Mathematical Logic Project

Sebastian Karlsson

January 12, 2022

1 Introduction

We will construct a first order theory T with vocabulary $\{+, 0\}$ such that for all models $\mathcal{M}$, $\mathcal{M} \models T$ if and only if $\mathcal{M}$ is an infinite abelian group in which every element is its own inverse (i.e. every element is an involution). We show that T is $\aleph_0$-categorical and that the set of Gödel numbers of theorems of T is recursive.

2 Axioms of T

Definition 1. Let T' be the following set of $\{+, 0\}$-formulas:

1. $\forall v_0(v_0 + 0 = v_0)$
2. $\forall v_0(v_0 + v_0 = 0)$
3. $\forall v_0 \forall v_1 \forall v_2((v_0 + v_1) + v_2 = v_0 + (v_1 + v_2))$
4. $\forall v_0 \forall v_1(v_0 + v_1 = v_1 + v_0)$
5. For each $n \in \mathbb{N} \setminus \{0\}$, we have the following schema:

$$\psi_n := \exists v_0 \exists v_1 ... \exists v_n \left(\bigwedge_{0 \leq i < j \leq n} \neg v_i = v_j \right)$$

We now let T be the first order theory axiomatized by T', i.e.

$$T = \{\varphi | \varphi \text{ is a } \{+, 0\}\text{-sentence and } T' \vdash \varphi\}$$

We use the same definition of provability of a formula φ from a set of formulas Σ (denoted by $\Sigma \vdash \varphi$) as in [1].

Example 1. The point of axioms 1-4 is to ensure that models of T are abelian groups with all elements involutions. The point of the 5-th axiom (schema) is to ensure that all models of T are infinite. ψ_n is satisfied in a model whenever the model have at least n elements. For $n = 1$ and $n = 2$, ψ_n is:

$$\psi_1 = \exists v_0 \exists v_1 (\neg v_0 = v_1)$$
$$\psi_2 = \exists v_0 \exists v_1 \exists v_2 (\neg v_0 = v_1 \wedge \neg v_0 = v_2 \wedge \neg v_1 = v_2)$$

3 Models of T

A $\{+, 0\}$ model $\mathcal{M}$ is a triple $(M, +^{\mathcal{M}}, 0^{\mathcal{M}})$ where M is any set, $0^{\mathcal{M}} \in M$ and $+^{\mathcal{M}} : M \times M \to M$ is a binary operation on M. For simplicity, we write just 0 and + for $0^{\mathcal{M}}$ and $+^{\mathcal{M}}$.

Theorem 1. *For any model $\mathcal{M}$, $\mathcal{M} \models T$ if and only if $\mathcal{M}$ is an infinite abelian group in which every element is an involution.*

Proof. By the soundness theorem, if $\mathcal{M} \models T'$ then $\mathcal{M} \models T$. Since $T' \subset T$, the converse holds as well. Thus, it is sufficient to prove the theorem for T'.

For the direction from left to right, by Tarski's truth definition:

1. If $\mathcal{M} \models$ ax. 1. then for all $x \in M$, $x + 0 = x$. Together with axiom 4, we also get that $0 + x = x$. Thus, M contains a two-sided inverse with respect to +.

2. If $\mathcal{M} \models$ ax. 2. then for all $x \in M$, $x + x = 0$. Hence, every element in M is an involution (which implies that every element also has an inverse).

3. If $\mathcal{M} \models$ ax. 3. then for all x, y and $z \in M$, $(x + y) + z = x + (y + z)$, i.e. + is an associative operation.

4. If $\mathcal{M} \models$ ax. 4. then for all $x, y \in M$, $x + y = y + x$ so + is commutative.

5. If $\mathcal{M} \models \psi_n$ then M contains at least n distinct elements. Since this is true for each $n \in \mathbb{N} \setminus \{0\}$, M contains infinitely many elements.

