The equational theory of $\langle \mathbb{N}, 0, 1, +, \times, \uparrow \rangle$ is decidable, but not finitely axiomatisable

Roberto Di Cosmo and Thomas Dufour

{dicosmo,dufour}@pps.jussieu.fr
PPS Laboratory (http://www.pps.jussieu.fr)
Université Paris 7
France

Abstract. In 1969, Tarski asked whether the arithmetic identities taught in high school are complete for showing all arithmetic equations valid for the natural numbers. We know the answer to this question for various subsystems obtained by restricting in different ways the language of arithmetic expressions, yet, up to now we knew nothing of the original system that Tarski considered when he started all this research, namely the theory of integers under sum, product, exponentiation with two constants for zero and one.
This paper closes this long standing open problem, by providing an elementary proof, relying on previous work of R. Gurevič, of the fact that Tarski's original system is decidable, yet not finitely aximatisable.
We also show some consequences of this result for the theory of isomorphisms of types.

1 Introduction

Over forty years ago, Tarski asked whether the arithmetic identities taught in high school are complete for showing all arithmetic equations valid for the natural numbers. The answer to this question has occupied many prestigious mathematicians over half a century, that gave the answer for various subsystems, the most intriguing one being the one involving a constant for the number one and the operations of product and exponentiation, for which a complete equational theory exists and also characterizes isomorphism in the typed lambda calculus and in Cartesian Closed Categories, thus exposing interesting connections between number theory, category theory, lambda calculus and type theory.

Yet, up to now we knew nothing of the original system that Tarski considered when he started all this research, namely the equational theory of natural numbers under sum, product, exponentiation and with the two constants for zero and one.

We provide here an elementary proof, relying on previous work of R. Gurevič, of the fact that the equational theory of the arithmetical system with constants 0 and 1 is decidable, but not finitely axiomatisable. By "elementary", we do not mean "simple", but we do want to stress the fact that we proceed by a set of transformations of derivations and formal systems that are well in the tradition of logic and theoretical computer science.

As a first consequence of this result, we can conclude that the theory of isomorphisms of types for bicartesian closed categories is undecidable, a question left open in [BDCF02].

The paper is organized as follows: subsection 1.1 gives a rather comprehensive overview of Tarski's High School Algebra Problem, and subsection 1.2 pinpoints its interest in computer science; section 2 provides a few basic definitions and notations; section 3 provides a proof that the equational theory of $\langle \mathbb{N}, 0, 1, +, \times, \uparrow \rangle$ can be reduced to the equational theory of $\langle \mathbb{N}, 1, +, \times, \uparrow \rangle$, modulo the equations and the conditional equation involving zero that we are taught in high school (figure 2), which in turn gives a decision procedure for the system; section 4 shows that the theory of $\langle \mathbb{N}, 0, 1, +, \times, \uparrow \rangle$ is not finitely axiomatisable, and section 5 concludes.

1.1 Tarski's high school algebra problem.

In 1969, Tarski [DT69] asked if the equational theory $\mathcal{E}$ of the usual arithmetic identities of figure 1 that are taught in high school are complete for the standard model $\langle \mathbb{N}, 1, +, \times, \uparrow \rangle$ of positive natural numbers; i.e. , if they are enough to prove all the arithmetic identities (he considered zero fundamental too, but, probably due to the presence of one conditional equation, he left for further investigation the case of the other equations of figure 2, that we are also taught in high school).

$$(\mathcal{E}_1)\ 1 \times x = x \quad (\mathcal{E}_2)\ x \times y = y \times x \quad (\mathcal{E}_3)\ (x \times y) \times z = x \times (y \times z)$$

$$(\mathcal{E}_4)\ x^1 = x \qquad (\mathcal{E}_5)\ 1^x = 1$$
$$(\mathcal{E}_6)\ x^{y \times z} = (x^y)^z \qquad (\mathcal{E}_7)\ (x \times y)^z = x^z \times y^z$$

$$(\mathcal{E}_8)\ \ x + y = y + x \qquad (\mathcal{E}_9)\ \ (x + y) + z = x + (y + z)$$
$$(\mathcal{E}_{10})\ x \times (y + z) = x \times y + x \times z \qquad (\mathcal{E}_{11})\ x^{(y+z)} = x^y \times x^z$$

