z)$, where $\vec{x'} = \vec{x} \setminus \{x_n\}$, and with all coefficients $a_{ij} \neq 0$. In each i-conjunct, the union of Q_i arithmetic progressions $\{x \mid a_{ij}x \equiv -b_{ij} \mod z_{ij}\}_{j=1}^{Q_i}$ covers $\mathbb{N}$. By Theorem 1 it is sufficient (and trivially necessary) to cover only the first 2^{Q_i} values. The equivalent form, with x_n eliminated, is the following: $\bigwedge_{i=1}^{P} \bigwedge_{t=1}^{2^{Q_i}} \bigvee_{j=1}^{Q_i} z_{ij}|a_{ij}t + b_{ij} \vee \psi_i(z)$. The size of the resulting formula (in CNF this time) is simply exponential in the size of the input.

The Universal Mixed Case Let us consider again the formula (2) with the matrix written in conjunctive normal form:

$$\bigwedge_{i=1}^{P} \forall x_n \Big(\bigvee_{j=1}^{Q_i} z_{ij}|f_{ij}(\vec{x}, z) \vee \bigvee_{j=1}^{R_i} z_{ij} \not| g_{ij}(\vec{x}, z) \Big) \vee \psi_i(z) \tag{5}$$

Again, we can assume w.l.o.g. that x_n occurs in each f_{ij}, g_{ij} with a non-zero coefficient. Also Q_i, R_i can be considered greater than zero for all $1 \leq i \leq n$, the other cases being treated in the previous. Each i-conjunct, omitting the i subscript, is: $\forall x_n \Big(\bigwedge_{j=1}^{R} z_j | g_j(\vec{x}, z) \rightarrow \bigvee_{j=1}^{Q} z_j | f_j(\vec{x}, z) \Big) \vee \psi(z)$. The parenthesized formula can be understood as coverage of an arithmetic progression by a finite union of arithmetic progressions. Assuming $g_j(\vec{x}, z) = a_j x_n + b_j(\vec{x}, z)$ with $a_j \neq 0$, let us compute the period of the set $\{x : \bigwedge_{j=1}^{R} z_j | g_j(\vec{x}, z)\} = \bigcap_{j=1}^{R} \{x : a_j x \equiv b_j \mod z_j\}$. Each linear congruence $a_j x \equiv b_j \mod z_j$ has a periodic solution with period $\frac{z_j}{(z_j, a_j)}$. The period of the intersection is the least common multiple of the individual periods i.e., $\Big[\{\frac{z_j}{(z_j, a_j)}\}_{j=1}^{R}\Big]$. Since all z_j's are either $a'_j z$, for $a'_j \in \mathbb{N} \setminus \{0\}$ or some constants c_j, using Lemma 3 from Appendix A, we can simplify the expression of the period to the form $\frac{zk_j}{(z, l_j)}$ for some (effectively computable) constant values $k_j, l_j \in \mathbb{N} \setminus \{0\}$. Now we can apply Theorem 1 and eliminate $\forall x_n$ from the i-th conjunct of the formula (5). Supposing $f_j(\vec{x}, z) = c_j x_n + d_j(\vec{x}, z)$ for some $c_j, d_j \in \mathbb{Z}, c_j \neq 0$, the result is: $\neg \exists y \bigwedge_{j=1}^{R} z_j | a_j y + b_j(\vec{x}, z) \vee \exists y \bigwedge_{j=1}^{R} z_j | a_j y + b_j(\vec{x}, z) \wedge \bigwedge_{t=1}^{2^Q} \bigvee_{j=1}^{Q} z_j | c_j \Big(y + \frac{zk_j t}{(z, l_j)} \Big) + d_j(\vec{x}, z)$. The first disjunct is for the trivial case, in which the set $\{x : \bigwedge_{j=1}^{R} z_j | g_j(\vec{x}, z)\}$ is empty, while the second disjunct assumes the existence of an element y of this set and encodes the equivalent condition of Theorem 1, namely that the first 2^Q elements of this set, starting with y, must be covered by the union of Q progressions. Now y can be eliminated from the above formula using CRT, as in the existential positive case, treated in the previous. Notice that, in addition to the existential positive case, we have introduced a subterm of the form $\frac{zk}{(z,l)}$ within the functions f_j. This is reflected in the definition of the solved form, in the next section. As in the previous case, the size of the output formula is simply exponential in the size of the input formula.

The Solved Form The three cases from the previous section can be successively applied to eliminate all quantified variables $Q_1 x_1, \ldots Q_n x_n$ from (2). For any formula of type (2), the result of this transformation belongs to the following *solved form*:

$$\bigvee_{i=1}^{N} \bigwedge_{j=1}^{M_i} a_{ij} z | f_{ij}(z) \wedge \bigwedge_{j=1}^{P_i} b_{ij} z \not| g_{ij}(z) \wedge \psi_i(z) \tag{6}$$

where a_{ij} and b_{ij} are positive integers, f_{ij} and g_{ij} are linear combinations of terms of the form $\frac{z}{(z,k)}$ with $k \in \mathbb{N} \setminus \{0\}$[5] and ψ_i are Presburger formulas in z.

We will consider the expressions $az | f(z)$, where a is one of a_{ij}, b_{ij} and f is one of f_{ij}, g_{ij}. Let $f(z) = \Sigma_{i=1}^{n} \frac{zc_i}{(z,k_i)} + c_0$. We write $az | f(z)$, equivalently as: $\bigvee_{(d_1, \ldots, d_n) \in \text{div}(k_1) \times \ldots \times \text{div}(k_n)} \bigwedge_{i=1}^{n} (z, k_i) = d_i \wedge aDz | z \Sigma_{i=1}^{n} c_i D_i + c_0 D$, where $D = \Pi_{i=1}^{n} d_i$, $D_i = \frac{D}{d_i}$ and $\text{div}(k)$ denotes the set of divisors of k. Notice that the last conjunct of each clause implies that $z | c_0 D$, i.e., $z \in \text{div}(c_0 D)$. The entire formula is equivalent to: $\bigvee_{(d, d_1, \ldots, d_n) \in \text{div}(c_0 D) \times \text{div}(k_1) \times \ldots \times \text{div}(k_n)} \bigwedge_{i=1}^{n} (d, k_i) = d_i \wedge aDd | d \Sigma_{i=1}^{n} c_i D_i + c_0 D$. Each divisibility proposition of the solved form can thus be evaluated. The solved form is then either trivially false or equivalent to a disjunction of the form $\psi_{i_1} \vee \ldots \vee \psi_{i_n}$, for some $1 \leq i_1, \ldots, i_n \leq N$. The latter is obviously a Presburger formula.

