Undecidability and Concatenation

Andrzej Grzegorczyk Konrad Zdanowski

April 12, 2007

Abstract

We consider the problem stated by Andrzej Grzegorczyk in "Undecidability without arithmetization" (Studia Logica 79(2005)) whether certain weak theory of concatenation is essentially undecidable. We give a positive answer for this problem.

1 Introduction and motivations

The present paper is devoted to proving the essential undecidability of the theory TC of concatenation of words. The paper may be treated as a continuation of the paper [Grz05] written by the first author. We adopt some of the style, notation, abbreviations and results of [Grz05].

We consider the theory of concatenation as presented in [Grz05]. This is a weak theory of words over two letter alphabet $\Sigma = \{a, b\}$. The axioms are the following:

TC1 $x\frown(y\frown z) = (x\frown y)\frown z$,

TC2 $x\frown y = z\frown w \Rightarrow$

$$((x = z \wedge y = w) \vee \exists u((x\frown u = z \wedge y = u\frown w) \vee (x = z\frown u \wedge u\frown y = w))),$$

TC3 $\neg(\alpha = x\frown y)$,

TC4 $\neg(\beta = x\frown y)$,

TC5 $\neg(\alpha = \beta)$.

Here α and β denote one letter words a and b respectively. Concatenation may be understood as a function defined on arbitrary texts and such that:

if x and y are some texts then $x \frown y$ is a text composed of the texts x and y in such a manner that the text y follows immediately the text x.

TC1 and TC2 are due to A. Tarski. The other axioms say only that one letter words a and b are indivisible and different. Let us note that we adopt the convention from [Grz05] and we do not have in our universe the empty word. This is inessential convention since it is easily seen that both theories of concatenation of words: with and without the empty word are interpretable one into the other one.[1]

We call the axiom TC2 as the editor axiom. The intuition for that name is the following. Let us assume that two editors, A and B, divide the same book into two volumes: A into x and y and B into z and w. Then, one of the two things happens. Either they divided the book into the same volumes or there is a part of the book u such that their partitions differ exactly with the respect to the placement of u into the end of the first volume or into the beginning of the second one.

The above theory TC is proved undecidable in [Grz05]. Here we prove that it is essentially undecidable.

Now, let us say a bit more about motivations. In [Grz05] there are mentioned some arguments why the theory TC seems to be interesting. One can add an argument more. The theory TC may be understood as the theory of concatenation of texts which may be also infinite ordered strings having any arbitrary power of symbols and which are ordered in substrings of any arbitrary order and any power. Hence concatenation may be conceived as an operation on order-types, which have an additional peculiarity. The conception of order-types has been defined by George Cantor. Cantor defined also the operation which he called addition of order-types. The Cantor's addition satisfies the axioms TC1 and TC2. Cantor's order-type is the class of abstraction of a similarity s which is an isomorphic mapping of order. A text may be conceived as a type of an order R, but we also suppose that the similarity s identifies the elements which have the peculiarities of a given set P.

Thus a formal definition of text as a class of abstraction may be the

[1]Indeed, if we have the empty word in the universe then the formula $\exists y(x \frown y \neq y \vee y \frown x \neq y)$ defines the submodel with the universe consisting of the nonempty words. And moreover, each model of TC can be obtained as such restriction.

It is a bit harder to define a model with the empty word in a model of TC. If $M = (U, \frown, a, b)$ is a model of TC then we can define the set of pairs $\{(a, a)\} \cup \{b\} \times U$ and treat the element (a, a) as the unique empty word and the elements (b, a), (b, b) as two one letter word. The concatenation operation can be defined from the concatenation in M. Again, each model of the theory or words with the empty word can be obtained is this way.

following: Let U be an universe and let P be a set (of letters). We consider pairs $\langle R, F\rangle$ such that R is an order of U and F is a mapping from U into P. Then, we can set Texts($\langle R, F\rangle$) as the following class of abstraction:

$$\begin{aligned}&\text{Texts}(\langle R, F\rangle) = \{\langle R', F'\rangle : \exists s\colon U \longrightarrow U[\ s \text{ is 1--1 and ``onto'' and} \\ &\quad \forall x \in U \forall y \in U\,(xRy \equiv s(x)R's(y)) \wedge \forall x \in U(F(x) = F'(s(x)))]\}.\end{aligned}$$

A simple example is when the set P contains only two elements and a mapping F is such that

$$\forall x \in U(F(x) = a \vee F(x) = b),$$

where a and b are different.

One can also imagine strings as geometrically continuous entities which cannot be understood as composed of separate atoms (like points). Thinking in TC we are not obliged to think about something similar to real finite texts of letters. These facts open also some new perspectives larger than the arithmetic of natural numbers.

2 Basic notions

We extend our language with new definable relations. So, we write $x \subseteq y$ as a shorthand for

$$x = y \vee \exists u_1 \exists u_2 (u_1 \frown x = y \vee u_1 \frown x \frown u_2 = y \vee x \frown u_2 = y).$$

Of course, the intuitive meaning of $x \subseteq y$ is that the word x is a subword of y. We write $x \nsubseteq y$ for the negation of $x \subseteq y$.

For a given alphabet Γ, we write Γ^+ to denote the set of all finite nonempty words over Γ. With some abuse of notation we write also $u \subseteq w$, for $u, w \in \Gamma^+$, to state that u is a subword of w. It should be always clear from the context whether we mean a formula of our formal theory or the relation between words. These two things should not be mixed together. The formula, like $x \subseteq y$, is just a sequence of symbols in our language which can be interpreted in many various ways, the relation $\subseteq$, which is a subset of $\Gamma^+ \times \Gamma^+$, is a set theoretical object which refers to a property of words (from the standard model of TC). Therefore, the reader is asked for a constant attention to differentiate the situation when we talk about words $u, w \in \Gamma^+$ such that $u \subseteq w$ from that when we use $x \subseteq y$ as a formula of TC.

We use also $x \subseteq_e y$ as a shorthand for

$$x = y \vee \exists u\,(x \frown u = y).$$

The intuitive meaning of the above formula is that x is a word which is an initial subword of y. However, in contrast to $x \subseteq y$, we treat $x \subseteq_e y$ only as a definitional extension, not as a new atomic formula.

We will often skip the concatenation symbol between two words just as it is in case of the multiplication symbol in arithmetic. So xy should be read as $x \frown y$. We do this especially often when we concatenate one letter words. Thus, e.g. $\alpha\beta\alpha$ should be read as a term $\alpha \frown \beta \frown \alpha$ and the intuitive meaning of this term is the word aba. Let us note that we did not write parenthesis in $\alpha \frown \beta \frown \alpha$. Thus, this term can be read either as $(\alpha \frown \beta) \frown \alpha$ or $\alpha \frown (\beta \frown \alpha)$. However, these two terms are provably equal under TC1. We will skip parenthesis in terms whenever possible, that is everywhere.

In our proof we use a theory of concatenation over 3 letters alphabet $\Sigma' = \{a, b, c\}$. So, the language of our theory has one binary function symbol $\frown$ for concatenation and constants α, β and γ for denoting one letter words a, b and c, respectively. Accordingly, we need to extend the set of axioms. We change TC5 into

TC5′ $\neg(\alpha = \beta \vee \alpha = \gamma \vee \beta = \gamma)$

and we add

TC6 $\neg(\gamma = x \frown y)$.

We call this theory TC′. This small extension simplifies our reasoning and does not affect the main result since this theory is easily interpretable in the theory TC of concatenation over two letters alphabet. Indeed, working with the two letter alphabet one can consider only words from the set $\{aba, abba, abbba\}^+$. Then, the formula $\varphi_U(x)$ of the form

$$\beta\alpha\beta \not\subseteq x \wedge \alpha\alpha\alpha \not\subseteq x \wedge \beta\beta\beta\beta \not\subseteq x \wedge$$

$$\exists u \subseteq x(\alpha\beta \frown u = x) \wedge \exists u \subseteq x(u \frown \beta\alpha = x)$$

defines within Σ^+ the universe of the words from $\{aba, abba, abbba\}^+$. Moreover, it is straightforward to show that we can prove in TC all axioms of TC′ if we define α, β and γ as terms $\alpha\beta\alpha$, $\alpha\beta\beta\alpha$ and $\alpha\beta\beta\beta\alpha$ and restrict quantification to the set defined by $\varphi_U(x)$.