1-3 shows that $\mathcal{M}$ is a group (and every element is an involution), 4 shows that $\mathcal{M}$ is abelian and 5 that $\mathcal{M}$ is infinite. Thus, $\mathcal{M}$ is as desired. The direction from right to left is similar. $\square$

If we have an arbitrary sum of elements in a model $\mathcal{M}$ of T, say $x+y+y+x+x+z$ for $x, y, z \in M$, we note that since $\mathcal{M}$ is abelian, we can rearrange the terms as follows: $x+x+x+y+y+z$. Furthermore, since any two elements that are the same take each other out, we can count the elements modulo 2 and write:

$$x+x+x+y+y+z = 1x + 0y + 1z$$

Using this notation, it turns out that $\mathcal{M}$ can be seen as a vector space over $\mathbb{Z}/2\mathbb{Z}$. For $a \in \mathbb{Z}/2\mathbb{Z}$ and $m \in \mathcal{M}$, we define:

$$\mathcal{M} \ni am = \begin{cases} m & \text{if } a = 1 \\ 0 & \text{if } a = 0 \end{cases} \tag{1}$$

Theorem 2. *Using the scalar multiplication defined in (1), any model $\mathcal{M}$ of T is a vector space over $\mathbb{Z}/2\mathbb{Z}$.*

Proof. We already know that $+$ is associative and commutative, that there is an identity $0^{\mathcal{M}} \in \mathcal{M}$ and that inverses exist. We are left to verify the vector space axioms involving scalar multiplication:

$$\begin{aligned} a(a'm) &= (a \cdot a')m \\ 1m &= m \\ a(m+m') &= am + am' \\ (a+a')m &= am + a'm \end{aligned}$$

Where $a, a' \in \mathbb{Z}/2\mathbb{Z}$ and $m, m' \in \mathcal{M}$. Since $\mathbb{Z}/2\mathbb{Z}$ only contains 2 elements, one may verify each case separately. For example, if $a = 0$ and $a' = 1$ then the first axiom is correct:

$$a(a'm) = 0(1m) = 0m = (0 \cdot 1)m = (a \cdot a')m$$

The other axioms and cases can be verified similarly. $\square$

Example 2. The set of all polynomials over $\mathbb{Z}/2\mathbb{Z}$ is under addition a model of T.

Since any model $\mathcal{M}$ of T is a vector space, it follows that $\mathcal{M}$ has a basis B [2], i.e. that every $m \in \mathcal{M}$ can be written in the form $a_0b_0 + a_1b_1 + ... + a_nb_n$ for $a_i \in \mathbb{Z}/2\mathbb{Z}$ and $b_i \in B$, $0 \leq i \leq n$. Furthermore, if each a_i is required to be nonzero, then this representation is unique up to the order of the terms, and we can just express this as follows: Each $m \in \mathcal{M}$ can be written uniquely as a sum of distinct elements $b_0, b_1, ...b_n \in B$, $m = b_0 + b_1 + ... + b_n$.

Lemma 1. *Let $\mathcal{M}$ be a model of T. Any basis B of $\mathcal{M}$ is infinite.*

Proof. Suppose $B = \{b_0, b_1, ..., b_n\}$ is a finite basis of $\mathcal{M}$. Then any $m \in \mathcal{M}$ has a unique representation $m = b_{i_1} + b_{i_2} + ... + b_{i_m}$ where $0 \leq i_1 < i_2 < ... < i_m \leq n$. Since there are only finitely many representations of this form, it follows that $\mathcal{M}$ contains only finitely many elements. This is a contradiction. □

Theorem 3. *T is $\aleph_0$-categorical.*

Proof. Suppose that $\mathcal{M}$ and $\mathcal{M}'$ are two countable models of T. If we can show that $\mathcal{M} \cong \mathcal{M}'$, then T is $\aleph_0$-categorical. By lemma 1, both $\mathcal{M}$ and $\mathcal{M}'$ are vector spaces over $\mathbb{Z}/2\mathbb{Z}$ with bases B and B'. Since $|B| = \aleph_0$ and $|B'| = \aleph_0$, they have the same dimension. Thus, $\mathcal{M}$ and $\mathcal{M}'$ are isomorphic as vector spaces [3] and hence also isomorphic as groups.