[5] Notice that we can also write z as $\frac{z}{(z,1)}$.

Block Elimination of Universal Quantifiers

This section presents results that are used in a generalization of the universal positive and universal mixed cases, to perform the elimination of an entire *block* of successive universal quantifiers with simple exponential complexity. A set of vectors $(x_1, \ldots, x_n) \in \mathbb{Z}^n$ satisfying the linear congruence $a_1x_1 + \ldots + a_nx_n + b \equiv 0 \mod m$ is called a n-dimensional arithmetic progression. The block quantifier elimination problem is equivalent to the coverage of an n-dimensional arithmetic progression by a finite union of n-dimensional progressions. The latter can be solved in simple exponential time, as shown by the following consequence of Theorem 1:

Corollary 2 *Let $a_{ij} \in \mathbb{Z}, b_i \in \mathbb{Z}, m_i \in \mathbb{N}$, $1 \leq i \leq k$, $1 \leq j \leq n$. The set of progressions $\{\Sigma_{j=1}^n a_{ij}x_j + b_i \equiv 0 \mod m_i\}_{i=1}^k$ covers $\mathbb{Z}^n$ if and only if it covers the set $\{1 \ldots 2^k\}^n$.*

Proof: Suppose that $\{\Sigma_{j=1}^n a_{ij}x_j + b_i \equiv 0 \mod m_i\}_{i=1}^k$ does not cover $\mathbb{Z}^n$ i.e., there exists a point $(x_1, \ldots, x_n)$ that is not covered. Then for each $1 \leq j \leq n$, x_j satisfies none of congruences $a_{ij}x_j + \Sigma_{1 \leq l \leq n}^{l \neq j} a_{il}x_l + b_i \equiv 0 \mod m_i$, $1 \leq i \leq k$. By Theorem 1, there exists also a number $x'_j \in \{1 \ldots 2^k\}$ for which this is also the case. Then $(x'_1, \ldots, x'_n) \in \{1 \ldots 2^k\}^n$, where each x'_j is found as in the previous, does not satisfy any of the initial progressions. □

This takes care of the universal positive case. In the universal mixed case we need to effectively compute the period of the intersection of any given number of n-dimensional progressions. Let $\mathcal{L}\mathbb{Z}[z]$ denote the monoid of first degree polynomials in z, with integer coefficients. Since our problem is parameterized by z, we consider a system of progressions of the form $\bigwedge_{i=1}^k \Sigma_{j=1}^n a_{ij}x_j \equiv 0 \mod z$, with solutions from $\mathcal{L}\mathbb{Z}[z]$. We need to show that this set is a finitely generated monoid, and moreover, that its base is effectively computable. The following theorem gives the result:

Theorem 2 *Let $a_i \in \mathbb{Z}$, $1 \leq i \leq n$, $n > 1$.*

1. *The set of integer solutions to the equation $\Sigma_{i=1}^n a_ix_i = 0$ is a finitely generated submonoid M of $(\mathbb{Z}^n, +)$. It is moreover possible to construct a base of M of size $n - 1$.*

2. *The set of integer coefficient solutions to the congruence $\Sigma_{i=1}^n a_ix_i \equiv 0 \mod z$ is a finitely generated submonoid $M[z]$ of $(\mathcal{L}\mathbb{Z}^n[z], +)$. It is moreover possible to construct a base of $M[z]$ of the form $\{v_1, \ldots, v_{n-1}, zv_1, \ldots, zv_{n-1},$
$zv_n\}$, with $v_1, \ldots, v_n \in \mathbb{Z}^n$.*

Proof: 1. By induction on n. In the base case $n = 2$, the solution is generated by $\left(\frac{-a_2}{(a_1,a_2)}, \frac{a_1}{(a_1,a_2)}\right)$. Indeed, since $a_1x_1 = -a_2x_2$, we have $[a_1, a_2] | a_1x_1$, which is equivalent to $\frac{a_2}{(a_1,a_2)} | x_1$ and similarly, $\frac{a_1}{(a_1,a_2)} | x_2$ i.e., $x_1 = k\frac{a_2}{(a_1,a_2)}$, $x_2 = l\frac{a_1}{(a_1,a_2)}$). But since (x_1, x_2) is a solution, $k = -l$. For the induction step, let $a_1x_1 + \ldots + a_{n-1}x_{n-1} = -a_nx_n$. We distinguish two cases. First, if $x_n = 0$, let $\{v_1, \ldots, v_{n-2}\}$ be the base of the set of solutions for $a_1x_1 + \ldots + a_{n-1}x_{n-1} = 0$. By induction hypothesis, this set is effectively computable. For the case $x_n \neq 0$, let $v =$

$\left(\frac{-a_n u_1}{(a_1,\ldots,a_n)},\ldots,\frac{-a_n u_{n-1}}{(a_1,\ldots,a_n)},\frac{(a_1,\ldots,a_{n-1})}{(a_1,\ldots,a_n)}\right)$, where $u_1,\ldots,u_{n-1}\in\mathbb{Z}$ are numbers satisfying $\Sigma_{i=1}^{n-1}\frac{a_i u_i}{(a_1,\ldots,a_{n-1})} = 1$. Such numbers exists and can be effectively computed, by Bézout Lemma, since $\frac{a_i}{(a_1,\ldots,a_{n-1})}$, $1\le i\le n-1$ are altogether relatively prime. We claim that the vectors $v_1 0,\ldots,v_{n-2}0, v\in\mathbb{Z}^n$ form a base for the set of all solutions. First, notice that v is linearly independent on $v_1 0$, …, $v_{n-2}0$. Second, the fact that any linear combination of these vectors is a solution to the equation is an easy, mechanic check. Third, letting $(x_1,\ldots,x_n)$ be a solution of the above equation, we have that $\left(\frac{-a_n u_1 x_n}{(a_1,\ldots,a_n)},\ldots,\frac{-a_n u_{n-1} x_n}{(a_1,\ldots,a_n)},\frac{(a_1,\ldots,a_{n-1})x_n}{(a_1,\ldots,a_n)}\right)$ is also a solution, hence the vector:

$$\left(x_1+\frac{a_n u_1 x_n}{(a_1,\ldots,a_{n-1})},\ldots,x_{n-1}+\frac{a_n u_{n-1} x_n}{(a_1,\ldots,a_{n-1})}\right)\in\mathbb{Z}^{n-1}$$

is a solution to $\Sigma_{i=1}^{n-1}a_i x_i = 0$, and by the induction hypothesis, a linear combination of $v_1,\ldots,v_{n-2}$. Since $(a_1,\ldots,a_{n-1})|a_n x_n$, we have $\big[(a_1,\ldots,a_{n-1}),a_n\big]|a_n x_n$ i.e., $\frac{(a_1,\ldots,a_{n-1})}{(a_1,\ldots,a_{n-1},a_n)}|x_n$. By putting $x_n = \frac{(a_1,\ldots,a_{n-1})}{(a_1,\ldots,a_{n-1},a_n)}k$ for some $k\in\mathbb{Z}$, we obtain that $(x_1,\ldots,x_n)$ is a linear combination of $v_1 0,\ldots,v_{n-1}0, v$.