Fig. 1. Equations without zero

$$(\mathcal{Z}_1)\ 0 \times x = 0 \quad (\mathcal{Z}_2)\ 0 + x = x \qquad (\mathcal{Z}_3)\ x^0 = 1$$

$$(\mathcal{Z}_4)\ 0^x = 0 \quad (x > 0)$$

Fig. 2. Equations and conditional equation for zero

He conjectured that they were[1], but was not able to prove the result. Martin [Mar72] showed that the identity $(\mathcal{E}_6)$ is complete for the standard model $\langle \mathbb{N}, \uparrow \rangle$ of positive nat-

[1] Actually, he conjectured something stronger, namely that $\mathcal{E}$ is complete for $\langle \mathbb{N}, Ack(n, \_, \_) \rangle$, the natural numbers equipped with a family of generalised binary operators $Ack(n, \_, \_)$ that

ural numbers with exponentiation, and that the identities $(\mathcal{E}_2)$, $(\mathcal{E}_3)$, $(\mathcal{E}_6)$, and $(\mathcal{E}_7)$ are complete for the standard model $\langle \mathbb{N}, \times, \uparrow \rangle$ of positive natural numbers with multiplication and exponentiation. Further, he exhibited the identity

$$(x^u + x^u)^v \times (y^v + y^v)^u = (x^v + x^v)^u \times (y^u + y^u)^v$$

that in the language without the constant 1 is not provable in $\mathcal{E}$. [2] The question was not completely settled by this counterexample, because it is was only a counterexample in the language without a constant for 1, that Tarski clearly considered necessary in his paper, as well as the constant for 0, even if he did not explicitly mention it in his conjecture. In the presence of a constant 1, the following new equations come into play, and allow us to easily prove Martin's equality.

$$1a = a \quad a^1 = a \quad 1^a = 1$$

This problem attracted the interest of many other mathematicians, like Leon Henkin, who focused on the equalities valid in $\langle \mathbb{N}, 0, + \rangle$, and showed the completeness of the usual known axioms (commutativity, associativity of the sum and the zero axiom), and gives a very nice presentation of the topic in [Hen77].

Wilkie [Wil81] was the first to establish Tarski's conjecture in the negative. Indeed, by a proof-theoretic analysis, he showed that the identity

$$(A^x + B^x)^y \times (C^y + D^y)^x = (A^y + B^y)^x \times (C^x + D^x)^y$$

where $A = 1 + x$, $B = 1 + x + x^2$, $C = 1 + x^3$, $D = 1 + x^2 + x^4$ is not provable in $\mathcal{E}$.

Gurevič later gave an argument by an ad hoc counter-model [Gur85] and, more importantly, showed that there is no finite axiomatisation for the valid equations in the standard model $\langle \mathbb{N}, 1, +, \times, \uparrow \rangle$ of positive natural numbers with one, multiplication, exponentiation, and addition [Gur90]. He did this by producing an infinite family of equations such that for every sound finite set of axioms one of the equations can be shown not to follow. Gurevič's identities, which generalize Wilkie's identities, are the following

$$\left(A^x + {B_n}^x\right)^{2^x} \times \left({C_n}^{2^x} + {D_n}^{2^x}\right)^x = \left(A^{2^x} + {B_n}^{2^x}\right)^x \times \left({C_n}^x + {D_n}^x\right)^{2^x}$$

where

$$\begin{aligned} A &= 1 + x \\ B_n &= 1 + x + \cdots + x^{n-1} \;=\; \textstyle\sum_{i=0}^{n-1} x^i \\ C_n &= 1 + x^n \\ D_n &= 1 + x^2 + \cdots + x^{2(n-1)} \;=\; \textstyle\sum_{i=0}^{n-1} x^{2i} \\ n &\geq 3 \quad \text{is odd} \end{aligned}$$

---

extend the usual sum $+$, product $\times$ and exponentiation $\uparrow$ operators. In Tarski's definition, $Ack(0, \_, \_)$ is the sum, $Ack(1, \_, \_)$ is multiplication, $Ack(2, \_, \_)$ is exponentiation (for the other cases see for example [Rog88]).

[2] He also showed that there are no nontrivial equations for $\langle \mathbb{N}, Ack(n, \_, \_) \rangle$ if $n > 2$.

Nonetheless, equality in all these structures, even if not finitely axiomatisable, was shown to be decidable [Mac81,Gur85].[3]

As often happens in number theory, these last results use far more complex tools than simple arithmetic reasoning, as in the case of [HR84], where Nevanlinna theory is used to identify a subclass of numerical expressions for which the usual axioms for $+$, $\times$, $\uparrow$ and 1 are complete.

