Complete fragments of arithmetic

Anders Moen Hagalisletto

May 25, 2004

Abstract

In the famous paper of Kurt Gödel he proved that number theory, containing axioms for addition and multiplication is incomplete. But what about simpler theories? Are they complete? The answer is yes. The theories of addition and multiplication are both complete, but the argument that they are decidable is far from trivial. In the following essay we shall present the weak fragments of number theory and outline the proofs why they provide an algorithm answering yes or no on questions about truth.

1 Introduction

The most cited and well-known result in mathematical logic is due to Kurt Gödel [G$\ddot{3}$1], and is called *first incompleteness theorem*. The theorem states that any theory that contains addition and multiplication is incomplete, that is there are true sentences that are not provable in the theory.

An interesting question is where the borderline between completeness and incompleteness lies. If full arithmetic is incomplete, then what about fragments of arithmetic? They should be complete if we strip off enough expressive power. But the completeness results do not come for free, technically speaking. The results due to Presburger and Skolem [Sko70], concerning respectively completeness of addition and multiplication, makes extensive use of quantifier elimination and number theory.

The essay is organized as follows. First, we present the theorem of quantifier elimination, that says that any theory permitting elimination of existential quantifiers over conjunctions of atomic formulas, permits elimination of quantifiers in general. Secondly, we go deeper into the proofs of Presburger and Skolem, and give the proof of the decidability of the addition-fragment of arithmetic. Finally, we shall consider negative aspects, what can not be defined and why this is so. Since expressibility of a language is the key to understand the decidability, we shall spend some time explaining it using the Ginsburg Spanier Theorem. Having

this result and its close relatives, in the tool-box, one is able to reason precisely about non-definability.

2 General Quantifier elimination

Both the proof by Presburger and Skolem rely on the possibility to eliminate quantifiers. Quantifier elimination is a standard technique, and we base our presentation on [Men97], [Sho67], [Smo91]:

Lemma 1 $\mathrm{Th} \vdash \exists x \bigvee_{i=1}^{k} \bigwedge_{j=1}^{m} \varphi_i^j(x) \leftrightarrow \bigvee_{i=1}^{k} \exists x \bigwedge_{j=1}^{m} \varphi_i^j(x)$

Proof: Induction on k. Induction basis is trivial. Consider induction step:
$\mathrm{Th} \vdash \exists x \bigvee_{i=1}^{k+1} \bigwedge_{j=1}^{m} \varphi_i^j(x) \leftrightarrow_{\mathrm{def}} \exists x(\bigvee_{i=1}^{k} \bigwedge_{j=1}^{m} \varphi_i^j(x) \vee \bigwedge_{j=1}^{m} \varphi_{k+1}^j(x)) \leftrightarrow_{\mathrm{FOL}}$
$\exists x(\bigvee_{i=1}^{k} \bigwedge_{j=1}^{m} \varphi_i^j(x)) \vee \exists x(\bigwedge_{j=1}^{m} \varphi_{k+1}^j(x)) \leftrightarrow_{\mathrm{I.H.}}$
$\bigvee_{i=1}^{k} \exists x(\bigwedge_{j=1}^{m} \varphi_i^j(x)) \vee \bigvee_{i=k+1}^{k+1} \exists x(\bigwedge_{j=1}^{m} \varphi_i^j(x)) \leftrightarrow_{\mathrm{def}} \bigvee_{i=1}^{k+1} \exists x \bigwedge_{j=1}^{m} \varphi_i^j(x)$ $\square$

Lemma 2 *If every formula on the form $\exists x \bigwedge_{i=1}^{m} \varphi_i(x)$, where each $\varphi_i(x)$ is a literal is equivalent to a quantifier free formula Ψ, i.e.*
$\mathrm{Th} \vdash \exists x \bigwedge_{i=1}^{m} \varphi_i(x) \leftrightarrow \Psi$*, then* Th *permits quantifier elimination.*

Proof: (Shoenfield/Smorynski) Let $(\exists - \mathrm{red})$ denote the sentence:

> For every set of literals $\{\varphi_i \mid 0 \leq i \leq m\}$ there exists a quantifier free formula Ψ, such that $\mathrm{Th} \vdash \exists x \bigwedge_{i=1}^{m} \varphi_i(x) \leftrightarrow \Psi$.

and let (Conj) denote the sentence

> For every formula ξ over the language $\mathcal{L}$, there exists a quantifier free formula Ψ^* such that $\mathrm{Th} \vdash \xi \leftrightarrow \Psi^*$.

We are going to prove that $\exists - \mathrm{red} \implies \mathrm{Conj}$. The elimination begins with the innermost quantifiers first, and then removes the rest successively. The algorithm starts with the formula ξ and only redesign sub-formulas of ξ.

By induction on $\deg(\xi)$ (where $\deg()$ denotes the syntactic complexity of the formula defined in the obvious way), we prove the implication.

Basis case: If $\deg(\xi) = 0$, then ξ is atomic, and hence quantifier-free. By $\xi = \Psi^*$, the lemma obviously holds, since $\mathrm{Th} \vdash \Psi^* \leftrightarrow \Psi^*$.