2. By the first point, the set of solutions for the equation $\Sigma_{i=1}^{n}a_i x_i = 0$ is generated by a base $\{v_1,\ldots,v_{n-1}\}$. Let $v_n = (u_1,\ldots,u_n)$ where u_i are Bézout numbers satisfying $\Sigma_{i=1}^{n}\frac{a_i u_i}{(a_1,\ldots,a_n)} = 1$. We claim that the subset $\{v_1,\ldots,v_{n-1}, zv_1,\ldots,zv_{n-1}, zv_n\}$ of $\mathcal{L}\mathbb{Z}^n[z]$ is a base for the set of solutions to the linear congruence $\Sigma_{i=1}^{n}a_i x_i \equiv 0 \mod z$. That all vectors in this set are linear independent is an easy check. So is that every linear combination gives a solution to the congruence. To show completeness, notice that the congruence can be seen as a linear equation in $n+1$ variables $\Sigma_{i=1}^{n}a_i x_i - zy = 0$, where $x_i\in\mathcal{L}\mathbb{Z}[z]$ and $y\in\mathbb{Z}$ are unknowns. Moreover, $x_i = s_i z + t_i$, for some $s_i,t_i\in\mathbb{Z}$, $1\le i\le n$. We have $z\Sigma_{i=1}^{n}(a_i s_i - y)+\Sigma_{i=1}^{n}a_i t_i = 0$, and, since z is a parameter, this is equivalent to $\Sigma_{i=1}^{n}a_i s_i - y = 0$ and $\Sigma_{i=1}^{n}a_i t_i = 0$. Notice that the solutions to the those equations in $\mathbb{Z}^{n+1}$ and $\mathbb{Z}^n$ are generated by $\{v_1,\ldots,v_{n-1},v_n\}$ and $\{v_1,\ldots,v_{n-1}\}$, respectively. Hence $\vec{x} = z\big(\Sigma_{i=1}^{n-1}\alpha_i v_i + \alpha_n v_n\big)+\Sigma_{i=1}^{n-1}\beta_i v_i = \Sigma_{i=1}^{n-1}\alpha_i z v_i + \alpha_n z v_n + \Sigma_{i=1}^{n-1}\beta_i v_i$. □

Theorem 2 gives us the means to characterize the solution of a system of n-dimensional progressions, parameterized by z. This is done inductively. Suppose that we have already computed a base $\{v_1,\ldots,v_{n-1},zv_1,\ldots,zv_{n-1},zv_n\}$ for the system $\bigwedge_{i=1}^{k-1}\Sigma_{j=1}^{n}a_{ij}x_j\equiv 0 \mod z$, according to the second point of Theorem 2. We are now looking after a base generating the solutions to $\bigwedge_{i=1}^{k}\Sigma_{j=1}^{n}a_{ij}x_j\equiv 0 \mod z$. The solutions to the system are of the form $\vec{x} = \Sigma_{j=1}^{n-1}\alpha_j v_j + z\Sigma_{j=1}^{n}\beta_j v_j$ with $\alpha_j,\beta_j\in\mathbb{Z}$. Introducing those values into $\Sigma_{i=1}^{n}a_{ki}x_i\equiv 0 \mod z$, we obtain that $\Sigma_{i=1}^{n}a_{ki}\big(\Sigma_{j=1}^{n-1}\alpha_j v_j^{(i)} + z\Sigma_{j=1}^{n}\beta_j v_j^{(i)}\big)\equiv 0 \mod z$ must be the case, where $v^{(i)}$ denotes the i-th component of a vector v. This is furthermore equivalent to $\Sigma_{i=1}^{n}a_{ki}\Sigma_{j=1}^{n-1}\alpha_j v_j^{(i)}\equiv 0 \mod z$, or to the system with unknowns α_j: $\Sigma_{j=1}^{n-1}\big(\Sigma_{i=1}^{n}a_{ki}v_j^{(i)}\big)\alpha_j\equiv 0 \mod z$. According to Theorem 2, the solutions of the latter system are generated by a base $\{u_1,\ldots,u_{n-2},zu_1,\ldots,zu_{n-1}\}$. Thus the solutions of the original system $\bigwedge_{i=1}^{k}\Sigma_{j=1}^{n}a_{ij}x_j\equiv 0 \mod z$ are of the form $\vec{x} = \Sigma_{l=1}^{n-2}\gamma_l\Sigma_{j=1}^{n-1}u_l^{(j)}v_j + z\Sigma_{l=1}^{n-1}\delta_l\Sigma_{j=1}^{n}u_l^{(j)}v_j$, with $\gamma_l,\delta_l\in\mathbb{Z}$. The block quantifier elimination can be now performed along the same lines of the universal mixed case, discussed in the previous.

Extending to the entire $\mathcal{L}_{|}^{(1)}$

Let us now revisit the quantifier elimination procedure for the general case, where the divisibility propositions are of the form $f(z)|g(\vec{x}, z)$, with f, g linear functions. The only two differences w.r.t. the case $f(z) = z$ are encountered when applying the existential positive and the universal mixed cases.