1.2 Connections with type isomorphisms and applications in library search

Two types A and B in a given language are called *isomorphic* if there exist conversion functions $f : A \to B$ and $g : B \to A$ which are mutual inverses [DC95].

From a practical perspective, type isomorphisms are used as a basis for library search tools of various kind, and one is interested in knowing whether type isomorphisms in the presence of sums are finitely axiomatisable, and whether an efficient decision procedure exists, to incorporate it in library search tools like those described in [Rit90,DC95].

There is a connection between the characterization of type isomorphisms in typed lambda calculi and Tarski's high school algebra problem: for types built out of type constructors chosen amongst the unit, product, and arrow, two types are isomorphic if and only if their associated arithmetic expressions (obtained by interpreting the unit by the number one, product by multiplication, and arrow by exponentiation) are equal in the standard model of natural numbers. In this case, type isomorphism (and numerical equality) is finitely axiomatisable and decidable; hence so is the equational theory of isomorphisms in cartesian closed categories. Zibin, Gil and Considine [ZGC03] provide very efficient $O(n \log n)$ decision procedures for this system. In the same vein, Soloviev [Sol93], gave a complete axiomatisation of isomorphisms in symmetric monoidal closed categories, and Dosen and Petric [DP97] provided the arithmetic structure that exactly corresponds to these isomorphisms.

Balat, Fiore and the first author investigated the question as to whether such correspondence was limited to the case of the well-behaved unit, product, and arrow type constructors and, in particular, if it could be extended to more problematic types involving the empty type and the sum type constructor [BDCF02,BDCF04], with the following fundamental result:

> Gurevič's identities are indeed type isomorphisms, and one can then show that the theory of type isomorphisms in the presence of the product, arrow, and sum type constructors, and the unit type is not finitely axiomatisable.

Since nothing was known for arithmetic equality in the presence of zero, one could not conclude the non finite axiomatisability of type isomorphisms in the presence of the empty type: it could be the case that, with the zero added, the Gurevič's identities collapse into a finite set of equations.

[3] For the interested reader, here is how the decision procedure works: from the size of the equation that has to be verified, it is possible to derive an upper bound; if the two sides coincide for all values of the variables up to this upper bound, then they coincide everywhere.

Worse than that: even if every isomorphism does produce a numerical equality[4], when the zero constant is added, there is a numerical equality which is not an isomorphism, hence type isomorphism and arithmetic equality no longer coincide in the presence of zero.

With the results of this paper, we can conclude that the family of Gurevič's identities does not collapse in the presence of zero, and hence, even with the empty set, type isomorphisms are not finitely axiomatisable.

2 Definitions and notations

Definition 1. *The terms in* $\langle \mathbb{N}, 0, 1, +, \times, \uparrow \rangle$ *are* $t ::= x \,|\, 0 \,|\, 1 \,|\, t + t \,|\, t \times t \,|\, t^t$*, and the terms in* $\langle \mathbb{N}, 1, +, \times, \uparrow \rangle$ *are* $\bar{t} ::= x \,|\, 1 \,|\, \bar{t} + \bar{t} \,|\, \bar{t} \times \bar{t} \,|\, \bar{t}^{\bar{t}}$*, where* x *is a metavariable denoting a countably infinite set of variables* $\mathcal{V} = \{x, y, z, \dots\}$*. We will use the letters* $t, s, u, \dots$ *for the terms of* $\langle \mathbb{N}, 0, 1, +, \times, \uparrow \rangle$*.*

Definition 2. *Let* t *be a term of* $\langle \mathbb{N}, 0, 1, +, \times, \uparrow \rangle$*, we write* $\mathrm{Var}(t)$ *for the set of its variables.*

Definition 3 (Context). *A* ***context*** *– written* $\Gamma, \Delta, \dots$ *– is a formula of the propositional logic with the operators* $\neg, \vee, \wedge$*, in which the atomic formulas are the "*$x = 0$*", for* $x \in \mathcal{V}$*. We also include* $\top$ *(true), and* $\bot$ *(false).*

Definition 4 (Exhaustive context). *Given* $A, B \subset \mathcal{V}$ *two finite sets, we let* $[A, B]$ *be the following context:*

$$[A, B] = \bigwedge_{x \in A} x = 0 \wedge \bigwedge_{x \in B \setminus A} \neg x = 0$$