Induction step: In case $\deg(\xi) = k + 1$ there are 5 cases to consider.

$\xi = \neg\xi_1$. By induction hypothesis there exists a quantifier-free Ψ_1^*, such that

$\mathrm{Th} \vdash \xi_1 \leftrightarrow \Psi_1^*$. But then by PL $\mathrm{Th} \vdash \neg\xi_1 \leftrightarrow \neg\Psi_1^*$, and $\neg\Psi_1^*$ is of course quantifier-free.

The case for $\wedge$ and $\vee$ is similar. Consider $\xi = \exists x\ \xi_1(x)$. By induction hypothesis $\mathrm{Th} \vdash \xi_1(x) \leftrightarrow \Psi_1^*(x)$. Since $\Psi_1^*(x)$ is quantifier-free, it can be written on disjunctive normal form; $\mathrm{Th} \vdash \Psi_1^*(x) \leftrightarrow \bigvee_{i=1}^k \bigwedge_{j=1}^m \xi_i^j(x)$ were each $\xi_i^j(x)$ is a literal. Then from the fact that $\mathrm{Th} \vdash \xi_1(x) \leftrightarrow \bigvee_{i=1}^k \bigwedge_{j=1}^m \xi_i^j(x)$ gives $\mathrm{Th} \vdash \exists x\ \xi_1(x) \leftrightarrow \exists x\ \bigvee_{i=1}^k \bigwedge_{j=1}^m \xi_i^j(x) \leftrightarrow \bigvee_{i=1}^k \exists x\ \bigwedge_{j=1}^m \xi_i^j(x)$. By $(\exists-\mathrm{red})$ then since the premiss of the lemma gives $\vdash \exists x\ \bigwedge_{j=1}^m \xi_i^j(x) \leftrightarrow \Psi_i^j(x)$ for each i, the result follows. $\square$

3 Elementary number theory

The language of elementary number theory is a finite language in the sense that it contains finitely many constants. The following functions are definable in elementary arithmetic, and shall be used later on:

x is a divisor in y:	$x\|y \leftrightarrow_{\mathrm{def}} \exists z \leq y(y = zx)$
the greatest integer in x/y:	$z = [x/y] \leftrightarrow_{\mathrm{def}} \exists r \leq x(x = zy + (r-1))$
equality modulo n	$x = y \pmod n \leftrightarrow_{\mathrm{def}} \exists z\,(x = y + (\underbrace{z + \ldots + z}_{n}))$.

By the famous result of Gödel we know that the language containing successor s, addition $+$, and multiplication $\times$ are prone to incompleteness. The reason for this is that the expressibility of the language increases. A beautiful result by Ginsburg and Spanier gives a very precise answer to the question of definability within such restricted languages.

The language of addition is then the finite language consisting of the primitives 0, s, $+$, $=$ and $<$. Recall that the greatest integer function $[x/y]$, returns the rounded down-wards integer closest to x/y, hence $[3/4] = 0, [8/3] = 2$. The proof by Skolem uses an extended language, the greatest integer function and constant multipliers. Constant multipliers, written $q \cdot x$ can be viewed as abbreviations for q number of additions, $\underbrace{x + \ldots + x}_{q}$. Whenever only scalar multiplication is present we write $\cdot$, and if general multiplication is part of the signature we write $\times$. So, instead of proving that quantifiers can be eliminated directly for $(\mathbb{N}; <, +, 0, 1)$ directly, Skolem proves the result for $(\mathbb{Z}; <, +, 0, 1)$ by working inside $(\mathbb{Q}; \mathbb{Z}; <, +, \{q\cdot|q \in \mathbb{Q}\}, [/], 0, 1)$. To justify the transfer of reasoning between various different structures we need the concept of realizations:

Definition 1 *Let $\mathcal{A}$ and $\mathcal{B}$ be two structures for a language $\mathscr{L}$, and suppose that $\mathcal{A}$ is a substructure of $\mathcal{B}$, $\mathcal{A} \subseteq \mathcal{B}$. Let $|\mathcal{A}| = A$ and $|\mathcal{B}| = B$ denote the domain of these two structures. Suppose that $|\mathcal{A}|$ is definable in $\mathcal{B}$ by a formula $x \in B$. Then for any formula φ in $\mathscr{L}_A$, its* relativization, *φ^A to the set A, is defined by*

(i) $\varphi^A = \varphi$, *if* $\mathrm{degr}(\varphi) = 0$
(ii) $(\neg\varphi)^A = \neg(\varphi^A)$
(iii) $(\varphi_1 \vee \varphi_2)^A = \varphi_1^A \vee \varphi_2^A$ *and* $(\varphi_1 \wedge \varphi_2)^A = \varphi_1^A \wedge \varphi_2^A$
(iv) $(\exists x\ \varphi(x))^A = \exists x\ (x \in A \wedge \varphi(x)^A)$ *and* $(\forall x\ \varphi(x))^A = \forall x\ (x \in A \rightarrow \varphi^A)$

Then we can prove the relativization theorem [1]

Theorem 1 *For every φ in $\mathscr{L}_A$, $\mathcal{A} \models \varphi$ if and only if $\mathcal{B} \models \varphi^A$.*