□

Corollary 1. *T is complete.*

Proof. By example 2, T has a model so T is consistent. By the Łos-Vaught theorem, since T has no finite models and since T is $\aleph_0$-categorical, T is complete. □

4 The set of T-theorems is recursive

The set of $\{+, 0\}$-formulas can be seen as a subset of formulas of number theory (using vocabulary $\{0, 1, +, \times, exp\}$). Thus, we may define the Gödel number of a $\{+, 0\}$-formula to be the Gödel number of that same formula viewed as a formula of number theory. We use the same gödel numbering as in [1]. We let Sen_T be the set of Gödel numbers of all $\{+, 0\}$-sentences and Thm_T be the set of Gödel numbers of all theorems of T.

The goal of this section is to prove that Thm_T is a recursive set. First, one has to prove that the set of all $\{+, 0\}$-sentences is recursive. The easiest way to do this is to utilize the already known theorem that the set of sentences of number theory, Sen, is primitive recursive, and then restrict this set to those sentences that don't contain the symbols $1, \times$ and exp. Since $\#(1) = 1$, $\#(\times) = 3$ and $\#(exp) = 4$, we know that a word w doesn't contain these symbols if and only if there is no prime that divides w precisely 2, 4 or 5 times. Define:

$$f_k(n) = (\mu m \leq n)(isPrime(m) \wedge m^k \mid n \wedge m^{k+1} \nmid n)$$

Now $f_k(n)$ is a primitive recursive function that gives the smallest prime which divides n precisely k times, or 0 if no such prime exists.

Theorem 4. *Sen_T is a primitive recursive set.*

Proof. Because $n \in \mathrm{Sen}_T$ if and only if

$$n \in \text{ Sen } \wedge f_2(n) = 0 \wedge f_4(n) = 0 \wedge f_5(n) = 0$$

□

The next step is to prove that Thm_T is recursively enumerable. This can be used together with the completeness of T to prove that Thm_T is also recursive. Once again, one may take shortcuts from the already proven theorems of these things in number theory. However, first we must show that the set of Gödel numbers of axioms of T is p.r.

Lemma 2. $\{\ulcorner \psi_n \urcorner \mid n \in \mathbb{N}\}$ *is p.r.*

Proof. Let $w_n = \exists v_0 \exists v_1 ... \exists v_n$ and

$$\psi'_n = \bigwedge_{0 \leq i < j \leq n} \neg v_i = v_j$$

One notes that for $n > 1$

$$\psi'_n = \left(\bigwedge_{0 \leq i < j \leq n-1} \neg v_i = v_j \right) \wedge \neg v_0 = v_n \wedge \neg v_1 = v_n \wedge ... \wedge \neg v_{n-1} = v_n$$

so we define $\sigma_n := \neg v_0 = v_n \wedge \neg v_1 = v_n \wedge ... \wedge \neg v_{n-1} = v_n$. The function $g_\sigma(n) := \ulcorner \sigma_n \urcorner$ is primitive recursive:

$$g_\sigma(n) = \prod_{i=0}^{5n-2} p_i^{h(i,n)+1}$$

where h is the primitive recursive function

$$h(i,n) = \begin{cases} \#(\neg) & \text{if } i \equiv 0 \mod 5 \\ \#(v_{(i-1)/5}) & \text{if } i \equiv 1 \mod 5 \\ \#(=) & \text{if } i \equiv 2 \mod 5 \\ \#(v_n) & \text{if } i \equiv 3 \mod 5 \\ \#(\wedge) & \text{if } i \equiv 4 \mod 5 \end{cases}$$

Now, let $g_{\psi'}(n) = \ulcorner \psi'_{n+1} \urcorner$. $g_{\psi'}$ is primitive recursive:

$$\begin{cases} g_{\psi'}(0) & = g_\sigma(1) \\ g_{\psi'}(n+1) & = g_{\psi'}(n) * \ulcorner \wedge \urcorner * g_\sigma(n+1) \end{cases}$$