A context Γ *will be said to be* ***exhaustive for*** t *(a term) if there exist two finite sets* A *and* $B \supset \mathrm{Var}(t)$ *such that* Γ *is equivalent – as a logical proposition – to* $[A, B]$*.*

Definition 5 (Syntactically positive terms). *A term* t *in* $\langle \mathbb{N}, 0, 1, +, \times, \uparrow \rangle$ *is said to be* ***syntactically positive in context*** Γ *when* Γ *is exhaustive for* t *and* $\forall x \in \mathrm{Var}(t)$*,* $\Gamma \Rightarrow \neg x = 0$*.*

Definition 6. *Let* φ *be a valuation (*$\varphi : \mathcal{V} \to \mathbb{N}$*). We write* $[\![t]\!]_\varphi$ *the interpretation of* t *relative to this valuation.*

Definition 7. *Let* Γ *be a context and* φ *a valuation, we write* $[\![\Gamma]\!]_\varphi$ *the logical value defined as follows:*

$$[\![x = 0]\!]_\varphi = \begin{cases} \top \text{ if } \varphi(x) = 0 \\ \bot \text{ if } \varphi(x) \neq 0 \end{cases}$$

$$[\![\Gamma \wedge \Delta]\!]_\varphi = [\![\Gamma]\!]_\varphi \wedge [\![\Delta]\!]_\varphi, \quad [\![\Gamma \vee \Delta]\!]_\varphi = [\![\Gamma]\!]_\varphi \vee [\![\Delta]\!]_\varphi, \quad [\![\neg\Gamma]\!]_\varphi = \neg[\![\Gamma]\!]_\varphi.$$

A valuation φ *will be said to* ***satisfy*** *a context* Γ *if* $[\![\Gamma]\!]_\varphi = \top$*.*

[4] A type isomorphism can be turned into a bijection of finite sets, and hence into an equation between cardinalities, expressed using the arithmetic languages; hence all isomorphisms are arithmetical equalities.

3 $\langle \mathbb{N}, 0, 1, +, \times, \uparrow \rangle$ as an extension of $\langle \mathbb{N}, 1, +, \times, \uparrow \rangle$

Introduction In this section we create a formal system (called *ZP*) that produces "conditional equations" of terms in $\langle \mathbb{N}, 0, 1, +, \times, \uparrow \rangle$. That system starts with the equalities in $\langle \mathbb{N}, 1, +, \times, \uparrow \rangle$ and builds on them. The semantics of this system will be proved to relate to equality in $\langle \mathbb{N}, 0, 1, +, \times, \uparrow \rangle$ in a fashion that allows us to deduce, first the relationship between equality in $\langle \mathbb{N}, 0, 1, +, \times, \uparrow \rangle$ and in $\langle \mathbb{N}, 1, +, \times, \uparrow \rangle$, second that equality in $\langle \mathbb{N}, 0, 1, +, \times, \uparrow \rangle$ is decidable.

Definition 8 (The *ZP* formal system). *We define a formal system, which we will call ZP. It contains two statements: "$\Gamma \vdash t \doteq s$" and "$\Gamma \vdash t$ positive", which are inferred as described in figure 3.*

Remark Informally, these statements mean: "If Γ holds, then t and s are equal (respectively: t is positive)". Proving this is actually the point of proposition 2.

Proposition 1. *Let t be a term, and Γ a context which is exhaustive for t. There are a term t' and a derivation that proves $\Gamma \vdash t \doteq t'$, where one of the following conditions holds:*

1. $t' = 0$
2. *t' is syntactically positive in context Γ.*

PROOF: The proof is essentially a reduction by induction on t and can be seen in appendix A.1. □

Lemma 1 *Let t be a term which is syntactically positive term in context Γ. There exists a derivation of the statement $\Gamma \vdash t$ positive.*

PROOF: With the fact that being syntactically positive extends to sub-terms, plus rules N0, N1, N3-N5, we have an obvious proof by structural induction. □

Proposition 2 (Semantics of the statements of *ZP*). *The following statements hold:*

$$\Gamma \vdash t \doteq s \Leftrightarrow \forall \varphi \text{ satisfying } \Gamma \ [\![t]\!]_\varphi = [\![s]\!]_\varphi \tag{1}$$

$$\Gamma \vdash t \text{ positive} \Leftrightarrow \forall \varphi \text{ satisfying } \Gamma \ [\![t]\!]_\varphi \neq 0 \tag{2}$$

PROOF: The left-to-right implications in (1) and (2) will be proved simultaneously by structural induction on the derivation of the statement. This is shown in appendix A.2.