Proof: Induction over $\mathrm{degr}(\varphi)$. Ind. basis follows direct from definition 1. Suppose that $\varphi = \exists x\ \varphi(x)$: Then $\mathcal{B} \models (\exists x\ \varphi(x))^A$ iff $\mathcal{B} \models \exists x\ (x \in A \wedge \varphi(x)^A)$ iff there exists $a^{\mathcal{B}} \in |\mathcal{B}|$ such that $\mathcal{B} \models \varphi(a)$ where $a^{\mathcal{B}} \in A^{\mathcal{B}}$ iff
there exists an $a^{\mathcal{A}} \in |\mathcal{A}|$ such that $\mathcal{A} \models \varphi(a)$ where $a^{\mathcal{A}} \in A^{\mathcal{A}}$ by induction hypothesis and the fact that $\mathcal{A} \subseteq \mathcal{B}$ iff there exists an $a^{\mathcal{A}} \in |\mathcal{A}|$ such that $\mathcal{A} \models \varphi(a)$ iff $\mathcal{A} \models \exists x\ \varphi(x)$. $\square$

Theorem 2 *(Skolem)* $\mathrm{Th}_{(\mathrm{Z},<,+,0,1)}$ *permits quantifier elimination, relative to the extended language of constant multipliers $q \cdot ()$ and greatest integer function* $[/]$.

Proof: In the proof we follow Smorynski's exposition of Skolem's argument. From the quantifier elimination lemma we know that, it is sufficient to prove that
$\vdash \exists x\ \bigwedge_{j=1}^{\alpha} \varphi_{\mathrm{L}}^j(x) \leftrightarrow \phi(x)$, where $\phi(x)$ is quantifier free and each $\xi_{\mathrm{L}}^j(x)$ is a literal. The proof is split into three main steps.

I. $\vdash \exists x\ \bigwedge_{i=1}^{\alpha} \varphi_{\mathrm{L}}^i(x) \leftrightarrow \bigvee_{j=1}^{\beta} \exists x\ \bigwedge_{j=1} \varphi_{\mathrm{ATO}}^{ij}(x)$
II. $\vdash \exists x\ \bigwedge_{j=1}^{\alpha} \varphi_{\mathrm{ATO}}^j(x) \leftrightarrow$
$\bigvee_{l=0}^{m-1} \exists w\ (\bigwedge_{i=1}^{\gamma} w < s_i \wedge \bigwedge_{j=1}^{\delta} t_j < w \wedge \bigwedge_{k=1}^{\epsilon} w = u_k)$
III. Elimination of $\exists w$ in $\exists w\ (\bigwedge_{i=1}^{\gamma} w < s_i \wedge \bigwedge_{j=1}^{\delta} t_j < w \wedge \bigwedge_{k=1}^{\epsilon} w = u_k)$

Note that $\varphi_{\mathrm{ATO}}^j(x)$ is atomic. The rational number chosen for m is going to be explained later in the proof.

In step I. the negated atomic sentences are removed in the equivalent sentence, such that only positive atomic formulas occur. In step II. the positive atomic formulas are replaced by formulas where the existential variable occurs alone at one

[1] [Hod97] p. 101-102 or [Smo91] p. 309. For standard definitions of the concepts *signature*, *structure* and *substructure*, see [Hod97] p. 2-6

side of the (in)equalities. Finally, step III. performs the actual elimination of the existential quantifier.

Step I. Each of the $\varphi^j_{\mathrm{L}}(x)$ are either positive or or negative. If $\varphi^j_{\mathrm{L}}(x)$ is positive then do nothing. If $\varphi^j_{\mathrm{L}}(x) = \neg\varphi^j_{\mathrm{ATO}}(x)$, then there are two possibilities either $\neg t = s$ or $\neg t < s$. But by replacing the former with $s < t \vee t < s$ and the latter with $s = t \vee s < t$, we achieve

$\vdash \exists x \ \bigwedge_{i=1}^{\alpha} \varphi^i_{\mathrm{L}}(x) \leftrightarrow \exists x \ \bigwedge_{i=1}^{\alpha} \bigvee_{j=1}^{b} \varphi^{ij}_{\mathrm{ATO}}(x)$, where $1 \leq b \leq 2$. The quantifier part of the formula can be transformed to DNF, by α applications of the distribution law $A \wedge (B \vee C) \leftrightarrow (A \wedge B) \vee (A \wedge C)$, which gives rise to at most 2^{α} disjunctions.
Explicitly this states $\vdash \exists x \ \bigwedge_{i=1}^{\alpha} \bigvee_{j=1}^{b} \varphi^{ij}_{\mathrm{ATO}}(x) \leftrightarrow \exists x \ \bigvee_{j=\beta}^{\beta} \bigwedge_{i=1}^{\alpha} \varphi^{ij}_{\mathrm{ATO}}(x)$, where $\beta \leq 2^{\alpha}$. Then finally by lemma 1,
$\vdash \exists x \ \bigvee_{j=1}^{\beta} \bigwedge_{i=1}^{\alpha} \varphi^{ij}_{\mathrm{ATO}}(x) \leftrightarrow \bigvee_{j=1}^{\beta} \exists x \ \bigwedge_{i=1}^{\alpha} \varphi^{ij}_{\mathrm{ATO}}(x)$, which concludes the proof of I.