In the existential positive case, subsequent to the application of the CRT, we need to simplify formulas of the following two forms, where $a_i \in \mathbb{N}$ and $f_i(z), f_j(z), h_{ij}(\vec{x}, z), h_i(\vec{x}, z)$ are arbitrary linear functions:

1. $(f_i, f_j)|h_{ij}$. We distinguish two cases:
   - if either f_i divides f_j or f_j divides f_i in terms of polynomial division, then $(f_i, f_j) = f_i$ or $(f_i, f_j) = f_j$, respectively. Let us consider the first situation, the other one being symmetric. We obtain, equivalently, $f_i|r$, where r is the constant polynomial representing the remainder of h_{ij} divided by f_i. This can be expressed as a finite disjunction in Presburger arithmetic.
   - otherwise, (f_i, f_j) can be written equivalently as (g_{ij}, k) where g_{ij} is a linear function in z and $k \in \mathbb{Z}$, by applying Euclid's g.c.d. algorithm in the polynomial ring $\mathbb{Z}[z]$. We have reduced the problem to case 2.
2. $(f_i, a_i)|h_i$ is equivalent to $\bigvee_{0 \leq r < a_i} f_i \equiv r \mod a_i \wedge (r, a_i)|h_i$.

In the universal mixed case, subsequent to the application of Erdös Conjecture, we obtain subterms of the form $\pi = \left[\left\{\frac{h_j}{(h_j,a_j)}\right\}_{j=1}^{R}\right]$ occurring within atomic propositions of the form $h_i|a_i\pi + g_i$. where $h_i(z), h_j(z)$ and $g_i(\vec{x}, z)$ are linear functions. The first step is to substitute (h_j, a_j) for constants i.e. $\pi = \left[\left\{\frac{h_j}{d_j}\right\}_{j=1}^{R}\right]$, for some $d_j \in \text{div}(a_j)$. The equivalent form is now $\pi = \frac{\left[\{D_j h_j\}_{j=1}^{R}\right]}{D} = \frac{\Pi_{j=1}^{R} D_j h_j}{D\left(\{D_j h_j\}_{j=1}^{R}\right)}$, where $D = \Pi_{j=1}^{R} d_j$ and $D_j = \frac{D}{d_j}$. Now the denominator expression is the g.c.d. of a number of linear functions in z, and can be reduced either to a linear function or to a constant, chosen from a set of divisors, like in the existential positive case above. Hence π is a polynomial from $\mathbb{Q}[z]$, of degree at most R. Every atomic proposition involving π can be put in the form $h(z)|p(z)$, where $h, p \in \mathbb{Z}[z]$ (just multiply both sides with the l.c.m of all denominators in π). We consider the following two cases:

- if z occurs in h with a non-zero coefficient, let r be the remainder of p divided by h, the degree of r being zero. Hence $h(z)|r$, which is written as a finite disjunction in Presburger arithmetic.
- otherwise, h is a constant $c \in \mathbb{Z}$. We have $p(z) \equiv 0 \mod c$, which is further equivalent to $\bigvee_{r \in \{0,\ldots,|c|-1\}} z \equiv r \mod c \wedge p(r) \equiv 0 \mod c$

Example It is time to illustrate our method by means of an example. Let us find all positive integers z that satisfy the formula $\forall x \forall y \; z|12x+4y \to z|3x+12y$. To eliminate y we apply the universal mixed case and obtain:

$$\forall x \left[\neg \exists y \; z|12x+4y \vee \exists y \; z|12x+4y \wedge z|3x+12y \wedge z|3x+12(y+\frac{z}{(z,4)})\right]$$

By an application of the CRT, $\exists y \; z|12x+4y$ is equivalent to $(z,4)|12x$ which is trivially true, since $(z,4)|4$ and $4|12x$. Moreover, if $z|3x+12y$, then $z|3x+12y+12\frac{z}{(z,4)}$ is equivalent to $z|12\frac{z}{(z,4)}$, which is also trivially true. Hence, the formula can be simplified down to: $\forall x \exists y \; z|12x+4y \wedge z|3x+12y$ By an application of the CRT we obtain: $\forall x \; z|33x \wedge (z,4)|12x \wedge (z,12)|3x$ which, after trivial simplifications, is equivalent to $z|33 \wedge (z,12)|3$, leading to $z \in \{1,3,11,33\}$. $\square$

Complexity Assessment The quantifier elimination has non-elementary worst case complexity. Let φ be any formula of $\mathcal{L}_|^{(1)}$. Since the elimination of an existential quantifier in the positive case can be done in time $|\varphi|^2$, and the elimination of any block of n universal quantifiers in time $2^{n|\varphi|}$, the only reason for non-elementary blow-up lies within the alternation of existential and universal quantifiers. Even in the positive case, alternation of quantifiers causes a formula to be translated from disjunctive to conjunctive normal form or viceversa, this fact alone introducing an exponential blow-up. However it is clear that the alternation-free subset of $\mathcal{L}_|^{(1)}$can be dealt with in at most simple exponential time. the whole decision procedure takes at most $2^{m2^{\cdot^{\cdot^{\cdot^{2^{m|\varphi|}}}}}}\Big\}_{2d}$ time, where d is the alternation depth of φ and m the maximum size of an alternation-free quantifier block.

5 Decidability of $\exists \mathcal{L}_|^{(*)+}$

After performing the preliminary substitution of variables x_i that occur together with some z_j in a linear constraint, we reduce a formula of the $\exists \mathcal{L}_|^{(*)}$class to the following form:

$$\exists z_1 \ldots \exists z_n Q_1 x_1 \ldots Q_m x_m \bigvee_{i=1}^{N} \Big(\bigwedge_{j=1}^{M_i} f_{ij}(\vec{z})|g_{ij}(\vec{x},\vec{z}) \wedge \bigwedge_{j=1}^{P_i} f'_{ij}(\vec{z}) \not| g'_{ij}(\vec{x},\vec{z}) \wedge \varphi_i(\vec{z}) \Big)$$

where $f_{ij}, g_{ij}, f'_{ij}, g'_{ij}$ are all linear functions. In this section we reduce an arbitrary *positive* $\exists \mathcal{L}_|^{(*)}$formula to an existentially quantified formula of $\langle \mathbb{N}, +, |, 0, 1 \rangle$. In other words, we suppose that $P_i = 0$, for all $1 \le i \le n$.