In order to prove the right-to-left implication in (1), we will begin by stating that it is enough to prove it under the following stronger hypotheses:

For all $A \subset B = \mathrm{Var}(t + s)$,

$$\forall \psi \text{ satisfying } [A, B] \ [\![t]\!]_\psi = [\![s]\!]_\psi \Rightarrow [A, B] \vdash t \doteq s$$

This is supported by the four quite simple facts about contexts and valuations that can be found in appendix A.3.

$$\boxed{\text{E0}}\ \frac{}{\Gamma \vdash t \doteq s}\quad \text{If condition (†) holds}$$

(†) : t and s are syntactically positive in context Γ, and $t = s$ in $\langle \mathbb{N}, 1, +, \times, \uparrow \rangle$[5].

$$\boxed{\text{E1}}\ \frac{}{x = 0 \vdash x \doteq 0}$$

$$\boxed{\text{E2}}\ \frac{}{\top \vdash t + 0 \doteq t} \qquad \boxed{\text{E2'}}\ \frac{}{\top \vdash 0 + t \doteq t}$$

$$\boxed{\text{E3}}\ \frac{}{\top \vdash t \times 0 \doteq 0} \qquad \boxed{\text{E3'}}\ \frac{}{\top \vdash 0 \times t \doteq 0}$$

$$\boxed{\text{E4}}\ \frac{}{\top \vdash t^0 \doteq 1} \qquad \boxed{\text{E5}}\ \frac{\Gamma \vdash t \text{ positive}}{\Gamma \vdash 0^t \doteq 0}$$

$$\boxed{\text{E6}}\ \frac{\Gamma \vdash t \doteq s}{\Delta \vdash t \doteq s}\quad \text{If } \Delta \Rightarrow \Gamma$$

$$\boxed{\text{E7}}\ \frac{\Gamma \vdash t \doteq s \quad \Delta \vdash t \doteq s}{\Gamma \vee \Delta \vdash t \doteq s}$$

$$\boxed{\text{N0}}\ \frac{}{\neg x = 0 \vdash x \text{ positive}} \qquad \boxed{\text{N1}}\ \frac{}{\top \vdash 1 \text{ positive}}$$

$$\boxed{\text{N2}}\ \frac{\Gamma \vdash t \text{ positive} \quad \Gamma \vdash t \doteq s}{\Gamma \vdash s \text{ positive}} \qquad \boxed{\text{N3}}\ \frac{\Gamma \vdash t \text{ positive}}{\Gamma \vdash t + s \text{ positive}}$$

$$\boxed{\text{N4}}\ \frac{\Gamma \vdash t \text{ positive} \quad \Gamma \vdash s \text{ positive}}{\Gamma \vdash t \times s \text{ positive}} \qquad \boxed{\text{N5}}\ \frac{\Gamma \vdash t \text{ positive} \quad \Gamma \vdash s \text{ positive}}{\Gamma \vdash t^s \text{ positive}}$$

$$\boxed{\text{N6}}\ \frac{\Gamma \vdash t \text{ positive}}{\Delta \vdash t \text{ positive}}\quad \text{If } \Delta \Rightarrow \Gamma$$

$$\boxed{\text{N7}}\ \frac{\Gamma \vdash t \text{ positive} \quad \Delta \vdash t \text{ positive}}{\Gamma \vee \Delta \vdash t \text{ positive}}$$

$$\boxed{\text{REFL}}\ \frac{}{\top \vdash t \doteq t} \qquad \boxed{\text{SYM}}\ \frac{\Gamma \vdash t \doteq s}{\Gamma \vdash s \doteq t} \qquad \boxed{\text{TRANS}}\ \frac{\Gamma \vdash t \doteq s \quad \Gamma \vdash s \doteq u}{\Gamma \vdash t \doteq u}$$

$$\boxed{\text{CONT}}\ \frac{\Gamma \vdash t \doteq s}{\Gamma \vdash C[t] \doteq C[s]}\quad C[\cdot] \text{ denotes a context with only one placeholder}^6$$

Fig. 3. Rules of inference of the statements "$\Gamma \vdash t \doteq s$" and "$\Gamma \vdash t$ positive" (ZP)

Let us now prove this restricted property: $[A, B]$ is exhaustive for t and s so proposition 1 stipulates that there exist some terms t' and s', which are both 0 or syn-

[5] Since t and s are syntactically positive, they contain no 0, so it is meaningful to ask whether they are equal as terms of $\langle \mathbb{N}, 1, +, \times, \uparrow \rangle$.