We say that a formula φ is Δ_0 if all quantifiers in φ are of the form $Qx \subseteq y$, where $Q \in \{\exists, \forall\}$. That means that all quantifiers are relativized to subwords of other words. This relativization is a special case of relativizations of quantifications to a set definable by a formula $\varphi(x)$. In such situations we use notation

$$(\forall x{:}\varphi(x))\, \psi(x) \text{ which is } \forall x(\varphi(x) \Rightarrow \psi(x))$$

and

$$(\exists x{:}\varphi(x))\,\psi(x) \text{ which is } \exists x(\varphi(x) \wedge \psi(x)).$$

Let us define Δ_0 formulae which will be used most often as formulae to which we relativize quantifiers:

1. $\alpha\beta(x) = (\gamma \not\subseteq x)$ which says that x is a word which does not contain c;
2. $\alpha(x) = (\beta \not\subseteq x \wedge \gamma \not\subseteq x)$ which says that x is a word which does not contain b and c;
3. $\beta(x) = (\alpha \not\subseteq x \wedge \gamma \not\subseteq x)$ which says that x is a word which does not contain a and c.

All words in Σ'^{+} have their names in TC$'$. We take a convention from arithmetic and for $u \in \Sigma'^{+}$ by $\underline{u}$ we denote the term whose denotation is u. E.g. $\underline{abca} = \alpha\beta\gamma\alpha$.

We use also an ω–type ordering on the set of words from $\{a, b\}^{+}$.

Definition 1 *For $u, w \in \{a, b\}^{+}$, $u < w$ if either the length of u is less than the length of w or u and w have equal length and u is smaller than w in the usual lexicographic ordering. More formally, for $u, w \in \{a, b\}^{+}$, $u = u_n \dots u_0$ and $w = w_k \dots w_0$, where $u_i, w_j \in \{a, b\}$, for $i \leq n$, $j \leq k$, it holds that $u < w$ if*

$$n < k \vee [n = k \wedge \exists i \leq n(\forall j \leq n(i < j \Rightarrow u_j = w_j) \wedge u_i = a \wedge w_i = b)].$$

An initial segment of this ordering is the following: a, b, aa, ab, ba, bb, aaa, aab, aba. We fix this enumeration as $\{u_i\}_{i\in\omega}$, so e.g. $u_0 = a$, $u_1 = b$, $u_2 = aa$. We will show later that this ordering is definable by a formula $\varphi_<(x, y)$ of TC$'$ and that TC$'$ proves useful properties of $\varphi_<(x, y)$. This formula uses all three symbols: α, β and γ. We could write this definition already in TC without the use of the third letter (see e.g. [Qui46] for such a definition). However, this would make unnecessary complications.

3 The essential undecidability of TC

Our line of the proof of the essential undecidability of TC is classical. Firstly, we take TC$'$, an extension of TC. By the remark made in Section 2 it is enough to show the essential undecidability of TC$'$. Then, we show the Σ_1–completeness of TC$'$. Namely, we show for any Σ_1–formula φ which is true in the standard model $\{a, b, c\}^{+}$ that φ is also provable in TC$'$. Next, we provide a Σ_1 formula $\varphi_<(x, y)$ which defines the ω–type ordering $<$ on the words from $\{a,b\}^+$ in the standard model $\{a,b,c\}^+$. Then, we show that for any word $u \in \{a,b\}^+$,

$$\mathrm{TC}' \vdash (\forall x{:}\alpha\beta(x))(\varphi_<(x,\underline{u}) \iff \bigvee_{w<u} x = \underline{w}).$$

Moreover, there is a formula, which we call $\mathrm{HasWit}(x)$, such that for all $u \in \{a,b\}^+$,

$$\mathrm{TC}' \vdash \mathrm{HasWit}(\underline{u})$$

and

$$\mathrm{TC}' \vdash \forall x(\mathrm{HasWit}(x) \Rightarrow (\varphi_<(x,\underline{u}) \vee x = \underline{u} \vee \varphi_<(\underline{u},x))).$$

Having the above facts it is easy to show, using some coding of computations as finite words, that TC' is essentially undecidable. We show this final argument at the end of the paper.

3.1 Σ_1–completeness of TC'

Each element $u \in \{a,b,c\}^+$ has its name $\underline{u}$ in TC'. Thus, to show that TC' proves all Σ_1–sentences true in $\{a,b\}^+$ it is enough to show this only for Δ_0–sentences. We do this in a series of lemmas. This result itself was proven in [Grz05]. So we do not include the full proof here but we only write the basic steps of the proof. We decided to do this because our present formalization differs from that of [Grz05].

Lemma 2 *For each $u, w \in \{a,b,c\}^+$,*

$$\mathrm{TC}' \vdash \neg(\underline{u} = \underline{w}) \textit{ if and only if } u \neq w.$$

Proof. The proof is by induction on (the length of) u. For the base case one should use TC5′. For the induction step one should also use associativity and the editor axiom. We skip the proof here. □

Now, we show that TC' can handle $x \subseteq y$ relation.

Lemma 3 *For all $u \in \{a,b,c\}^+$,*

$$\mathrm{TC}' \vdash \forall x(x \subseteq \underline{u} \iff \bigvee_{w \subseteq u} x = \underline{w}).$$

Proof. Let us observe that the implication from the right to the left is obvious. Thus, we prove only the converse.

The proof is by induction on the word u. For $u = a$ the thesis follows from the fact that $\forall x \neg(\alpha = x \frown y)$. Similar arguments is used for $u = b$ or $u = c$.

Now, let us assume that for some $u \in \{a, b, c\}^+$

$$\mathrm{TC}' \vdash \forall x (x \subseteq \underline{u} \iff \bigvee_{w \subseteq u} x = \underline{w}).$$

and consider $u \frown a$. Now, we work in TC′. Let us assume that $x \subseteq \underline{u} \frown \alpha$. If $x = \underline{u} \frown \alpha$ then there is nothing to prove. So, let us consider three remaining cases:

1. $\exists z\, x \frown z = \underline{u} \frown \alpha$,
2. $\exists z\, z \frown x = \underline{u} \frown \alpha$,
3. $\exists z \exists w\, z \frown x \frown w = \underline{u} \frown \alpha$.

Let us consider the first case. Then, by the editor axiom, either $x = \underline{u}$ and $z = \alpha$, and we are done, or there exists w such that

$$x \frown w = \underline{u} \text{ and } z = w \frown \alpha$$

or

$$x = \underline{u} \frown w \text{ and } w \frown z = \alpha.$$

The latter case is impossible by TC3. The only remaining case is when $x \frown w = \underline{u}$ and $z = w \frown \alpha$. In this case $x \subseteq \underline{u}$ and we may use our inductive assumption.

In the second case, $z \frown x = \underline{u} \frown \alpha$, if $x = \alpha$ then we are done. If $x \neq \alpha$, then there is w such that

$$z \frown w = \underline{u} \text{ and } x = w \frown \alpha.$$

Because $z \frown w = \underline{u}$, we have that $w \subseteq \underline{u}$. Thus, by the inductive assumption,

$$\bigvee_{r \subseteq u} w = \underline{r}.$$

It follows that

$$\bigvee_{r \subseteq u} x = \underline{r} \frown \alpha.$$

In the third case either $w = \alpha$ or there is r such that

$$z \frown x \frown r = \underline{u} \wedge w = r \frown \alpha.$$

In both cases $x \subseteq \underline{u}$ and we can use our inductive assumption. □

As a corollary we obtain the following.