We are going to apply essentially the same quantifier elimination method from Section 4 and analyze its outcome in case of multiple variables of type z_i. Let us have a look first at the existential case i.e., $Q_m \equiv \exists$. Application of the CRT to eliminate x_m yields atomic propositions of the form $(f_1, f_2)|g_{12}$, where $g_{12}(\vec{x},\vec{z})$ is a linear function. On the other hand, in the universal case ($Q_m \equiv \forall$) we just substitute x_m by a constant quantified over a finite range $\{1, \ldots, 2^{M_i}\}$ for some $1 \leq i \leq N$. Since negation does not involve divisibility propositions, the universal mixed case does not apply. The solved form is, in this case: $\bigvee_{i=1}^{N} \bigwedge_{j=1}^{M_i} \left(\{f_k(\vec{z})\}_{k=1}^{P_{ij}} \right) | h_{ij}(\vec{z}) \wedge \psi_i(\vec{z})$, where f_k and h_{ij} are linear functions over $\vec{z}$. Since the g.c.d. operator is left-right associative, we can apply CRT and write each divisibility proposition $(f_1, \ldots, f_P)|h$ in the equivalent form: $\exists y_1 \ldots \exists y_{P-1}\ f_1|y_1 - h \wedge \bigwedge_{i=2}^{P-1} f_i|y_i - y_{i-1} \wedge f_P|y_{P-1}$. Since $z_1, \ldots, z_n$ occur existentially quantified, we have obtained that $\exists\mathcal{L}_{|}^{(*)+}$ can be reduced to $\langle \mathbb{N}, +, |, 0, 1 \rangle^{\exists}$, hence it is decidable[6]. The worst-case complexity bound for the quantifier elimination is, as in the case for $\mathcal{L}_{|}^{(1)}$, non-elementary. According to [Lip76], the decision complexity for the underlying theory is bounded by $2^{(N+1)^{8N^3}}$, where N is the maximum between $|\varphi|$ and the maximum absolute value of the coefficients in φ[7].

To show the undecidability of the $\exists\mathcal{L}_{|}^{(*)}$ fragment with negation, we define the existential subset of the $\langle \mathbb{N}, +, [], 0, 1 \rangle$ theory into it. This is done using the classical definition of the l.c.m. relation $[x, y] = z$ [Rob49]: $\forall t\ x|t \wedge y|t \leftrightarrow z|t$. To show undecidability of the latter, we use that, for $x \neq 0$, $x^2 = y \leftrightarrow y + x = [x, x+1]$ to define the perfect square relation[8], and $(x+y)^2 - (x-y)^2 = 4xy$ to define multiplication. The rest is an application of the undecidability of Hilbert's Tenth Problem [Mat70].

6 Application to the Verification of Programs with Lists

The results in this paper are used to solve a decision problem related to the verification of programs that manipulate dynamic memory structures, specified by recursive data types. Examples include lists, trees, and, in general, graphs. We are interested in establishing *shape invariants* such as e.g. absence of cycles and data sharing, but also by *quantitative properties* involving lengths of paths within the heap of a program. For instance, consider a list reversal program that works by keeping two disjoint lists and moving pointers successively from one list to another. A shape invariant of this program is that, given a non-cyclic list as input, the two lists are always disjoint. A quantitative invariant is that the sum of their lengths must equal the length of the input list.

In order to express shape and quantitative properties of the dynamic memory of programs performing selector updating operations, we have defined a specification logic called *alias logic with counters* [BIL04]. Formulas in this logic are interpreted over finite directed graphs with edges labeled with symbols from a finite alphabet Σ. Formally such a graph is a triple $G = \langle N, V, E \rangle$, where N is the set of nodes, $E : N \times \Sigma \to N$ is the *deterministic* edge relation, $V \subseteq N$ is a designated set of nodes called *variables* on which the requirement is that for no $n \in N, \sigma \in \Sigma$: $E(n, \sigma) \in V$. In other words, the graph is *rooted* on V. A *path* in the graph is a finite sequence $\pi = v\sigma_1\sigma_2 \ldots \in V\Sigma^*$. Since the graph is deterministic, every path may lead to at most one node. Let $\widehat{\pi}$ denote this node, if defined. We say that two paths π_1 and π_2 are *aliased*

[6] When interpreting $\exists\mathcal{L}_{|}^{(*)}$ over $\mathbb{Z}$ we assume the $\leq$ relation, since the decidability proof from [Lip76] uses orderings of variables.

[7] Actually this expression is the result of some simplifications, the original expression being rather intricate.

[8] If we interpret over $\mathbb{Z}$, we use $-y - x = [x, x+1]$ for negative x.

if $\widehat{\pi_1}, \widehat{\pi_2}$ are defined and $\widehat{\pi_1} = \widehat{\pi_2}$. A *quantitative path* is a sequence $\pi(\vec{x}) = v\sigma_1^{f_1}\sigma_2^{f_2}\ldots$, where $\vec{x}$ is a finite set of variables, interpreted over $\mathbb{N}$, and $f_1, f_2, \ldots$ are linear functions on $\vec{x}$. Given an interpretation of variables $\iota : \vec{x} \to \mathbb{N}$, the interpretation of a quantitative path π, denoted as $\iota(\pi)$, is the result of evaluating the functions $f_1, f_2, \ldots$ and replacing each occurrence of σ^k by the word $\sigma \ldots \sigma$, repeated k times.

The logic of *aliases with counters* is the first-order additive arithmetic of natural numbers, to which we add alias propositions of the form $\pi_1(\vec{x})\diamond\pi_2(\vec{x})$. Given an interpretation of variables, an alias proposition $\pi_1\diamond\pi_2$ holds in a graph if the interpretations of the quantified paths involved are defined and they "meet" in the same node: $\widehat{\iota(\pi_1)} = \widehat{\iota(\pi_2)}$. The satisfaction of a closed formula φ on a graph G, denoted as $G \models \varphi$, is defined recursively on the syntax of φ, as usual.

For example, to specify that u and v are two program variables pointing towards two disjoint non-cyclic lists chained by the selector field σ, and whose lengths sum up to l, we write the following formula. The notation $\delta(\pi)$ stands for $\pi\diamond\pi$, meaning that the node $\widehat{\pi}$ is defined in the graph.

$$\begin{aligned}\exists x \exists y\; x + y = l \wedge \delta(u\sigma^x) \wedge \delta(v\sigma^y) \wedge \forall z \forall t\; z > x \to \neg\delta(u\sigma^z) \wedge z > y \to \neg\delta(v\sigma^z) \wedge \\ z \leq x \wedge t \leq y \to \neg u\sigma^z \diamond v\sigma^t\end{aligned}$$

We have studied the satisfiability problem for this logic and found that it is undecidable on unrestricted graph and dag models, and decidable on tree models. For details, the interested reader is pointed to [BIL04]. The problem in case of simply linked lists is surprisingly more difficult than for trees, due to the presence of loops. However, we can show decidability now, with the aid of the positive fragment of the theory $\exists\mathcal{L}_{|}^{(*)}$.