[6] Here "context" has its usual meaning with terms of a first-order language. Such a context is a term of the language with an extra 0-ary symbol $[\cdot]$ called placeholder, which can be seen as a

tactically positive in context $[A, B]$, such that $[A, B] \vdash t \doteq t'$ and $[A, B] \vdash s \doteq s'$. Then let ψ be a valuation that satisfies $[A, B]$, we have $[\![t]\!]_\psi = [\![t']\!]_\psi$ and $[\![s]\!]_\psi = [\![s']\!]_\psi$, so $[\![t']\!]_\psi = [\![s']\!]_\psi$.

With what we proved earlier in this proposition (namely the left-to-right implications), we can state that either:

- $t' = 0$ and $s' = 0$, and $[A, B] \vdash t' \doteq s'$ is derived with REFL, or
- t' and s' are both syntactically positive. Let φ be a valuation with values in $\mathbb{N} \setminus \{0\}$, there exists a valuation ψ satisfying $[A, B]$ such that $[\![t']\!]_\psi = [\![t']\!]_\varphi$, and $[\![s']\!]_\psi = [\![s']\!]_\varphi$[7]. Hence t' is equal to s' in $\langle \mathbb{N}, 1, +, \times, \uparrow \rangle$, and we have a derivation of $[A, B] \vdash t' \doteq s'$ with rule E0.

Finally, to prove the right-to-left implication in (2), let us notice that it also suffices, reasoning like we just did, to prove this when Γ is exhaustive for t. In that case, proposition 1 implies that there is a term t' such that $\Gamma \vdash t \doteq t'$ and t' is syntactically positive in context Γ[8], so lemma 1 gives us a derivation of $\Gamma \vdash t'$ positive, and with rule N2 a derivation of $\Gamma \vdash t$ positive. □

Corollary 2 *Equality in* $\langle \mathbb{N}, 0, 1, +, \times, \uparrow \rangle$ *is decidable.*

PROOF: It is a known fact that equality in $\langle \mathbb{N}, 1, +, \times, \uparrow \rangle$ is decidable.

Let t and s be two terms of $\langle \mathbb{N}, 0, 1, +, \times, \uparrow \rangle$. Let also $\mathcal{C}$ be the following set of contexts:

$$\mathcal{C} = \{[X, \mathrm{Var}(t + s)] \mid X \subseteq \mathrm{Var}(t + s)\}$$

We contend that $\top \vdash t \doteq s$ if and only if $\forall \Gamma \in \mathcal{C}\ \Gamma \vdash t \doteq s$. This is a direct consequence of proposition 2.

By using proposition 1, we get two new terms t' and s' such that $\Gamma \vdash t \doteq s$ is equivalent to $\Gamma \vdash t' \doteq s'$. Since these new terms are either 0 or syntactically positive in context Γ, the new equality is either obviously true or false, or an equality in $\langle \mathbb{N}, 1, +, \times, \uparrow \rangle$. We have reduced deciding an equality in $\langle \mathbb{N}, 0, 1, +, \times, \uparrow \rangle$ to deciding a finite number of equalities in $\langle \mathbb{N}, 1, +, \times, \uparrow \rangle$, therefore equality in $\langle \mathbb{N}, 0, 1, +, \times, \uparrow \rangle$ is decidable. □

Conclusion Eventually, we have displayed a formal system whose derivations prove the equalities of $\langle \mathbb{N}, 0, 1, +, \times, \uparrow \rangle$, which are represented by the statement $\top \vdash t \doteq s$. This statement calls upon equality in $\langle \mathbb{N}, 1, +, \times, \uparrow \rangle$ plus rules depicting the equations: $t + 0 = t$, $t \times 0 = 0$, $t^0 = 1$ and $0^t = 0$ if $t \neq 0$.

---

special variable, and $C[t]$ stands for $C[\forall[\cdot]]$ (usual substitution). For example if $C = x + [\cdot]$ and $t = x^{1+x}$, $C[t] = x + x^{1+x}$.

[7] This is due to the fact that the variables in A can no longer occur in t' or s', since these terms are syntactically positive in context$[A, B]$.

[8] Obviously t' cannot be 0, because of (1).