Corollary 4 *For each $u, w \in \{a,b,c\}^+$,*

$$\mathrm{TC}' \vdash (\underline{u} \subseteq \underline{w}) \text{ if and only if } u \subseteq w$$

and

$$\mathrm{TC}' \vdash \neg(\underline{u} \subseteq \underline{w}) \text{ if and only if } u \not\subseteq w$$

Proof. Let $u, w \in \{a,b,c\}^+$. By Lemma 3 we can reduce in TC′ all formulae $\underline{u} \subseteq \underline{w}$ to equations between words. Then, by Lemma 2, we can prove or disprove all equations between words in $\{a,b,c\}^+$. □

Now, we can easily prove the theorem on Σ_1–completeness (originally proven in [Grz05]).

Theorem 5 ([Grz05]) TC′ *proves all true (in $\{a,b,c\}^+$) Σ_1–sentences.*

Proof. It is enough to show the theorem only for Δ_0–sentences. This follows from the fact that each element of $\{a,b,c\}^+$ has its name in TC′.

The proof is by induction on the complexity of a formula $\varphi(\underline{r_1}, \ldots, \underline{r_k})$, where φ is Δ_0 and $r_1, \ldots, r_k \in \{a,b,c\}^+$. For basic cases, $\underline{u} = \underline{w}$, $\neg(\underline{u} = \underline{w})$, $\underline{u} \subseteq \underline{w}$ and $\neg(\underline{u} \subseteq \underline{w})$ one should use Lemma 2 and Corollary 4.

We consider the hardest case when φ is of the form $\forall x \subseteq \underline{u}\, \psi(x, \underline{r_1}, \ldots, \underline{r_k})$ for $u, r_1, \ldots, r_k \in \{a,b,c\}^+$. For this case we can write φ in the following equivalent form using Lemma 3:

$$\bigvee_{w \subseteq u} \psi(\underline{w}, \underline{r_1}, \ldots, \underline{r_k}).$$

Now, it is enough to observe that, for each $w \subseteq u$, our inductive assumption holds for $\psi(\underline{w}, \underline{u_1}, \ldots, \underline{u_k})$. □

3.2 The construction of the ω–type ordering

Now, we present the main new ingredient of this work. We show how to define the ω–type ordering on $\{a,b\}^+$ in such a way that its properties will be provable in TC′. The inspiration for the formula $\varphi_<(x,y)$ which defines the ordering $<$ is from the article by Quine, [Qui46]. However, the constructions of [Qui46] are of semantical character and work in the standard model. We put the main stress on the provability of some properties of $\varphi_<$ in a weak theory TC′.

Definition 6 *Let* $\{u_i\}_{i\in\omega}$ *be the enumeration of words from* $\{a,b\}^+$ *in the ordering* $<$. *The witness for a word* $u = u_i$ *is the word of the form*

$$c\frown u_0\frown c\frown u_1\frown c\frown u_2\frown \ldots \frown c\frown u_{i-1}\frown c\frown u_i\frown c.$$

We denote the witness for u_i *by* w_i.

We also want to provide a recursive definition of the witness w_i for a word u_i. A witness for $u_0 = a$ is $w_0 = cac$ and the witness for u_{i+1} is a word $w_i\frown u_{i+1}\frown c$, where w_i is a witness for u_i.

Now, we define the formula $\mathrm{Next}(z,x,y,w)$ which states that x and y are successive parts of w such that $x \in \{a\}^+$, $y \in \{b\}^+$, $cxc \subseteq w$ and $cyc \subseteq w$ and such that there is no word in w of the form csc, for $s \in \{a\}^+ \cup \{b\}^+$, between x and y. Moreover, to fix a position of x in w we use an additional word z such that $z\frown x \subseteq_e w$. Thus, x is a subword of w which starts just after z.

Definition 7 *Let the formula* $\mathrm{Next}(z,x,y,w)$ *be the following*

$$\alpha(x) \wedge \beta(y) \wedge zx \subseteq_e w \wedge (z = \gamma \vee \exists t \subseteq z(t\gamma = z)) \wedge zx\gamma \subseteq_e w \wedge$$

$$\{zx\gamma y\gamma \subseteq_e w \vee \exists t \subseteq w[zx\gamma t\gamma y\gamma \subseteq_e w \wedge$$
$$(\forall s{:}\alpha\beta(y))\,(\gamma s\gamma \subseteq \gamma t\gamma \Rightarrow (\neg\alpha(s) \wedge \neg\beta(s)))]\}.$$

Now, we define a formula $\mathrm{Wit}(x,y)$ which defines a relation "y is the witness for x".

Definition 8 *The formula* $\mathrm{Wit}(x,y)$ *is the following formula*

$$\begin{aligned}
&(x = \alpha \wedge y = \gamma\alpha\gamma) \vee (x = \beta \wedge y = \gamma\alpha\gamma\beta\gamma)\vee\\
&\{\alpha\beta(x) \wedge x \neq \alpha \wedge x \neq \beta \wedge \gamma\alpha\gamma\beta\gamma \subseteq_e y \wedge \exists z \subseteq y(z\gamma x\gamma = y \wedge \neg(x \subseteq z))\wedge\\
&\quad \forall z \subseteq y(\forall z_1{:}\alpha\beta(z_1))(\forall z_2{:}\alpha\beta(z_2))(z\gamma z_1\gamma z_2\gamma \subseteq_e y \Rightarrow \mathrm{Succ}(z\gamma, z_1, z_2, y))\wedge\\
&\forall z \subseteq y(\forall z_1{:}\alpha\beta(z_1))((z\gamma z_1\gamma \subseteq_e y \wedge z_1 \neq x) \Rightarrow\\
&\qquad\qquad (\exists z_2{:}\alpha\beta(z_2))(z\gamma z_1\gamma z_2\gamma \subseteq_e y \wedge \mathrm{Succ}(z\gamma, z_1, z_2, y)))\},
\end{aligned}$$

where $\mathrm{Succ}(z,z_1,z_2,y)$ *states (with the help of* y*) that* z_2 *is a successor of* z_1

in the ordering $<$*. It assumes that* $zz_1\gamma z_2 \subseteq_e y$*. It has the form*

$$
\begin{aligned}
&(z_1 = \alpha \wedge z_2 = \beta)\vee \\
&\exists u \subseteq z_1(u\alpha = z_1 \wedge u\beta = z_2)\vee \\
&(\beta(z_1) \wedge \exists s \subseteq_e z\, \exists t \subseteq z(\mathrm{Next}(s,t,z_1,y) \wedge z_2 = \alpha t))\vee \\
&\exists u \subseteq z_1(\beta(u) \wedge \alpha u = z_1 \wedge \\
&\qquad \exists s \subseteq_e z\, \exists t \subseteq w(\alpha(t) \wedge \mathrm{Next}(s,t,u,w) \wedge z_2 = \beta t)))\vee \\
&\exists u \subseteq z_1(\beta(u) \wedge \exists r \subseteq z_1(r\alpha u = z_1 \wedge \\
&\qquad \exists s \subseteq_e z\, \exists t \subseteq z(\alpha(t) \wedge \mathrm{Next}(s,t,u,w) \wedge z_2 = r\beta t))).
\end{aligned}
$$

Before we comment on formulae Wit and Succ we present a simple lemma which will be usefull in our analysis.

Lemma 9 *Let* $u, w \in \{a,b,c\}^+$ *such that* $(\{a,b,c\}^+, \frown, a, b, c) \models \mathrm{Wit}[u,w]$*. Then, for all* $s \in \{a,b,c\}^+$ *and for all* $i, j > 0$ *such that* $(\{a,b,c\}^+, \frown, a, b, c) \models \mathrm{Next}[s, a^i, b^j, w]$ *it holds that* $i = j$*.*

Proof. Let us assume that $(\{a,b,c\}^+, \frown, a, b, c) \models \mathrm{Wit}[u,w]$. We prove by induction on the length of s that for all $i, j > 0$, if $(\{a,b,c\}^+, \frown, a, b, c) \models \mathrm{Next}[s, a^i, b^j, w]$ then $i = j$.