Since all memory structures considered are lists, we can assume that they are implemented using only one selector field. In other words, the label alphabet can be assumed to be a singleton $\Sigma = \{\sigma\}$. Hence we can write each quantitative path in the normal form $v\sigma^f$, with f a linear function over $\vec{x}$. Consequently, from now on we will only consider alias propositions of the form $u\sigma^f \diamond v\sigma^g$.

To decide whether a closed formula φ in alias logic with counters has a model, we use a notion of *parametric graph* $G(\vec{z})$ over a set of variables $\vec{z}$, which is an abstraction of an infinite class of graphs. A formal definition of a parametric graph is given in the next section. The important point is that, in the case of lists with one selector, the total number of parametric graphs is finite. In fact, this number depends only on the number of program variables. Hence, the satisfiability problem is reduced to deciding whether there exists $z_1, \ldots, z_n$ such that $G(\vec{z}) \models \varphi$. To solve the latter problem, we shall derive an open formula $\Psi_{G,\varphi}(\vec{z})$ in the language of $\mathcal{L}_{|}^{(*)}$, such that, for all interpretations $\iota : \vec{z} \to \mathbb{N}$, $\Psi_{G,\varphi}(\iota(\vec{z}))$ holds if and only if $G(\iota(\vec{z})) \models \varphi$. The formula φ is then satisfiable, if and only if there exists a parametric graph G such that $\exists z_1, \ldots \exists z_n \Psi_{G,\varphi}$ is satisfiable. Moreover, as it will be pointed out, $\Psi_{G,\varphi}$ is positive and the only variables occurring on the left of the divisibility are $\vec{z}$. Hence the latter condition is decidable. The following discussion is meant only as a proof of decidability for alias logic with counters in the case $\Sigma = \{\sigma\}$, the algorithmic effectiveness of the decision procedure being left out of the scope of this paper.

A Parametric Model Checking Problem

A parametric graph over a set of variables $\vec{z}$ is a graph $G = \langle N, V, E \rangle$, the only difference w.r.t. the previous definition being the edge alphabet, which is taken to be $\Sigma \times \vec{z}$, instead of Σ. In other words, each edge is of the form $n \xrightarrow{\sigma,z} m$. We assume that each edge is labeled with a different variable from $\vec{z}$, and thus $\|E\| = \|\vec{z}\|$. Given an interpretation of variables $\iota : \vec{z} \rightarrow \mathbb{N}$, we define the interpretation of an edge to be the sequence of edges $n = n_1 \xrightarrow{\sigma} n_2 \xrightarrow{\sigma} \ldots n_k = m$ of length $k = \iota(z)$, with no branching along the way. The interpretation of a graph is the graph obtained by replacing each edge with its interpretation. As a convention, the values of $\vec{z}$ are assumed to be strictly greater than one. The reason is that, allowing zero length paths in the graph might contradict with the requirement that the graph is deterministic. A parametric graph is said to be in *normal form* if and only if:

- there are no two adjacent edges labeled with the same symbol e.g., $m \overset{\sigma,z_1}{\rightarrow} n \overset{\sigma,z_2}{\rightarrow} p$, such that either the indegree or the outdegree of their common node (n) is greater than one.

- each node in the graph is reachable from a root node in V.

Notice that each parametric graph can be put in normal form by replacing any pair of edges violating this condition by a single edge labeled with the same symbol. The interested reader may also consult [BFN04] for a notion very similar to the parametric graph.

In the rest of this section we shall consider the case $\Sigma = \{\sigma\}$. For any given set V of program variables, the number of parametric graphs $\langle N, V, E \rangle$ in normal form, is finite. This fact occurs as consequence of the following lemma:

Lemma 2 *Let $G = \langle N, V, E \rangle$ be a parametric graph over a singleton alphabet, in normal form. Then $\|N\| \leq 2\|V\|$.*

Proof: For a set of nodes $M \subset N$, let $succ(M) = \{n \mid m \rightarrow n\}$ denote the set of immediate successors of M, and, $fr_i(M) = succ^i(M) \setminus succ^{i-1}(M)$, where $succ^i(M)$ denotes the i-th application of the $succ$ function to M, for $i > 1$. By convention, we take $fr_0(M) = M$. Since each node is reachable from V, we have $N \subseteq \bigcup_{i \geq 0} succ^i(V) = \bigcup_{i \geq 0} fr_i(V)$, therefore $\|N\| \leq \Sigma_{i \geq 0} \|fr_i(V)\|$. Let $fr_k^{\geq 1}(M)$, $fr_k^{=1}(M)$ be the sets of nodes from $fr_k(M)$ with two or more predecessors, and with one predecessor respectively. Obviously, $\|fr_k(M)\| = \|fr_k^{\geq 1}(M)\| + \|fr_k^{=1}(M)\|$. By the first condition from the definition of a normal form, each node from $fr_k^{=1}(V)$ has no successors for all $k \geq 0$, so we have $\|fr_k^{\geq 1}(V)\| \leq \frac{\|fr_{k-1}^{\geq 1}(V)\| - \|fr_k^{=1}(V)\|}{2}$ for $k > 1$, and $\|fr_1^{\geq 1}(V)\| \leq \frac{\|fr_0(V)\| - \|fr_1^{=1}(N)\|}{2}$. Summing up, we obtain:

$$\Sigma_{i \geq 1} \|fr_i^{\geq 1}(V)\| \leq \frac{\|fr_0(V)\|}{2} + \Sigma_{i \geq 1} \frac{\|fr_i^{\geq 1}(V)\|}{2} - \Sigma_{i \geq 1} \frac{\|fr_i^{=1}(V)\|}{2}$$
$$\Sigma_{i \geq 1} \frac{\|fr_i^{\geq 1}(V)\|}{2} + \Sigma_{i \geq 1} \frac{\|fr_i^{=1}(V)\|}{2} \leq \frac{\|fr_0(V)\|}{2}$$
$$\Sigma_{i \geq 0} \|fr_i(V)\| \leq 2\|fr_0(V)\|$$
$$\|N\| \leq 2\|V\|$$

$$G \models \pi_1 \Diamond \pi_2 \quad : \quad \bigvee_{n \in N} \widehat{\pi_1} = n \wedge \widehat{\pi_2} = n \vee \exists y \bigvee_{n \xrightarrow{z} m} \widehat{\pi_1} = d(n,y) \wedge \widehat{\pi_2} = d(n,y) \wedge y < z$$

$$G \not\models \pi_1 \Diamond \pi_2 \quad : \quad \exists y_1 \exists y_2 \bigvee_{\substack{n_1 \xrightarrow{z_1} m_1 \\ n_2 \xrightarrow{z_2} m_2 \\ n_1 \neq n_2}} \widehat{\pi_1} = d(n_1,y_1) \wedge \widehat{\pi_2} = d(n_2,y_2) \wedge y_1 < z_1 \wedge y_2 < z_2$$

$$\vee \bigvee_{n \xrightarrow{z} m} \widehat{\pi_1} = d(n,y_1) \wedge \widehat{\pi_2} = d(n,y_2) \wedge y_1 < z \wedge y_2 < z \wedge y_1 \neq y_2$$