4 Axioms of equality in $\langle \mathbb{N}, 0, 1, +, \times, \uparrow \rangle$

Introduction Throughout this section (until just before theorem 7, actually) we will make the assumption that equality in $\langle \mathbb{N}, 0, 1, +, \times, \uparrow \rangle$ has a finite system of axioms, our goal being to prove the contrary.

We first need to modify the formal system *ZP*, replacing the equality imported from $\langle \mathbb{N}, 1, +, \times, \uparrow \rangle$ (which appeared in rule E0) with a finite set of axioms. We call ZP_{ax} this new system, which is equivalent to *ZP* under our finite axioms hypothesis.

We will then use our previous results, along with a few new notations, to prove that the axioms of equality in $\langle \mathbb{N}, 0, 1, +, \times, \uparrow \rangle$, once reasonably "projected" to $\langle \mathbb{N}, 1, +, \times, \uparrow \rangle$, form a finite system of axioms for equality in $\langle \mathbb{N}, 1, +, \times, \uparrow \rangle$, which is known to be impossible.

In order to realize this projection, we will evolve the system ZP_{ax} gradually, so that the derivations in ZP_{ax} will come to be transformed (also gradually) into derivations in $\langle \mathbb{N}, 1, +, \times, \uparrow \rangle$.

Definition 9 (The ZP_{ax} formal system). *The formal system we call ZP_{ax} includes the same rules as ZP, except that:*

- *A finite set of axioms $\mathcal{A}_1, \ldots, \mathcal{A}_n$ is added. These axioms are:*

$$\boxed{\mathcal{A}_i}\ \frac{}{\top \vdash l_i \doteq r_i}$$

- *Rule* E0 *is withdrawn.*

Definition 10 (Partial evaluation in a given context). *Given a context Γ, we define a partial function $\Gamma(t)$ for the terms t for which Γ is exhaustive.*

It is defined by structural induction on the term t, as shown in figure 4.

Proposition 3. *Let Γ be a context and t a term such that $\Gamma(t)$ is defined. We contend the following properties hold:*

1. *$\Gamma(t)$ is either 0, or a syntactically positive term (in context Γ);*
2. *If t is syntactically positive in context Γ then $\Gamma(t) = t$;*
3. *If $\Gamma(t) \neq 0$ then $\Gamma \vdash t$ positive can be derived in ZP;*
4. *$\Gamma \vdash \Gamma(t) \doteq t$ can be derived in ZP without* E0*;*
5. *The converse of 3. holds.*

PROOF:

1. This is trivially proved by structural induction.
2. Idem, recalling that being syntactically positive extends to sub-terms.
3. If $\Gamma(t) \neq 0$ then $\Gamma(t)$ is syntactically positive in context Γ, so that the statement $\Gamma \vdash t$ positive can be derived thanks to lemma 1.
4. This goes by structural induction on t. Let us examine further a single case.
   Suppose that $t = s + u$, with $\Gamma(s) \neq 0$ and $\Gamma(u) = 0$. By induction there is a derivation D of $\Gamma \vdash \Gamma(s) \doteq s$, and a derivation D' of $\Gamma \vdash 0 \doteq u$.
   We build the following derivation:

$$\Gamma(0) = 0 \quad \Gamma(1) = 1 \quad \Gamma(x) = \begin{cases} 0 \text{ if } \Gamma \Rightarrow x = 0 \\ x \text{ if } \Gamma \Rightarrow \neg x = 0 \end{cases}$$

$$\Gamma(t+s) = \begin{cases} \Gamma(t) & \text{if } \Gamma(s) = 0 \\ \Gamma(s) & \text{if } \Gamma(t) = 0 \\ \Gamma(t) + \Gamma(s) & \text{otherwise} \end{cases}$$

$$\Gamma(t \times s) = \begin{cases} 0 & \text{if } \Gamma(t) = 0 \text{ or } \Gamma(s) = 0 \\ \Gamma(t) \times \Gamma(s) & \text{otherwise} \end{cases}$$

$$\Gamma(t^s) = \begin{cases} 1 & \text{if } \Gamma(s) = 0 \\ 0 & \text{if } \Gamma(t) = 0 \text{ and } \Gamma(s) \neq 0 \\ \Gamma(t)^{\Gamma(s)} & \text{otherwise} \end{cases}$$