If the length of s is 1 then $s = c$ and, by the first line of Wit, $i = j = 1$.

Now, let $s \subseteq_e w$ be such that $(\{a,b,c\}^+, \frown, a, b, c) \models \mathrm{Wit}[s, a^i, b^j, w]$ and let us assume that the lemma holds for all $s' \subseteq_e w$ such that the length of s' is less than s.

There are words $x_1, \ldots, x_n \in \{a,b\}^+ - (\{a\}^+ \cup \{b\}^+)$ such that

$$sa^i cx_1c \ldots cx_n cb^j c \subseteq_e w.$$

Let $x_0 = a^i$ and $x_{n+1} = b^j$. By the third line of the formula Wit, for each $0 \leq k \leq n$,

$$(\{a,b,c\}^+, \frown, a, b, c) \models \mathrm{Succ}[sx_0c \ldots cx_{k-1}c, x_k, x_{k+1}, w]. \qquad (1)$$

Then, by our inductive assumption, for each $s' \subseteq_e s$ such that $s' \neq s$, if

$$(\{a,b,c\}^+, \frown, a, b, c) \models \mathrm{Next}[s', a^r, b^s, w]$$

then $r = s$. It follows that the only case in which the lengths of x_k and x_{k+1} in (1) may be different is described by the third line of the formula Succ. But this line never holds because for each $0 \leq k \leq n$, $x_{k+1} \notin \{a\}^+$. Thus, the lengths of $x_0, x_1, \ldots, x_{n+1}$ are equal and, in consequence, $i = j$. $\square$

Now, let us comment a bit on $\mathrm{Succ}(z, z_1, z_2, y)$. In the first line we just consider the case which is a kind of the starting point. In the second line of $\mathrm{Succ}(z, z_1, z_2, y)$ we consider the simple situation when z_1 is a word which ends with the letter a. Then, z_2 has to be the same word but with the last a changed to b. Then, we consider the situation when z_1 consists only of letters b and we find, using the formula $\mathrm{Next}(s, t, z_1, y)$, the word t which has the same length as z_1 and consists only of a's (here we need Lemma 9). In this situation z_2 is just t extended by one letter a. In the fourth and the fifth line we consider the situation when z_1 is of the form ab^n that is when it is the letter a followed by some number of b's. Then, z_2 has the form ba^n. The last lines are just a generalization of this case to the word z_1 of the form rab^n, where $r \in \{a, b\}^+$. Let us remark that we have to consider these cases separately because we have no empty word in our universe.

The formula $\mathrm{Wit}(x, y)$ is Δ_0 thus TC' proves all true instances of $\mathrm{Wit}(\underline{u}, \underline{w})$, for $u, w \in \{a, b\}^+$. However, we need the following stronger statement.

Lemma 10 *For all* $u \in \{a, b\}^+$,

$$\mathrm{TC}' \vdash \exists^{=1} w \mathrm{Wit}(\underline{u}, w).$$

Proof. Let $u = u_i$ in $<$–enumeration and let w_i be a witness for u. Then, since $\mathrm{Wit}(\underline{u_i}, \underline{w_i})$ is a true Δ_0–formula we have

$$\mathrm{TC}' \vdash \mathrm{Wit}(\underline{u_i}, \underline{w_i}).$$

Now, let t be a new constant. Then, by induction on $k < i$, we can prove the following statement

$$\mathrm{TC} + \mathrm{Wit}(\underline{u_i}, t) \vdash \exists r(\underline{w_k} \frown r = t).$$

Then, by the last line of the formula $\mathrm{Wit}(x, y)$ we have

$$\underline{w_i} = t \vee \exists r(\underline{w_i} \frown r = t).$$

However the second disjunct, $\exists r(\underline{w_i} \frown r = t)$, is impossible by the following argument. In the second line of the formula $\mathrm{Wit}(x, y)$ we state that y ends with $\gamma x \gamma$ and that there is no x before this occurrence. Thus, if $\mathrm{Wit}(\underline{u_i}, t)$ then

$$\exists z(z \gamma \underline{u_i} \gamma = t \wedge \neg(\underline{u_i} \subseteq z)).$$

But, we know that a witness for u_i is an initial segment of t and that this witness ends with a word $\gamma \underline{u_i} \gamma$. So, the only possibility is that $t = \underline{w_i}$. $\square$

Definition 11 *We write a formula $\varphi_<(x,y)$ which defines the $<$ ordering:*

$$\exists z \exists w(\mathrm{Wit}(x,z) \wedge \mathrm{Wit}(y,w) \wedge \exists r(z \frown r = w)).$$

We show that each finite fragment of the ordering $<$ which is below some $u \in \{a,b\}^+$ is properly described in TC$'$ by the formula $\varphi_<(x,y)$.

Lemma 12 *For all $u \in \{a,b\}^+$,*

$$\mathrm{TC}' \vdash (\forall x{:}\alpha\beta(x))(\varphi_<(x,\underline{u}) \iff \bigvee_{r<u} x = \underline{r}).$$

Proof. The direction from the right to the left is obvious. For the other direction let us assume that $\varphi_<(x,\underline{u})$. But then there is a witness z for x and there is r such that $z \frown r = \underline{w}$, where w is the unique witness for u. Thus, x has to be a subword of w, since z ends with $\gamma x \gamma$. But subwords of $\underline{w}$ from $\{a,b\}^+$ which occur in $\underline{w}$ before $\gamma \underline{u} \gamma$ are words less than $\underline{u}$. Thus, $\bigvee_{r<u} x = \underline{r}$. □

The important fact in the essential undecidability proof of a given arithmetical theory T is often the following:

$$\text{for each } n \in \omega,\ T \vdash \forall x(x < \underline{n} \vee x = n \vee \underline{n} < x),$$

where $\underline{n}$ is the term for the number n. Unfortunately, we cannot prove that for any $u \in \{a,b\}^+$, $\mathrm{TC}' \vdash \forall x(\varphi_<(x,\underline{u}) \vee x = \underline{u} \vee \varphi_<(\underline{u},x))$. Indeed, in some nonstandard models M for TC$'$ there are elements d for which there is no witness e such that $M \models \mathrm{Wit}(d,e)$. Such models can be constructed from the models for the arithmetic $I\Delta_0 + \neg\exp$.[2] Since this line of proof cannot be carried out we take the second option and we define within our universe the set of words for which there are witnesses.

Definition 13 *Let* $\mathrm{HasWit}(x)$ *be the formula* $\exists y\, \mathrm{Wit}(x,y)$.

By Lemma 10, for each $u \in \{a,b\}^+$, $\mathrm{TC}' \vdash \mathrm{HasWit}(\underline{u})$. Moreover, we can prove that words x which satisfy $\mathrm{HasWit}(x)$ have good properties in our ordering.

[2] Indeed, we can treat the elements of a given model $M \models I\Delta_0$ as words over some fixed k–ary alphabet, e.g. 0 could be the empty word, 1 the word a, 2 the word b, 3 is the word aa, etc. Then, the concatenation operation is definable by a Δ_0 formula and has the rate of growth of multiplication (see e.g. [HP93]). However, it could be proven, in $I\Delta_0$, that if a number w interprets a witness for a number u, then it has to be exponentially bigger than u. Thus, if our model does not satisfy the totality of exp then not all its elements will have witnesses.