Figure 2:

$\square$

Given a parametric graph and a closed formula in alias logic, we are interested in finding an open formula $\Psi_{G,\varphi}(\vec{z})$ that encodes $G(\vec{z}) \models \varphi$, for all possible interpretations of $\vec{z}$. We will define $\Psi_{G,\varphi}$ inductively on the structure of φ, by first defining characteristic formulas for the alias literals (alias propositions and negations of alias propositions). Intuitively, $\pi_1 \Diamond \pi_2$ holds on $G(\vec{z}) = \langle N, V, s \rangle$ if and only if the paths π_1 and π_2 meet either in an "explicit" node $n \in N$ or in a node that does not occur in N but is "abstracted" within a parametric edge. For the latter case, we need some notation. Given an interpretation ι of variables $\vec{z} \cup \{y\}$, let $d(n,y)$ denote the node situated at distance $\iota(y)$ from n in the (non-parametric) graph $G(\iota(\vec{z}))$. With this notation, Figure 2 defines the characteristic formulas $\Psi_{G,l}$, for alias literals l.

Since both positive and negative literals can be encoded as positive boolean combinations of equalities of the form $\widehat{\pi} = d(n,y)$[9], it is sufficient to show how such an equality can be defined as a positive formula of $\mathcal{L}_{|}^{(*)}$ with the only variables occurring on the left of divisibility being the ones in $\vec{z}$. Let $\pi = v\sigma^{f(\vec{x})}$ be a quantitative path. There are three possibilities:

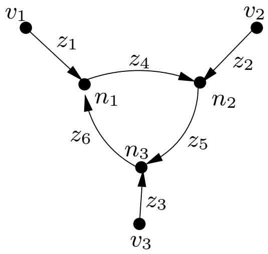
1. if there is no path in G from v to n, then $\widehat{\pi} = d(n,y)$ is false.

2. if there is an acyclic path $v \xrightarrow{z_1} n_1 \xrightarrow{z_2} \ldots n_{k-1} \xrightarrow{z_k} n$ in G, then $\widehat{\pi} = d(n,y)$ is equivalent to $f(\vec{x}) = \Sigma_{i=1}^{k} z_i + y$.

3. otherwise, there is a cyclic path $v \xrightarrow{z_1} \ldots n_{k-1} \xrightarrow{z_k} n_k = n \xrightarrow{z_{k+1}} n_{k+1} \ldots n_{l-1} \xrightarrow{z_l} n_l = n$ in G, and for all $1 \leq i < l$, $i \neq k$ we have $n_i \neq n$. Then $\widehat{\pi} = d(n,y)$ is equivalent to $f(\vec{x}) \geq \Sigma_{i=1}^{k} z_i + y \wedge \Sigma_{i=k+1}^{l} z_i | f(\vec{x}) - \Sigma_{i=1}^{k} z_i - y$, for the $v \xrightarrow{f}$ path may iterate through the $n_k, n_{k+1}, \ldots, n_l$ loop multiple times.

Example The encoding of a query of the form $G(\vec{z}) \models \widehat{\pi(\vec{x})} = n$ as a formula of $\mathcal{L}_{|}^{(*)}$ is better understood by means of an example. Figure 3 shows a parametric graph and three sample queries

[9] $\widehat{\pi} = n$ is $\widehat{\pi} = d(n, 0)$.



$$\widehat{v_1\sigma^x} = n_1 : x \geq z_1 \wedge z_4 + z_5 + z_6 | x - z_1$$
$$\widehat{v_1\sigma^x} = n_2 : x \geq z_1 + z_4 \wedge z_4 + z_5 + z_6 | x - z_1 - z_4$$
$$\widehat{v_1\sigma^x} = n_3 : x \geq z_1 + z_4 + z_5 \wedge z_4 + z_5 + z_6 | x - z_1 - z_4 - z_5$$

Figure 3:

with their equivalent encodings. □

Theorem 3 *If* $\|\Sigma\| = 1$*, then the satisfiability problem for the logic of* aliases with counters *is decidable.*

Proof: Let φ be a formula in which all alias propositions are of the form $v_1\sigma^{f_1} \diamond v_2\sigma^{f_2}$, $\Sigma = \{\sigma\}$ and let V be the set of all v_i occurring in (a quantitative path of) φ. Using the definitions from Figure 2, we reduce the satisfiability of φ to a positive boolean combination of atomic propositions of the form $\widehat{v\sigma^f} = n$. Hence φ has a model if and only if it has a model $\langle N, V, E\rangle$, with the set of roots V, as above. This is true if and only if φ is true over a parametric model with the set of roots V. By Lemma 2, the number of such parametric models is finite, and the parametric model checking problem can be defined in $\exists\mathcal{L}_{|}^{(*)+}$, hence it is decidable. The conclusion follows. □

7 Conclusion

We studied the decision problem for fragments of the arithmetic of addition and divisibility. It is known that the entire theory is undecidable [Rob49], while its existential subset is decidable [Lip76]. In defining our fragment we take in consideration on which side of the divisibility sign | do variables occur. Our main result is the decidability of the fragment of the form $QzQ_1x_1 \ldots Q_nx_n\varphi$ where the only divisibility propositions are of the form $f(z)|g(\vec{x}, z)$. For this fragment we show the existence of a quantifier elimination procedure. We apply the same procedure to formulas of the form $\exists z_1, \ldots, \exists z_n Q_1x_1, \ldots, Q_mx_m\varphi$ where the only divisibility propositions are of the form $f(\vec{z})|g(\vec{x}, \vec{z})$. Here we show decidability of the positive form i.e., in which no divisibility propositions occur negated. Moreover, the full fragment of this form is shown to be undecidable. We have applied the decidability results to a problem concerning the verification of programs with mutable data structures. Having introduced a specification logic for expressing shape and quantitative properties of recursive data structures, we show that this logic is decidable on list models, by reduction to first-order formulas using addition and divisibility.