In reduction II, we show that every atomic sentence can be written on a form, where the variable occurs alone on one of the sides of either $<$ or $=$. The difficult part in isolating only one occurrence of a variable, is to free it from multipliers. Suppose that x occurs in the scope of the multipliers $q_0 = \frac{n_0}{m_0}, \ldots, q_r = \frac{n_{r-1}}{m_{r-1}}$ in the formula $\bigwedge_{i=1}^{\alpha} \varphi^i_{\mathrm{ATO}}(x)$. Now collect the denominators of every "binding" multiplier into a big number $m = m_0 \cdot \ldots \cdot m_{r-1}$. Then by replacing each occurrence of the variable x by $m \cdot w + \overline{l}$, denoted $x/m \cdot w + \overline{l}$;

$$\exists x \bigwedge_{i=1}^{\alpha} \varphi^i_{\mathrm{ATO}}(x) \leftrightarrow \bigvee_{l=1}^{m-1} \exists w \bigwedge_{i=1}^{\alpha} \varphi^i_{\mathrm{ATO}}(x/m \cdot w + \overline{l})$$

But by elementary algebra each occurrence of the new variable w can be singlet out to stand alone on the side of an $<$ or $=$. Hence

$$\bigvee_{l=1}^{m-1} \exists w \bigwedge_{i=1}^{\alpha} \varphi^i_{\mathrm{ATO}}(m \cdot w + \overline{l}) \leftrightarrow \bigvee_{l=1}^{m-1} \exists w \, (\bigwedge_{i=1}^{\alpha_1} w < s_i \wedge \bigwedge_{j=1}^{\alpha_2} t_j < w \wedge \bigwedge_{k=1}^{\alpha_3} w = u_k \wedge \Psi)$$

where Ψ is does not contain w, neither does s_i, t_j nor u_k. Since w does not occur free in Ψ,

$$\exists w \, (\bigwedge_{i=1}^{\alpha_1} w < s_i \wedge \bigwedge_{j=1}^{\alpha_2} t_j < w \wedge \bigwedge_{k=1}^{\alpha_3} w = u_k \wedge \Psi) \leftrightarrow \exists w \, (\bigwedge_{i=1}^{\alpha_1} w < s_i \wedge \bigwedge_{j=1}^{\alpha_2} t_j < w \wedge \bigwedge_{k=1}^{\alpha_3} w = u_k) \wedge \Psi$$

which means that we end up with the problem of removing existential quantifiers in formulas of the form

$$\exists w \, (\bigwedge_{i=1}^{\alpha_1} w < s_i \wedge \bigwedge_{j=1}^{\alpha_2} t_j < w \wedge \bigwedge_{k=1}^{\alpha_3} w = u_k). \quad (\star)$$

Then finally in step III, we remove each existential quantifier $\exists w$ that after performing exhaustive II reductions. The reduction can be split into three cases according to the way ($\star$) looks.

(i) There is an equation (or more) such that $w = u_r$.
(ii) There are no equations and only one of the inequalities are true.
(iii) At least two of the different inequalities are true.

Case (i): by substitution, we get

$$\bigwedge_{i=1}^{\alpha_1} u_r < s_i \wedge \bigwedge_{j=1}^{\alpha_2} t_j < u_r \wedge \bigwedge_{k \in \{d | 1 \leq d \leq \alpha_2\} - \{r\}} u_r = u_k \wedge [u_r] = u_r.$$

The latter equation is added, since w ranges over integers to ascertain that u_r is of correct kind. It gives an inherent type-checking of the term.

Case (ii): If there are no equations then ($\star$) is of the form (a) $\exists w \ (\bigwedge_{i=1}^{\alpha_1} w < s_i)$ or (b) $\exists w \ (\bigwedge_{j=1}^{\alpha_2} t_j < w)$. In case (a), since we can choose a minimal element of the finite conjunction $w < s_1 \wedge w < s_2 \wedge \ldots \wedge w < s_{\alpha_1}$, lets say $u_{\min}$ because $\mathbb{Q}$ is unbounded down-wards, hence $u_{\min} < s_i \wedge u_{\min} < s_i \wedge \ldots \wedge u_{\min} < s_i$. In case (b) we choose a maximal element of the conjunction $t_1 < w \wedge t_2 < w \wedge \ldots \wedge t_{\alpha_2} < w$, denoted $u_{\max}$ and replace (b) in a similar manner by $\bigwedge_{j=1}^{\alpha_2}(t_j < u_{\max})$, since $\mathbb{Q}$ are unbounded up-wards.