Theorem 14 *For each* $u \in \{a,b\}^+$,

$$\mathrm{TC}' \vdash \forall x(\mathrm{HasWit}(x) \Rightarrow (\varphi_<(x,\underline{u}) \vee x = \underline{u} \vee \varphi_<(\underline{u},x))).$$

Proof. Let $u \in \{a,b\}^+$ be the i–th word in our ω–type enumeration, that is $u = u_i$. Then, for $k \leq i$, the word $w_k \in \{a,b,c\}^+$ is, by Lemma 10, the unique word such that

$$\mathrm{TC}' \vdash \mathrm{Wit}(\underline{u_k}, \underline{w_k}).$$

Now, let us assume that $\mathrm{HasWit}(x)$ and that w is such that $\mathrm{Wit}(x,w)$. Now, to prove the theorem we need to show in TC' that

$$\varphi_<(x,\underline{u}) \vee x = \underline{u} \vee \varphi_<(\underline{u},x).$$

So, we assume that $\neg x = \underline{u}$ and $\neg\varphi_<(x,\underline{u})$. By Lemma 12 this is equivalent to

$$\bigwedge_{k\leq i} \neg x = \underline{u_k}.$$

To finish the proof we need to show that $\varphi_<(\underline{u},x)$ what is equivalent to

$$\exists z(\underline{w_i} \frown z = w).$$

In order to do this, we prove by induction on k, that for all $k \leq i$,

$$\exists z(\underline{w_k} \frown z = w). \tag{2}$$

Of course we have no induction axioms among axioms of TC'. However, the induction we need involves only finitely many steps (to be exact i steps). Thus, we can carry out this reasoning within TC'.

Firstly, we rule out some easy cases. If $u = \underline{u_0} = \alpha$ and $x \neq \underline{u}$ then (2) follows from the first two lines of the formula Wit. Indeed, in this case either $w = \gamma\alpha\gamma\beta\gamma$ or $\gamma\alpha\gamma\beta\gamma \subseteq_e w$. In both cases $\exists z(\gamma\alpha\gamma \frown z = w)$. Thus, we assume that $x \neq \alpha$.

For $k = 0$ and $k = 1$ equation (2) follows just from the definition of the formula $\mathrm{Wit}(x,y)$ (the first two lines of this formula) and from the fact that $x \neq \alpha$ and $x \neq \beta$.

Now, let us assume that for some $k < i$,

$$\exists z(\underline{w_k} \frown z = w).$$

Then, by the last line of a formula $\mathrm{Wit}(x,y)$, for $z_1 = \underline{u_k}$ there is z_2 such that $\mathrm{Succ}(\underline{u_k}, z_2, w)$ and $\underline{w_k} \frown z_2 \frown \gamma \subseteq w$. But, z_2 is determined uniquely by the initial segment of w which is just w_k. So, $z_2 = \underline{u_{k+1}}$. Moreover, it is not the case that $\underline{w_k} \frown z_2 \frown \gamma = w$ since otherwise $x = \underline{u_{k+1}}$, the last word from $\{a,b\}^+$ in w. Thus,

$$\exists z(\underline{w_k} \frown \underline{u_{k+1}} \frown \gamma \frown z = w).$$

But $\underline{w_k} \frown \underline{u_{k+1}} \frown \gamma = \underline{w_{k+1}}$ and we obtain

$$\exists z(\underline{w_{k+1}} \frown z = w)$$

what is just (2) for $k+1$. $\square$

3.3 The main result

In this subsection we prove our main theorem. Our proof is in the spirit of many proofs of the essential undecidability of some theory T. We assume that the reader has some knowledge of basic concepts from the recursion theory as presented in [Rog67] or [Cut80].

Before we state the main theorem we discuss how one can code computations in the standard model for finite words.

Lemma 15 *There is a method of coding Turing machines, their inputs and computations as finite words over an alphabet $\{a,b\}$ such that there are Δ_0 formulae* Accept(x,y,z) *and* Reject(x,y,z) *with the following property: for all words $M, w, C \in \{a,b,c\}^+$,*

$$(\{a,b\}^+, \frown, a, b) \models \mathrm{Accept}(\underline{M}, \underline{w}, \underline{C}) \iff$$
C is an accepting computation of a machine M on the input w

and

$$(\{a,b\}^+, \frown, a, b) \models \mathrm{Reject}(\underline{M}, \underline{w}, \underline{C}) \iff$$
C is a rejecting computation of M on w.

Proof. We give only a sketch of a proof. The reader interested in an example of such a coding may consult e.g. the appendix of [Zda05]. Moreover, let us observe that in the formulation of the lemma we referred to *words* coding computations or Turing machines as to computations and Turing machines. This identification is assumed during the rest of this section. For simplicity, we consider only deterministic Turing machines using only two letter alphabet $\{a,b\}$.

We present the coding for words with more letters than $\{a,b\}$. This is not essential since we can interpret in TC the words over arbitrary finite alphabet and $(\{a,b\}^+, \frown, a, b)$ is, of course, a model of TC.

We can code a Turing machine by a concatenation of words of the form $[[q^n x]DCq^i]$, where [,] and q are letters from the alphabet, $x \in \{a,b\}$, $D \in \{L,R\}$ and $C \in \{a,b\}$. Then, the word $[[q^n x]DCq^i]$ indicates that being in the state n and reading the symbol x the machine writes C on the tape, moves its head left (L) or right (R) and enters the state i. It is straightforward to observe that we can write a Δ_0 formula which checks that a given word M is a concatenation of words as above and that no subword of the form $[q^n x]$ repeats twice (the machine is deterministic).

Next, we can code one state of the computation of a machine M as $\#u_1 q^i u_2\#$, where $\#$ is a letter from the alphabet and $u_1, u_2 \in \{a,b\}^+$ describe the content of the working tape and the string q^i indicates the position of the head and the state of the machine. Again, it is easy to write a Δ_0 formula which defines a set of states. Then, we can code a computation C of M as the word

$$MC_1 \ldots C_m,$$

where M is a code of the machine and C_i is the i-th configuration during the computation C. Let us make a convention that the initial state is always 1, the accepting state is 2 and the rejecting state is 3 and that before M stops it writes a's everywhere on the tape and goes to the beginning of the tape. Thus, the initial configuration on the input w is just a word qw, and the accepting and rejecting configurations are qqa^m and $qqqa^k$, for some $m, k \in \omega$, respectively. These configurations are easily characterized by Δ_0 formulae.

Now, the only difficulty is to write a Δ_0 formula which states that each configuration C_{r+1} is the next configuration after C_r, for $r < m$. Fortunately, M makes only local changes on the tape. Thus the formula which expresses this should simply find a word of the form $[[q^n x]DCq^i]$ in M such that the word $q^n x$ appears in C_r. Then, it should check that C_{r+1} can be constructed from C_r by applying changes according to $[[q^n x]DCq^i]$. The disjunction over all subwords of M of the form $[[q^n x]DCq^i]$ expresses that that C_{r+1} is the next configuration after C_r. This disjunction is easily expressible by an existential quantifiers restricted to subwords of M. □

Let us stress here that in the last lemma we require only that Accept and Reject are Δ_0 formulae which defines the suitable concepts in the standard model for finite words. Nevertheless, by Theorem 5, we can state the following: for all words $M, w, C \in \{a,b\}^+$,

$$\mathrm{TC}' \vdash \mathrm{Accept}(\underline{M}, \underline{w}, \underline{C}) \iff$$
$$C \text{ is an accepting computation of a machine } M \text{ on the input } w$$

and

$$\text{TC}' \vdash \text{Reject}(\underline{M}, \underline{w}, \underline{C}) \iff$$
$$C \text{ is a rejecting computation of } M \text{ on } w.$$

This fact will be used in the proof of Theorem 16.

Let us remark here that although TC' is over the three letters alphabet $\{a, b, c\}$ it proves exactly the same Δ_0 formulae with parameters from $\{a, b\}^+$ as TC. This is so because bounded quantification restricted to words from $\{a, b\}^+$ does not take us from $\{a, b\}^+$. So, in the above equations we may freely use TC or TC'.

Now, we formulate our main theorem.