Further directions of work concern, on one hand, algorithmic aspects of the decision problem, and namely, efficient implementations of the method. On the other hand, we are investigating the possibility of applying this theory to the problem of computing loop invariants of integer counter automata. This problem has been explored using Presburger arithmetic [CJ98], and extending the results by means of theories with divisibility seems to be a promising approach.

Acknowledgments: The authors are greatly indebted to their colleagues Yassine Lakhnech, Laurent Mazaré and Romain Janvier for the interesting discussions and enlightening suggestions concerning this paper.

References

[B02́] Alexis Bés. A survey of arithmetical definability. *A Tribute to Maurice Boffa. Bulletin de la Société Mathématique de Belgique*, 1 - 54, 2002. 1

[Bel76] A. P. Beltyukov. Decidability of the universal theory of natural numbers with addition and divisibility. *Zapiski Nauch. Sem. Leningrad Otdeleniya Mathematical Institute*, 60:15 – 28, 1976. 1

[BFN04] S. Bardin, A. Finkel, and D. Nowak. Toward symbolic verification of programs handling pointers. In *Proc. 3rd Int. Workshop on Automated Verification of Infinite-State Systems (AVIS 2004), Barcelona, Spain*. Electronic Notes in Theoretical Computer Science, 2004. 6

[BIL04] Marius Bozga, Radu Iosif, and Yassine Lakhnech. Counting aliases. Technical Report 17, Verimag, October 2004. 1, 6

[CE69] R. B. Crittenden and C. L. Vanden Eynden. A proof of a conjecture of Erdös. *Bulletin of American Mathematical Society*, (75):1326 – 1329, 1969. 2, 1

[Chu36] Alonzo Church. An unsolvable problem of elementary number theory. *American Journal of Mathematics*, 58:345 – 363, 1936. 1

[CJ98] Hubert Comon and Yan Jurski. Multiple Counters Automata, Safety Analysis and Presburger Arithmetic. In *Proceedings of the 10th International Conference on Computer Aided Verification*, volume 1427, pages 268 – 279. Lecture Notes in Computer Science, 1998. 7

[DPS99] C. Ding, D. Pei, and A. Salomaa. *Chinese Remainder Theorem: Applications in Computing, Coding, Cryptography*. World Scientific Publishing Company, 1999. 2

[FR74] M. J. Fischer and M. O. Rabin. Super-exponential complexity of Presburger arithmetic. *Complexity of Computation (AMS-SIAM Proceedings)*, 7(41), 1974. 3

[G3̈1] Kurt Gödel. Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I. *Monatshefte für Mathematik und Physik*, 38:173 – 198, 1931. 1

[Lip76] Leonard Lipshitz. The diophantine problem for addition and divisibility. *Transaction of the American Mathematical Society*, 235:271 – 283, January 1976. (document), 1, 3, 1, 3, 5, 6, 7

[Mat70] Yuri Matiyasevich. Enumerable sets are diophantine. *Journal of Sovietic Mathematics*, (11):354 – 358, 1970. 1, 5

[Pre29] Mojzesz Presburger. Über die Vollstandigkeit eines gewissen Systems der Arithmetik. *Comptes rendus du I Congrés des Pays Slaves*, Warsaw 1929. (document), 1, 3, 3, 4

[Rob49] Julia Robinson. Definability and decision problems in arithmetic. *The Journal of Symbolic Logic*, 14(2):98 – 114, June 1949. (document), 1, 5, 7

[Ros36] B. Rosser. Extensions of some theorems of Gödel and Church. *The Journal of Symbolic Logic*, 1:87 – 91, 1936. 1

[Woo81] A. Woods. Some problems in logic and number theory and their connections. Technical report, Phd Thesis, University of Manchester, 1981. 3

A Auxiliary Lemmas

Corollary 3 *Let $a_1, \dots, a_n \in \mathbb{Z}$ and $b_1, \dots, b_n \in \mathbb{N} \setminus \{0\}$. Then a set of progressions $\{a_i + b_i\mathbb{N}\}_{i=1}^n$ covers $\mathbb{N}$ if and only if it covers the set $\{1, \dots, 2^n\}$.*

Proof: We can assume w.l.o.g. that $a_i \le 2^n$ for all $1 \le i \le n$. Clearly if some $a_j > 2^n$ we have that $\{a_i + b_i\mathbb{N}\}_{1\le i\le n}^{i\neq j}$ covers $\{1, \dots, 2^n\}$, and we prove the result for the latter. Since $a_i + b_i\mathbb{N} \subseteq a_i + b_i\mathbb{Z}$, we have that $\{a_i + b_i\mathbb{Z}\}_{i=1}^n$ covers $\{1, \dots, 2^n\}$, and, by Theorem 1, it also covers $\mathbb{Z}$. Take $x > 2^n$. We will show that $x = a_j + b_jk$ for some $1 \le j \le n$ and $k > 0$. Since x is covered by some $a_j + b_j\mathbb{Z}$, we have that $x = a_j + b_jk$ for some $k \in \mathbb{Z}$. Since $a_j \le 2^n$ we have:

$$b_jk + 2^n \ge a_j + b_jk > 2^n$$

Since $b_j > 0$, we obtain $k > 0$. $\square$

For positive integers x and y, let (x, y) denote their greatest common divisor and $[x, y]$ their least common multiple.

Lemma 3 *Let z, a, b be positive integers. The following equalities hold:*

1. $((z, a), (z, b)) = (z, (a, b))$
2. $((z, a), b) = (z, (a, b))$
3. $\left[\frac{z}{(z,a)}, \frac{z}{(z,b)}\right] = \frac{z}{(z,(a,b))}$

4. $\left[\frac{z}{(z,a)}, b\right] = \frac{zb}{(z,ab)}$

Proof: Let p be any prime number and let p_z, p_a, p_b denote the powers under which p appears as a prime divisor of z, a, b, respectively. Then the above equalities, relative to p, are equivalent to:

1. $\min(\min(p_z, p_a), \min(p_z, p_a)) = \min(p_z, \min(p_a, p_b))$
2. $\min(\min(p_z, p_a), p_b) = \min(p_z, \min(p_a, p_b))$
3. $\max(p_z - \min(p_z, p_a), p_z - \min(p_z, p_b)) = p_z - \min(p_z, \min(p_a, p_b))$
4. $\max(p_z - \min(p_z, p_a), p_b) = p_z + p_b - \min(p_z, p_a + p_b)$

All these equalities are easy checks. $\square$