Case (iii): We have that ($\star$) is of the form

$$\exists w \ (\bigwedge_{i=1}^{\alpha_1} w < s_i \wedge \bigwedge_{j=1}^{\alpha_2} t_j < w).$$

The sentence says that there is an integer between each of the t_j's and the s_i's. Therefore w splits the two sets of terms by the conjunction $\bigwedge_{i=1}^{\alpha_1} \bigwedge_{j=1}^{\alpha_2} t_j < s_i$, which is quantifier free. But recall that although the replacing formula is still true, information about the squeezing integer w is lost. $\square$

Since we know that the t_j's and s_i's are split by an integer, we might more faithfully search for one of these splitting terms by approximation from below $u_{\text{split}} = \max\{t_j | 1 \leq j \leq \alpha_2\}$, by taking the greatest integer, but since $[\cdot]$ returns the closest integer rounded down-wards, we must increase it by one: $[u_{\text{split}}] + \overline{1}$. This allow us to write $\bigwedge_{j=1}^{\alpha_2} t_j < [u_{\text{split}}] + \overline{1} \wedge \bigwedge_{i=1}^{\alpha_1} [u_{\text{split}}] + \overline{1} < s_i$.

Corollary 1 $\mathrm{Th}_{(\mathbb{Z},<,+,0,1)}$ *is decidable.*

Proof: Since any formula ϕ constructed over $\mathrm{Th}_{(\mathrm{Z},<,+,0,1)}$ is equivalent to a quantifier-free formula Ψ by the Skolem's theorem, the truth value of Ψ can be computed by a program. The reason is that the theory contains only equality, =, and inequality, $<$. We know that the theory of equality is decidable. Since inequalities can be expressed by $x < y \leftrightarrow \exists z(y = s(z) + x)$, the theory can be reduced to a theory of equality. $\square$

4 Why + can not define $\times$

Now we return to some interesting results, that are, by no means controversial, although they characterize the limits of theory $\mathrm{Th}_{(\mathrm{Z},<,+,0,1)}$, in very precise way. We shall do this by using the Ginsburg Spanier Theorem, and some properties of number theory.

We say that X a subset of the natural numbers $\mathbb{N}$ is *ultimately periodic* if and only if $\exists p \in \mathbb{Z}\ \exists x_0 \in \mathbb{N}\ \forall x \geq x_0(x \in X \Longleftrightarrow x + p \in X)$.

Lemma 3 *Ultimately periodic sets are closed under finite union and complementation*

Proof: We prove only that the ultimatic periodic sets are closed under complementation and union. Then by DeMorgan it is closed under intersection. We therefore need to prove

> If X and Y are *ultimately periodic*, then both $\complement X$ and $X \cup Y$ are *ultimately periodic*.

Suppose X is *ultimately periodic*. Then by definition

$\exists p \in \mathbb{Z}\ \exists x_0 \in \mathbb{N}\ \forall x \geq x_0(x \in X \Leftrightarrow x + p \in X)$, hence by logic

$\exists p \in \mathbb{Z}\ \exists x_0 \in \mathbb{N}\ \forall x \geq x_0(x \notin X \Leftrightarrow x + p \notin X)$

In case of union we need to build an ultimately periodic set based on X and Y. Let X be ultimately periodic with x_0 and p as above and let Y be ultimately periodic with y_0 and q. The idea is to use both the period p and q to construct a new ultimately periodic set. Let $r = \mathrm{lcm}(p, q)$ denote the least common multiple of p and q, and let $z_0 = \max(x_0, y_0)$ denote the maximum of x_0 and y_0. Then we must prove;

$$\forall x \geq z_0\ x \in X \cup Y \Leftrightarrow x + r \in X \cup Y.$$

Since both X and Y are periodic, we have

(a) $x \in X \Leftrightarrow \underbrace{x + p \in X \Leftrightarrow x + \underbrace{p + p}_{2 \text{ times}} \in X \Leftrightarrow \ldots \Leftrightarrow x + \underbrace{p + \ldots + p}_{q \text{ times}} \in X}_{q \text{ times}}$ and

(b) $x \in Y \Leftrightarrow \underbrace{x + q \in Y \Leftrightarrow x + \underbrace{q + q}_{2 \text{ times}} \in Y \Leftrightarrow \ldots \Leftrightarrow x + \underbrace{q + \ldots + q}_{p \text{ times}} \in Y}_{p \text{ times}}$

But this means that for $r = p \cdot q$, we have $x + r \in X$ and $x + r \in Y$, hence for every $x \geq z_0$, $x \in X \cup Y \Leftrightarrow x \in X \vee x \in Y \Leftrightarrow_{(a),(b)} x + r \in X \vee x + r \in Y \Leftrightarrow x + r \in X \cup Y$

Then finally we observe that
$x \in X \cap Y \Leftrightarrow x \in \complement(\complement X \cup \complement Y) \Leftrightarrow x \in X \wedge x \in Y \Leftrightarrow x + r \in X \wedge x + r \in Y \Leftrightarrow x + r \in X \cap Y$ $\square$

In the following section we shall write ω and $(\mathbb{N}; <, +, 0, 1)$ interchangingly. We say that an *arithmetical progression* is a function $f : \mathbb{N} \longmapsto \mathbb{N}$ such that $\exists m \exists m(f(x) = m + n \times x)$. A set $X \subseteq \mathbb{N}$ is *semi-linear* if it is the union of the image of finite number of arithmetical progressions, i.e. $X = \cup_{f \in I} \mathrm{Rang}(f)$ where $|I|$ is finite. Then we come to the most important concept, the notion of *definability*, which is emphasized by the following distinguished definition:

Definition 2 *We say that a set $X \subseteq \mathbb{N}$ is* definable *in the language $(\mathbb{N}; <, +, 0, 1)$ if there exists a formula $\phi(y)$ over the language with only y as free variable such that $\forall x \in \mathbb{N}(x \in X \Leftrightarrow (\mathbb{N}; <, +, 0, 1) \models \phi(x))$*

Lemma 4 *Definability in $(\mathbb{N}; <, +, 0, 1)$ is an boolean algebra.*

Proof: The compositionality of definability for boolean operators is proven by showing

(a) $\complement X$ is definable $\Longleftrightarrow$ X is definable
(b) $X \cap Y$ is definable $\Longleftrightarrow$ X and Y are definable
(c) $\Longleftrightarrow$ $X \cup Y$ is definable

(a) follows directly from the definition of definability, since $\forall z \in \mathbb{N}$, we have $z \in \complement X \iff (\mathbb{N}; <, +, 0, 1) \models \neg\phi(z)$ iff $z \notin X \iff (\mathbb{N}; <, +, 0, 1) \not\models \phi(z)$ iff $z \in X \iff (\mathbb{N}; <, +, 0, 1) \models \phi(z)$.
The directions $\Longleftarrow$ for (b) and (c) follows directly: If both X and Y are definable there are formulas ϕ_1 and ϕ_2 with only one free variable such that for every $z \in \mathbb{N}$,
$z \in X \iff \omega \models \phi_1(z)$ and $z \in Y \iff \omega \models \phi_2(z)$
But this gives by logic, $z \in X \wedge z \in Y \iff \omega \models \phi_1(z) \wedge \omega \models \phi_2(z)$ hence $z \in X \cap Y \iff \omega \models \phi_1(z) \wedge \phi_2(z)$, which means that $X \cap Y$ is definable, since $\phi_1 \wedge \phi_2$ has been chosen to contain only one single free variable z.

Then observe that:

$z \in X \cap Y \iff (\mathbb{N}; <, +, 0, 1) \models (\phi_1 \wedge \phi_2)(z)$

$z \in X \cup Y \iff (\mathbb{N}; <, +, 0, 1) \models (\phi_1 \vee \phi_2)(z)$

If $X \cap Y$ is definable, then there is a formula $\phi = \phi_1 \wedge \phi_2$ with only one single free variable z such that X is defined by ϕ_1, and Y is defined by ϕ_2. $\square$

Lemma 5 *If X is ultimately periodic then X is semi-linear.*

Proof: Suppose that X is ultimately periodic. Choose one period $p > 0$ and an initial argument x_0 such that $\forall x \geq x_0(x \in X \iff x + p \in X))$. For every i, such that $0 \leq i < p$, $x_i = x_0 + i$ with $x_i \in X$, define an arithmetical progression, as follows: $f_i(x) = x_i + p \times x$ and for $j \leq x_0$ such that $j \in X$, define $g_j(x) = j + 0 \times x$. Then we have $X = \bigcup_{\{0 \leq i < p\}} \mathrm{Rang}(f_i) \cup \bigcup_{\{j < x_0 | j \in X\}} \mathrm{Rang}(g_j)$ $\square$

Lemma 6 *If X is semi-linear then X is definable in the language of $(\mathbb{N}; <, +, 0, 1)$.*

Proof: Suppose that X is semi-linear. Then X is the range of finitely many arithmetical progressions. Let us say that the number is t. Each these functions are on the form $f_i(x) = m_i + n_i \cdot x$. Each of these are definable by formulas $\exists v_{t+j}(v_j = \overline{m_j} + n_j \cdot v_{t+j})$. Let $f_1(x), \ldots, f_i(x), \ldots, f_t(x)$ be a listing of the finite number of arithmetical progressions. Then

$\exists v_{t+1}(v_1 = \overline{m_1} + n_1 \cdot v_{t+1}), \ldots, \exists v_{t+t}(v_j = \overline{m_t} + n_t \cdot v_{t+t})$ defines the ranges $\mathrm{Rang}(f_1), \ldots, \mathrm{Rang}(f_t)$, but then by lemma 4, generalized to finite disjunctions, gives the result since $\exists v_{t+1}(v_1 = \overline{m_1} + n_1 \cdot v_{t+1}) \vee \ldots \vee \exists v_{t+t}(v_j = \overline{m_t} + n_t \cdot v_{t+t})$ defines the finite union $\mathrm{Rang}(f_1) \cup \ldots \cup \mathrm{Rang}(f_t)$. But recall that $X = \mathrm{Rang}(f_1) \cup \ldots \cup \mathrm{Rang}(f_t)$ and we are done.

$\square$

Lemma 7 *If X is definable in the language of $(\mathbb{N}; <, +, 0, 1)$ then X is ultimately periodic.*

Proof: Suppose now that X is definable in the language of $(\mathbb{N}; <, +, 0, 1)$ by a formula $\phi(y)$. From the discussion above we know that $\phi(y)$ is equivalent to a quantifier free and positive formula Ψ with only one free variable. Then obviously Ψ also defines X. Then by induction over $\deg(\Psi)$ we prove that if X is definable in $(\mathbb{N}; <, +, 0, 1)$ by then X is ultimately periodic.