Theorem 16 TC *is essentially undecidable.*

Proof. We present the proof for the theory TC' which is interpretable in TC. Moreover, we assume

To show the essential undecidability of TC' we follow the usual reasoning. We take M to be a Turing machine such that the sets

$$A = \{u \in \{a, b\}^+ : M \text{ accepts } u\}$$

and

$$B = \{u \in \{a, b\}^+ : M \text{ rejects } u\}$$

are recursively inseparable. We define two formulae, $\gamma_A(x) :=$

$$\exists y(\text{HasWit}(y) \wedge \text{Accept}(\underline{M}, x, y) \wedge \forall z(\varphi_<(z, y) \Rightarrow \neg\text{Reject}(\underline{M}, x, z)))$$

and $\gamma_B(x) :=$

$$\exists y(\text{HasWit}(y) \wedge \text{Reject}(\underline{M}, x, y) \wedge \forall z(\varphi_<(z, y) \Rightarrow \neg\text{Accept}(\underline{M}, x, z))),$$

where Accept and Reject are formulae from Lemma 15. Then, for each $u \in \{a, b\}^+$,

$$\text{if } u \in A \text{ then } \text{TC}' \vdash \gamma_A(\underline{u}) \tag{3}$$

and

$$\text{if } u \in B \text{ then } \text{TC}' \vdash \gamma_B(\underline{u}). \tag{4}$$

We show (3). If $u \in A$ then there is a computation of M which accepts u. Let $C \in \{a, b\}^+$ be the word coding this computation. Then,

$$\text{TC}' \vdash \text{HasWit}(\underline{C}) \wedge \text{Accept}(\underline{M}, \underline{u}, \underline{C}).$$

Moreover, we have that

$$\mathrm{TC}' \vdash \forall x(\varphi_<(x, \underline{C}) \iff \bigvee_{w<C} x = \underline{w}).$$

But for all such $w < C$, w is not a rejecting computation of M on the input u. Thus,

$$\mathrm{TC}' \vdash \forall z(\varphi_<(z, \underline{C}) \Rightarrow \neg\mathrm{Reject}(\underline{M}, \underline{u}, z)).$$

It follows that $\mathrm{TC}' \vdash \gamma_A(\underline{u})$.

In the same way one can prove (4).

Now, we know that γ_A and γ_B represents sets A and B in TC'. However, essential features of these formulae are the following equations

$$\text{if } u \in A, \text{ then } \mathrm{TC}' \vdash \neg\gamma_B(\underline{u}) \tag{5}$$

and

$$\text{if } u \in B, \text{ then } \mathrm{TC}' \vdash \neg\gamma_A(\underline{u}). \tag{6}$$

To show (5) let us assume that $u \in A$ and let C be an accepting computation of M on the input u. We want to show that

$$\mathrm{TC}' \vdash \forall y((\mathrm{HasWit}(y) \wedge \mathrm{Reject}(\underline{M}, \underline{u}, y)) \Rightarrow \exists z(\varphi_<(z, y) \wedge \mathrm{Accept}(\underline{M}, \underline{u}, z))).$$

Now, we work in TC'. Let y be such that $\mathrm{HasWit}(y)$ and $\mathrm{Reject}(\underline{M}, \underline{u}, y)$. It suffices to show that

$$\varphi_<(\underline{C}, y) \wedge \mathrm{Accept}(\underline{M}, \underline{u}, \underline{C}).$$

By the definition of C we have $\mathrm{Accept}(\underline{M}, \underline{u}, \underline{C})$. So, it is enough to show that $\varphi_<(\underline{C}, y)$. Since C is a standard word we have, by Theorem 14,

$$\varphi_<(\underline{C}, y) \vee \underline{C} = y \vee \varphi_<(y, \underline{C}).$$

Then, by Lemma 12,

$$\mathrm{TC}' \vdash \forall x(\varphi_<(x, \underline{C}) \iff \bigvee_{r<C} x = \underline{r}).$$

None of the words $r \leq C$ is a rejecting computation of M on the input u. Moreover, because Reject is a Δ_0 formula, this fact is detected by TC': for all $r \leq C$,

$$\mathrm{TC}' \vdash \neg\mathrm{Reject}(\underline{M}, \underline{u}, \underline{r}).$$

Since we have $\text{Reject}(\underline{M}, \underline{u}, y)$, it follows that y cannot be a word which is less than or equal to C. So, we conclude that $\varphi_<(\underline{C}, y)$. The proof of (6) can be carried out in the very same manner.

Now, we show that there is no consistent T which extends TC' and has a decidable set of consequences. Let us assume, for the sake of contradiction, that we have such a T. Then, let us consider the set

$$S = \left\{u \in \{a, b\}^+ : T \vdash \gamma_A(\underline{u})\right\}.$$

Since T is decidable, S is decidable, too. By (3), $A \subseteq S$ and, by (6) and the fact that T is consistent, $B \cap S = \emptyset$. Thus, we have separated A and B by a recursive set what is impossible by the definition of A and B. We conclude that there is no decidable and consistent extension of TC'. $\square$

4 Final remarks

We have proven that TC is essentially undecidable. Let us observe that if we drop one of the axioms from TC2 to TC5 then we obtain a theory which has a decidable extension. Indeed, if we drop TC5 then we can interpret all axioms in the model for arithmetic of addition without zero $(\omega - \{0\}, +, 1, 1)$. By Presburger theorem this model has a decidable theory. Similarly, if we drop TC4, then this theory is satisfied in the model $(\omega - \{0\}, +, 1, 2)$. Finally, if we drop the editor axiom then such a theory is satisfied in a finite model $(\{a, b, c\}, f, a, b)$, where f is a constant binary function which maps everything to c. We conjecture that also TC without the first axiom has a decidable extension, so TC is an example of a minimal essentially undecidable theory.

We do not know whether our style of defining the ω–type ordering on words poses good properties provably in TC'. Indeed, we showed rather some basic facts which are needed in the proof of Theorem 16. In particular, we would like to ask whether there is a formula $\psi_\leq(x, y)$ such that $\psi_\leq(x, y)$ defines ω–type ordering on $\{a, b\}^+$ in the standard model for concatenation and such that TC' would prove that the set of words for which $\psi_\leq$ defines the linear ordering is closed on concatenation Namely, let $\gamma(x)$ be the following formula

$$\forall z_1 \forall z_2 \forall z_3 \{\bigwedge_{i \leq 3} \psi_\leq(z_i, x) \Rightarrow$$
$$[(\psi_\leq(z_1, z_2) \wedge \psi_\leq(z_2, z_3)) \Rightarrow \psi_\leq(z_1, z_3)) \wedge (\psi_\leq(z_1, z_2) \vee \psi_\leq(z_2, z_1))]\}.$$

Thus, $\gamma(x)$ states that $\psi_{\leq}(y,z)$ defines a linear ordering below x. We want to ask whether there exists such a formula $\psi_{\leq}(y,z)$ for which the set defined by $\gamma(x)$ constructed for this $\psi_{\leq}$ is closed on concatenation, provably in TC′:

$$\mathrm{TC}' \vdash \forall x \forall y((\gamma(x) \wedge \gamma(y)) \Rightarrow \gamma(x \frown y)).$$

We conjecture that the answer is positive.

As for the final remark, in [Grz05] the conjecture was stated that TC is essentially weaker than the Robinson arithmetic Q. Let us formulate this question in a bit more precise form: whether Q is interpretable in TC. Now, we feel that the answer is also positive.

Appendix An outline of the possibility of proving the essential undecidability of TC in another way

In our collaboration on the essential undecidability of TC we both have agreed to use the ω–type ordering $<$ of words, but we differ in the taste of applying it. Konrad Zdanowski wanted to apply the concept of the Turing machine, Andrzej Grzegorczyk would like to continue his analysis of discernible relations started in [Grz05] and tried to use the property of representability of GD relations. Konrad Zdanowski has accomplished his task earlier and his solution is exhibited in section 3. Now we draw up the other way of proving essential undecidability. We assume that the reader has in hand a copy of [Grz05]. Much of notational conventions in this appendix is from this article.