$g_w(n) = \ulcorner w_n \urcorner$ can be shown to be p.r. in a similar way as g_σ. Furthermore, $g(n) = \ulcorner \psi_{n+1} \urcorner$ is primitive recursive since $g(n) = g_w(n+1) * \ulcorner (\urcorner * g_{\psi'}(n) * \ulcorner) \urcorner$. It is now possible to define the characteristic function of $\{\ulcorner \psi_n \urcorner \mid n \in \mathbb{N}\}$, and conclude that the set is p.r.:

$$f(m) = \begin{cases} 1 & \text{if } (\exists n \leq m)(m = g(n)) \\ 0 & \text{otherwise} \end{cases}$$

□

Since the remaining axioms is just a finite collection, we can deduce the following corollary:

Corollary 2. *The set of Gödel numbers of elements of T' is p.r.*

Theorem 5. *Thm_T is recursively enumerable.*

Proof. We prove this in the same way as theorem 5.30 in [1], using the same notation. Let Prf_T be the set of numbers m such that $\langle (m)_0, (m)_1, ..., (m)_{\mathrm{len}(m)} \rangle$ is a deduction from T'. We start by showing that Prf_T is p.r. Let

$\mathrm{Fml}_T = \{\ulcorner \varphi \urcorner \mid \varphi \text{ is a } \{+, 0\}\text{-formula}\}$
$\mathrm{PrAx}_T = \mathrm{PrAx} \cap \mathrm{Fml}_T$
$\mathrm{IdAx}_T = \mathrm{IdAx} \cap \mathrm{Fml}_T$
$\mathrm{MP}_T = \mathrm{MP} \cap (\mathrm{Fml}_T \times \mathrm{Fml}_T \times \mathrm{Fml}_T)$
$\mathrm{Ug}_T = \mathrm{Ug} \cap (\mathbb{N} \times \mathrm{Fml}_T \times \mathrm{Fml}_T)$

Fml_T is p.r. by the same argument that Sen_T is p.r. Since PrAx, IdAx, MP and Ug are all primitive recursive sets, it follows that PrAx_T, IdAx_T, MP_T and Ug_T are as well. The characteristic function of Prf_T can now be defined with precisely the same formula as in [1], using T', PrAx_T, IdAx_T, MP_T and Ug_T instead of PeAx, PrAx, IdAx, MP and Ug. Thus, Prf_T is a recursive set. Now $n \in \mathrm{Thm}_T$ if and only if there is an $m \in \mathrm{Prf}_T$ such that $(m)_{\mathrm{len}(m)} = n$ and $n \in \mathrm{Sen}_T$. It now follows from lemma 5.29 in [1] that Thm_T is r.e.

□

Theorem 6. *Thm_T is recursive.*

Proof. Since T is complete, the complement of Thm_T (i.e. $\mathbb{N} \setminus \mathrm{Thm}_T$) is the set

$$\{\ulcorner \neg \urcorner * n \mid n \in \mathrm{Thm}_T\} \cup \{n \in \mathbb{N} \mid n \notin \mathrm{Sen}_T\}$$

Since Sen_T is recursive, it follows from theorem 5.27 in [1] that its complement is r.e. Let Sen_T^C be the range of the recursive function h_1. Furthermore, by theorem

5, Thm_T recursively enumerable by, say, the function h_2. Thus, we may define:

$$\begin{cases} h(2n) & = \ulcorner \neg \urcorner * h_2(n) \\ h(2n+1) & = h_1(n) \end{cases}$$

Now, $\mathrm{Thm}_T^C = \{h(n) | n \in \mathbb{N}\}$ and h is recursive so Thm_T^C is r.e. By theorem 5.27 in [1], it follows that Thm_T is recursive.

□

References

[1] Jouko Väänänen. *A Short Course on Mathematical Logic*. 2018.

[2] John L. Bell. The Axiom of Choice. In Edward N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University, Winter 2021 edition, 2021.

[3] George W. Mackey. On infinite-dimensional linear spaces. *Transactions of the American Mathematical Society*, 57(2):155–207, 1945.