The basis case is the hard one. If Ψ is atomic with free variable x, then we can assume that Ψ can be written on then forms

(a) $m \cdot x = \overline{k}$, (b) $m \cdot x < \overline{k}$,
(c) $\overline{k} < m \cdot x$ or (d) $m \cdot x \equiv \overline{k} (\mathrm{mod}\ n)$.

The assumption is justified by the following argument: For arbitrary terms $t_1(x)$, $t_2(x)$, either (i) $t_1(x) < t_2(x)$ or (ii) $t_1(x) = t_2(x)$. Start a simplification of (i) by rewriting the sentence by canceling each occurrence of $+\ x$ and $+\ 1$ successively on both sides of $<$. Then finally remove each occurrence of $+\ 0$. Then Ψ has the form $\underbrace{x + \ldots + x}_{m} < \underbrace{1 + \ldots + 1}_{k}$ or the form $\underbrace{1 + \ldots + 1}_{k} < \underbrace{x + \ldots + x}_{m}$. But this exactly (b) and (c). The case of equality is a bit more difficult, since the procedure to simplify ordering might give negative numbers. If this does not happens the simplification gives in a similar manner (a). Observe that (d) covers the case where simplifications would give a negative constant.

Both (a) and (b) defines a finite set, hence also an ultimate periodic set. Since the complement of (c) defines a finite set, by previous lemma itself defines an ultimate periodic set. Consider (d): Let c be the greatest common divisor of m and n, $c = \gcd(m, n)$. Then there are two options: Either d is a divisor in k or not.

If $\neg d|k$, then $m \cdot x \not\equiv \overline{k} (\mathrm{mod}\ n)$. But then (d) defines the empty set, which is an ultimately periodic set.

If $d|k$ then by dividing out (d), $m_0 \cdot x \equiv \overline{k_0} (\mathrm{mod}\ n_0)$, where m_0 and n_0 are relatively prime. But since ... m_0 has a multiplicative inverse m^{-1}. Then $m_0 \cdot x \equiv \overline{k_0} (\mathrm{mod}\ n_0) \Longleftrightarrow m^{-1} \cdot m_0 \cdot x \equiv m^{-1} \cdot \overline{k_0} (\mathrm{mod}\ n_0) \Longleftrightarrow x \equiv \overline{k_1} (\mathrm{mod}\ n_0)$. But $x \equiv \overline{k_1} (\mathrm{mod}\ n_0)$ defines a periodic set, and hence an ultimately periodic set.

Induction step: Suppose that X is definable by the formula $\Psi = \Psi_1 \wedge \Psi_2$. This means that $\forall x \in \mathbb{N} (x \in X \Leftrightarrow (\mathbb{N}; <, +, 0, 1) \models (\Psi_1 \wedge \Psi_2)(x)$ with at most one free variable x. But then by previous lemma X can be partitioned into the intersection of two sets $X = Z_1 \cap Z_2$, such that both Z_1 and Z_2 are definable by respectively Ψ_1 and Ψ_2. Then by induction hypothesis, Z_1 and Z_2 are both ultimately periodic. Since ultimately periodic sets are closed under intersections, $X = Z_1 \cap Z_2$ is ultimately periodic.

The cases where X is definable by formulas $\Psi_1 \vee \Psi_2$ is similar and therefore omitted. $\square$

Theorem 3 *(Ginsburg Spanier) Let $X \subseteq \mathbb{N}$. Then the following is equivalent:*

(i) *X is definable in the language of $(\mathbb{N}; <, +, 0, 1)$*

(ii) *X is ultimately periodic*

(iii) *X is semi-linear*

Proof: Given the three previous lemmas the proof is easy, since $(ii) \implies (iii)$ by lemma 5, $(iii) \implies (i)$ by lemma 6 and finally $(i) \implies (ii)$ lemma 7. $\square$

The original result by Ginsburg Spanier occurred in [GS66]. Their primary aim was to investigate relations between Presburger formulas and automatas.

The next corollary is the one telling us what limits of expressibility for such theories are:

Corollary 2 *In the language of* $(\mathbb{N}; <, +, 0, 1)$*, the following is not definable in the language: (i)* $z = x \times y$ *,* $(ii)x$ *is a square (iii)* $z = x|y$*, (iv)* x *is prime.*

Proof: The proof follows from the Ginsburg Spanier theorem. In each case (i) - (iv), it is sufficient to classify the sets as either not ultimately periodic or semi-linear. Since (ii) - (iv) are defined by (i), that is; $x|y \leftrightarrow \exists z \leq y\ (y = x \times z)$, $x^2 = x \times x$ and $\mathrm{Prime}(x) \leftrightarrow \forall y < x(y|x \rightarrow y = 1)$, it is sufficient to prove that $x \times y$ is not semi-linear. Suppose for contradiction that multiplication $F(x, y) = x \times y$ is semi-linear. This means that $F(x, y)$ is the union of the range of finitely many arithmetical progressions. Consider this set: $\bigcup_{f \in I} \mathrm{Rang}(f)$, where $|I| = n$ and $n \in \mathbb{N}$. This means that we can choose from functions $f_1(y) = m_1 + k_1 \cdot y, \ldots, f_n(y) = m_n + k_n \cdot y$. By assigning 0 to the constants $m_1, \ldots, m_n$, we get $f_1(y) = k_1 \cdot y, \ldots, f_n(y) = k_n \cdot y$. But in order to approach $x \times y$. we need an infinite number of k_i's to construct arbitrary x's. If we order the functions with the natural numbers we get $f_1(y) = \overline{1} \times y$, $f_2(y) = \overline{2} \times y, \ldots$. But since $f_x(y) = x \times y$ defines infinitely many arithmetical progressions $F(x, y)$ is not semi-linear. $\square$