Formally we can proceed in TC using Definition 8 of the present paper, or (perhaps easier) by writing a little different definition based on an intuition of comparison of two words u and w in the manner step by step: 'one symbol after another symbol'. Namely we assume that every word begins by its first symbol and if there are two words u and w:

$$u = u_1 u_2 \ldots u_k \text{ and } w = w_1 w_2 \ldots w_k \ldots w_n$$

then we consider the sequence of pairs of the initial subwords:

$$\langle u_1, w_1 \rangle, \langle u_1 u_2, w_1 w_2 \rangle, \ldots \text{ and so on.}$$

Then u is shorter or equal w (in the length) when there is such a sequence of pairs, in which for any subword of u there is a corresponding subword in w. This sequence of pairs should be defined as a text (word) by means of an inductive condition. To describe this procedure and the whole sequence we need to use a code, especially if we do not want to add a new constant γ. If the two words u, w have the same length then they have a common initial part and we put that $u < w$ when on the first place where they differ, there is the sign α in u and the sign β in w.

In this way of proving of our Essential Undecidability Theorem we also make use of several properties of the relations $<$ and $\leq$, which are or may be proved in TC. These properties bind the relations $<$ and $\leq$ with their defining formulae: $\varphi_<(u, w)$ and $\varphi_\leq(u, w)$. The properties which are necessary are mentioned below as lemmas LA - LE :

- LA For any $m \in \{a, b\}^+$, $TC \vdash \forall u(\varphi_<(u, \underline{m}) \iff \bigvee_{r<m} u = \underline{r})$.
- LB For any $n, m \in \{a, b\}^+$, $n < m \equiv \text{TC} \vdash \varphi_<(\underline{n}, \underline{m})$.
- LC $\text{TC} \vdash \forall y \forall u(\varphi_<(u, y) \Rightarrow \varphi_\leq(u, u))$
- LD For any $m \in \{a, b\}^+$, $\text{TC} \vdash \varphi_\leq(\underline{m}, \underline{m})$.
- LE For any $m \in \{a, b\}^+$, $\text{TC} \vdash \forall u(\varphi_\leq(u, u) \Rightarrow (\varphi_\leq(u, \underline{m}) \vee \varphi_\leq(\underline{m}, u)))$.

Let us recall from [Grz05] that ED is the smallest class of relations (of arbitrary arity) which contains: the binary relation of identity, the ternary relation of concatenation and which is closed under the logical constructions:

1. of the classical propositional calculus,
2. of the operation of quantification relativized to the subtexts of a given text.

Let us note that it follows from the definition that each relation in ED is definable in the standard model for concatenation by a Δ_0 formula.

The class GD satisfies the same conditions and is closed also under the operation of dual quantification. This means that:

If $S, T \in \text{GD}$ and the relation R satisfies two equivalences:

$$R(x, \ldots) \equiv \exists y S(y, x, \ldots) \text{ and } R(x, \ldots) \equiv \forall y T(y, x, \ldots)$$

then also $R \in \text{GD}$. The class GD (of General Discernible relations) in the domain of texts corresponds to the class of General Recursive relations of integers.

We need the following lemma.

Lemma 17 (The Normal Form Lemma) GD *is the class of all relations which may be defined from the relations of the class* ED *by at most one application of the operation of dual quantification. The application of dual quantification may be the last step in defining a given* GD *relation.*

Proof. We shall show that the operation of dual quantification may be always the last step of the defining-process of a GD relation. (In this proof all definitions and symbols are taken from [Grz05].) Suppose that $S, T \in$ GD and are defined by dual quantification:

$$S(x,\ldots) \equiv \forall y A(y,x,\ldots) \text{ and } S(x,\ldots) \equiv \exists y B(y,x,\ldots), \tag{7}$$

$$T(x,\ldots) \equiv \forall y C(y,x,\ldots) \text{ and } T(x,\ldots) \equiv \exists y D(y,x,\ldots). \tag{8}$$

where $A, B, C, D \in$ ED.

A new GD relation R (according to definition 6 (of [Grz05])) may be defined by S and T by using propositional connectives or quantifications limited or dual. Hence we shall consider the following 4 cases.
1. R is defined by negation:

$$R(x,\ldots) \equiv \neg S(x,\ldots).$$

Then by (7) the relation R may be presented in the dual form (according to the de Morgan rules) as follows:

$$R(x,\ldots) \equiv \forall y B(y,x,\ldots) \text{ and } R(x,\ldots) \equiv \exists y A(y,x,\ldots).$$

If $A, B \in$ ED then according to definition 5 also $A, B \in$ ED.
2. R is defined by means of conjunction:

$$R(x,\ldots) \equiv ((S(x,..) \wedge T(x,\ldots)) \tag{9}$$

Then by (7) and (8) R may be presented in the dual form as follows:

$$R(x,\ldots) \equiv \forall y (A(y,x,\ldots) \wedge C(y,x,\ldots)) \tag{10}$$

and

$$R(x,\ldots) \equiv \exists w (\exists y (y \subseteq w \wedge B(y,x,\ldots)) \wedge \exists u (u \subseteq w \wedge D(u,x,\ldots))). \tag{11}$$

The formula (10) follows from (9), (7) and (8) by logic of quantifiers.

The formula (11) follows from (9), (7) and (8) because in the theory of concatenation one can easily prove the following:

$$\forall y \forall u \exists w (y \subseteq w \wedge u \subseteq w),$$

namely $y\frown u$ is such an element w. If $A, B, C, D \in$ ED, then according to definition 5 we have that:

$$\{\langle y, x, \ldots\rangle : A(y, x, ..) \wedge C(y, x, ..)\} \in ED$$

and also:

$$\{\langle w, x, \ldots\rangle : \exists y(y \subseteq w \wedge B(y, x, \wedge)) \wedge \exists u(u \subseteq w \wedge D(u, x, ..)))\} \in \text{ED}.$$

3. R is defined by means of limited quantification:

$$R(x, u, \ldots) \equiv \forall z(z \subseteq u \Rightarrow S(z, x, ..)). \tag{12}$$

According to (7) the above definition (12) of R implies that:

$$R(x, u, \ldots) \equiv \forall z(z \subseteq u \Rightarrow \forall y A(y, z, x, \ldots)) \tag{13}$$

and

$$R(x, u, ..) \equiv \forall z(z \subseteq u \Rightarrow \exists y B(y, z, x, \ldots)). \tag{14}$$

From (13) we easily get the following:

$$R(x, u, \ldots) \equiv \forall w[\forall z(z \subseteq w \Rightarrow \forall y(y \subseteq w \Rightarrow (z \subseteq u \Rightarrow A(y, z, x, \ldots))))] \tag{15}$$

Namely as w we take the element $z\frown y$. The formula (15) shows that R is defined by application of the general quantifier to an ED relation.

To show that R may be presented also as an application of the existential quantifier to an ED relation we shall to use in the metatheory a stronger non-elementary construction.

First let notice that for every $x, \ldots$ and every $z \subseteq u$ there may be infinitely many y such that $B(y, z, x, \ldots)$. We should choose one of them. But we may use the fact that the set of all finite texts is well ordered by the ordering $<$. Hence there is the first such $y^{(z,x,\ldots)}$, that $B(y^{(z,x,\ldots)}, z, x, \ldots)$. For the fixed $u, x, \ldots$ the set of $z \subseteq u$ is finite, thus also the set of tuples $\langle z, x, \ldots\rangle$ for $z \subseteq u$ is finite and the set of $\{y^{(z,x,\ldots)} : z \subseteq u\}$ is also finite. Hence there exist also a text y_0, which contains all texts of the set $\{y^{(z,x,\ldots)} : z \subseteq u\}$, this means such that for any $z \subseteq u$ it is true that $y^{(z,x,\ldots)} \subseteq y_0$. Thus we can assert that:

$$R(x, u, \ldots) \equiv \exists y_0 \forall z(z \subseteq u \Rightarrow \exists y \subseteq y_0\, B(y, z, x, \ldots)). \tag{16}$$

The formula (16) is dual to (15). The formulae (15) and (16) prove that R is defined using ED relations by one operation of dual quantification.
4. R is defined by dual quantification.