5 Completeness of multiplication

A method for deciding theories form multiplication was presented in [Sko70]. Since Skolem was presenting his method through examples, he did not actually prove the theorem. The full proof was given by Andrzej Mostowski in [Mos52]. Mostowski's proved the decidability of multiplication by reducing the question of decidability of addition. By the fundamental theorem of arithmetic, every positive number can be written uniquely as the product of a prime number exponent. Moreover if $p_0 = 2, p_1, \ldots, p_m$ denotes the first prime numbers. Then the positive natural numbers x and y can be written on the form $x = p_0^{n_0} \times \ldots \times p_r^{n_r}$, $y = p_0^{m_0} \times \ldots \times p_s^{m_s}$, where $x \times y = p_0^{n_0+m_0} \times \ldots \times p_t^{n_t+m_t}$ where $t = \max(r, s)$. Moreover the unit, is given by $1 = p_0^0 \times \ldots \times p_t^0$. Then $\mathrm{Th}_{(\mathbb{N};\times,1)}$ is isomorphic to the weak directed power of $\mathrm{Th}_{(\mathbb{N};+,0)}$.

Theorem 4 *(Mostowski) If* T *is a decidable theory with a unique distinguished constant, then the theory of weak directed powers of models of* T *is decidable.*

Theorem 5 *(Skolem/Mostowski)* $\mathrm{Th}_{(\mathbb{N}^+;\times,1)}$ *is decidable.*

Proof: (Sketch) The theory ($\mathrm{Th}_{(\mathbb{N};+,0)}$ is decidable theory with a unique distinguished constant 0, as we know by Presburger and Skolem's result discussed earlier. But $\mathrm{Th}_{(\mathbb{N};\times,1)}$ is isomorphic to the weak directed power of $\mathrm{Th}_{(\mathbb{N};+,0)}$; with the correspondance $0 \approx 1$ and $+ \approx \times$. But this gives that the theory $\mathrm{Th}_{(\mathbb{N};\times,1)}$ is decidable, since it is the theory of weak directed powers of $\mathrm{Th}_{(\mathbb{N};+,0)}$. $\square$

A direct method for quantifier elimination of $\mathrm{Th}_{(\mathbb{N}^+;\times,1)}$ based on quantifier elimination of $\mathrm{Th}_{(\mathbb{N};+,0)}$ was given by [Ceg81].

6 Concluding remarks

Similar results can be obtained for the weaker theories of successor $\mathrm{Th}_{(\mathbb{N};\mathrm{s},0)}$, and successor with ordering $\mathrm{Th}_{(\mathbb{N};<,\mathrm{s},0)}$. Variants of the Ginsburg Spanier theorem accompanied by appropriate quantifier eliminations can also be used to show rather surprising results, e.g. that $<$ is not definable in the structure $(\mathbb{Z};+,0,1)$.

From the history of science it is interesting, maybe not accidential, that the incompleteness of full arithmetic was proven in the same year as the decidability of the weak fragments of arithmetic was settled. This might have come to be from a general interest at the time, in foundational issues by the leading researchers in logic.

References

[Ceg81] Patrick Cegielski. Theorie elementaire de la multiplication des entiers naturels. In *Model Theory and Arithmetic*. Springer Verlag, 1981.

[G$\ddot{3}$1] Kurt Gödel. Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I. In *Collected Works*, volume 1. Oxford University Press, 1931.

[GS66] Seymour Ginsburg and Edwin H. Spanier. Semigroups, Presburger Formulas, and Languages. *Pacific Journal of Mathematics*, 16(2):285 – 296, 1966.

[Hod97] Wilfid Hodges. *A shorter model theory*. Cambridge University Press, 1997.

[Men97] Elliott Mendelson. *Introduction to Mathematical Logic*. Chapman and Hall, 4 edition, 1997.

[Mos52] Andrzej Mostowski. On Direct Products of Theories. *Journal of Symbolic Logic*, 17(1):1 – 32, March 1952.

[Sho67] Joseph R. Shoenfield. *Mathematical Logic*. Association for symbolic Logic, 1967. Reprint 2000 of original manuscript.

[Sko70] Thoralf Skolem. Über einige Satzfunktionen in der Arithmetik. In Jens Erik Fenstad, editor, *Selected Works in Logic*, pages 281 – 306. Universitetsforlaget, 1970. Originally published 1931.

[Smo91] Craig Smorynski. *Logical Number Theory I; An Introduction*. Springer Verlag, 1991.