Now we suppose that:

$$R(\ldots) \equiv \forall x S(x, \ldots), \tag{17}$$

$$R(\ldots) \equiv \exists x T(x, \ldots), \tag{18}$$

where S and T satisfy the formulae (7) and (8). Then we shall prove that two applications of dual quantification (one (7),(8) and the second (17),(18)) can be condense to one. Indeed from (17) and (7) we get that:

$$R(\ldots) \equiv \forall x \forall y A(y, x, \ldots) \equiv \forall z (\forall x \subseteq z \forall y \subseteq z A(y, x, \ldots)) \tag{19}$$

and from (18) and (8) we infer that:

$$R(\ldots) \equiv \exists x \exists y D(y, x, \ldots) \equiv \exists z (\exists x \subseteq z\, \exists y \subseteq z\, D(y, x, \ldots)). \tag{20}$$

The proofs of (19) and (20) are elementary.

This accomplishes the proof of the lemma. □

Now we can prove the Representability Theorem[3]:

Theorem 18 (Representability Theorem) *If $R \in \mathrm{GD}$, $\mathrm{TC} \subseteq T$ and T is consistent, then R is represented in T.*

Proof. Let $R \in \mathrm{GD}$. According to the Normal Form Lemma there are two relations $A, B \in \mathrm{ED}$ such that for any word x, $R(x) \equiv \forall y A(x, y)$ and $R(x) \equiv \exists y B(x, y)$. Hence, we can also say that:

for each $R \in \mathrm{GD}$ there are two relations $A, B \in \mathrm{ED}$ such that for any word x,

$$R(x) \equiv \exists y A(x, y) \text{ and } \neg R(x) \equiv \exists y B(x, y). \tag{21}$$

According to theorem 12 of [Grz05] there are two formulae Φ and Ψ of TC such that for all x, y:

$$A(x, y) \equiv T \vdash \Phi(\underline{x}, \underline{y}) \text{ and } \neg A(x, y) \equiv T \vdash \neg\Phi(\underline{x}, \underline{y}), \tag{22}$$

$$B(x, y) \equiv T \vdash \Psi(\underline{x}, \underline{y}) \text{ and } \neg B(x, y) \equiv T \vdash \neg\Psi(\underline{x}, \underline{y}).^4 \tag{23}$$

---

[3] We recall that a relation R is said to be represented in the theory T by a formula φ if and only if for all words $x_1, \ldots, x_n$,

$$R(x_1, \ldots, x_n) \equiv T \vdash \varphi(\underline{x_1}, \ldots, \underline{x_n}).$$

[4] Instead of using theorem 12 of [Grz05] one may note that since $A \in \mathrm{ED}$ then there is a Δ_0 formula which defines A in the standard model for finite words. If we choose Φ to be that formula, we will obtain (22) by the fact that the negation of Φ is also a Δ_0 formula which defines the complement of A and by Theorem 5 which gives that all true Δ_0 sentences are decided in TC.

In the same way one can show (23).

Starting from the rule: $R \vee \neg R$ we get, from: (21)–(23), that:

$$\forall x \exists y (A(x,y) \vee B(x,y)).$$

Hence there is also the smallest element $m(x)$ (with respect to the relation $<$ which is of the type ω). Thus, let us define

$$m(x) = \min\{y : A(x,y) \vee B(x,y)\}, \tag{24}$$

and thus $A(x, m(x)) \vee B(x, m(x))$ and

$$\forall x \forall y (y < m(x) \Rightarrow \neg(A(x,y) \vee B(x,y))), \tag{25}$$

$$\exists y\, A(x,y) \equiv A(x, m(x)) \text{ and } \exists y\, B(x,y) \equiv B(x, m(x)). \tag{26}$$

According to definition 7 of [Grz05] and adjusting to the style assumed in the present paper we shall prove that: there is a formula TC such that: for every $x \in \{a,b\}^+$,

$$R(x) \equiv T \vdash \Xi(\underline{x}).$$

For the relation R the corresponding formula may be the following :

$$\Xi(x) = \exists y (\Phi(x,y) \wedge \forall u (\varphi'_<(u,y) \Rightarrow \neg(\Phi(x,u) \vee \Psi(x,u)))),$$

where the formula $\varphi'_<(u,y)$ is the following:

$$(\varphi_{\varphi_\leq}(u,y) \wedge \neg(u = y) \wedge \varphi_\leq(y,y)) \vee (\varphi_\leq(u,u) \wedge \neg\varphi_\leq(y,y)). \tag{$\varphi'_<$}$$

Indeed, for $x \in \{a,b\}^+$ suppose that $R(x)$. Hence from (21), (26) and (22) we get that:

$$T \vdash \Phi(\underline{x}, \underline{m(x)}) \tag{27}$$

From ($\varphi'_<$), lemmas LA, LB, LD and (25), (22), (23) we get that:

$$T \vdash \forall u (\varphi'_<(u, \underline{m(x)}) \Rightarrow \neg(\Phi(\underline{x}, u) \vee \Psi(\underline{x}, u))) \tag{28}$$

The premises (27) and (28) give the implication: $R(x)$ implies $T \vdash \Xi(\underline{x})$.

Now, to prove the converse implication suppose that: $T \vdash \Xi(\underline{x})$. If (on the ground of T) we suppose that:

$$\Phi(\underline{x}, y), \tag{29}$$

$$\forall u (\varphi'_<(u,y) \Rightarrow \neg(\Phi(\underline{x}, u) \vee \Psi(\underline{x}, u)))). \tag{30}$$

Then on the ground of T we may compare the element y with the element which has the name: $\underline{m(x)}$. From (22), (23), (24) we get that:

$$T \vdash (\Phi(\underline{x}, \underline{m(x)}) \vee \Psi(\underline{x}, \underline{m(x)})) \tag{31}$$

Hence from (30) and (31) on the ground of T we get that:

$$\neg\varphi'_<(\underline{m(x)}, y)) \tag{32}$$

On the other hand $m(x) \in \{a,b\}^+$. Then by LD, (32) and ($\varphi'_<$) we get that:

$$\varphi_\leq(\underline{m(x)}, y) \Rightarrow \underline{m(x)} = y, \tag{33}$$

$$\varphi_\leq(y, y). \tag{34}$$

By (33), (34) and LE we have that:

$$\varphi_\leq(y, \underline{m(x)}) \vee \underline{m(x)} = y. \tag{35}$$

But according to LA the first possibility of (35) is contradictory to (25), (22), and (29). Hence it remains that

$$\underline{m(x)} = y. \tag{36}$$

The conclusion (36) which is obtained in the consistent theory T together with the premise (29) give that $T \vdash \Phi(\underline{x}, \underline{m(x)})$. Hence by (26), (22), (21) we get that $R(x)$. This accomplishes the proof of representability. □

Having the Representability Theorem we can repeat Gödel's diagonal procedure exactly in the same way as in the proof of theorem 17 from [Grz05]. Of course now we take T not as true in the standard model but as an arbitrary consistent extension of TC.

References

[Cut80] N. Cutland. *Computability: An Introduction to Recursive Function Theory*. Cambridge University Press, 1980.

[Grz05] Andrzej Grzegorczyk. Undecidability without arithmetization. *Studia Logica*, 1(79):163–230, 2005.

[HP93] P. Hájek and P. Pudlák. *Metamathematics of First–Order Arithmetic*. Springer Verlag, 1993.

[Qui46] W. Quine. Concatenation as a basis for arithmetic. *Journal of Symbolic Logic*, 11:105–114, 1946.

[Rog67] H. Rogers. *Theory of Recursive Functions and Effective Computability*. McGraw-Hill Education, 1967.

[Zda05] K. Zdanowski. *Arithmetics in finite but potentially infinite worlds.* PhD thesis, Warsaw University, 2005. available at `http://www.impan.gov.pl/~kz/files/KZ_PhD.pdf` .