Fig. 4. Partial evaulation of terms in a context Γ

$$\dfrac{\dfrac{\dfrac{(D)}{\Gamma \vdash \Gamma(s) \doteq s}}{\Gamma \vdash \Gamma(s) + 0 \doteq s + 0} \qquad \dfrac{\dfrac{(D')}{\Gamma \vdash 0 \doteq u}}{\Gamma \vdash s + 0 \doteq s + u}}{\dfrac{\Gamma \vdash \Gamma(s) + 0 \doteq s + u}{\Gamma \vdash \Gamma(s) \doteq s + u}}$$

The last step is actually a contraction of E2 and TRANS, written so for improved readability. Since $\Gamma(t) = \Gamma(s)$, this is the derivation we wanted. Other cases are similarly treated (let us notice, although, that when $t = s^u$ with $\Gamma(s) = 0$ and $\Gamma(u) \neq 0$, we need to summon point 3. to get a derivation of $\Gamma \vdash u$ positive).

5. This is a consequence of point 4. and proposition 2. □

Remark This shows that partial evaluation is actually an implementation of the existential result in proposition 1.

Definition 11 (The $ZP^+_{\mathbf{ax}}$ formal system). *The formal system called ZP^+_{ax} is the system ZP_{ax} to which we add the following new axioms $\mathcal{A}^+_1, \ldots, \mathcal{A}^+_n$:*

$$\boxed{\mathcal{A}^+_i} \ \dfrac{}{\Gamma_{\mathcal{A}_i} \vdash \Gamma_{\mathcal{A}_i}(l_i) \doteq \Gamma_{\mathcal{A}_i}(r_i)} \quad \textit{where } \Gamma_{\mathcal{A}_i} = [\varnothing, \mathrm{Var}(l_i + r_i)]$$

Remark The "axioms" $\mathcal{A}^+_i$ can actually be derived in the system ZP_{ax}, as proposition 3 implies that $\Gamma_{\mathcal{A}_i} \vdash \Gamma_{\mathcal{A}_i}(l_i) \doteq l_i$ can be derived in ZP_{ax} (mutatis mutandis r_i).

Definition 12 (Local equality statements). *The statement $\Gamma \vdash t \doteq s$ is said to be **local** if Γ is exhaustive for $t + s$.*

Definition 13. *We define two particular sets of rules:*

$$G_0 = \{\text{E1}, \text{E2}, \text{E2'}, \text{E3}, \text{E3'}, \text{E4}, \text{REFL}\}$$

$$G = G_0 \cup \{\mathcal{A}_1, \ldots, \mathcal{A}_n\}$$

Definition 14 ("L" property). *A derivation D in ZP_{ax} will be said to have the property "**L**" (or to be an **L**-derivation), if the following properties hold:*

L1 *The conclusion of D is $\Delta \vdash t \doteq s$, and this statement is local.*
L2 *Any statement $\Gamma \vdash t' \doteq s'$ occurring in D has one of the following qualities:*
- *$\Gamma = \top$ or $\Gamma = (x = 0)$ and this statement follows immediately a rule in G, or*
- *$\Gamma = \Delta$ (as in **L1**), and this statement is local.*

L3 *No rule* E7 *occurs in D.*
L4 *Rule* E6 *only occurs in D where it follows immediately a rule $R \in G$.*

Conditions **L2** *to* **L4** *are lifted for any part of the derivation "above" an occurrence of rule* E5.

Remark The caution of this last sentence is justified by the possibility of equality statements to appear above an E5, because of rule N2. Practically, in the following proofs by structural induction on derivations, we will never use induction hypotheses when said derivation ends with an E5.

Definition 15 ("EL" property). *Let $G' = G_0 \cup \{\mathcal{A}_1^+, \ldots, \mathcal{A}_n^+\}$. A derivation in ZP_{ax}^+ will be said to have the property "**EL**" (or to be an **EL**-derivation) if it has the properties* **L1** *to* **L4***, where G is replaced with G' in* **L2** *and* **L4***, and the following two extra properties :*

EL1 *No original axiom $\mathcal{A}_i$ occurs in D.*
EL2 *For any statement $\Gamma \vdash t \doteq s$ in D such that $\Gamma(t)$ and $\Gamma(s)$ are defined, $\Gamma(t) = t$ and $\Gamma(s) = s$.*

We now contend that certain derivations (namely those made in contexts where all variables are positive) can be transformed into **L**-derivations, and then into **EL**-derivations, which is the topic of the three next lemmas.

The first of this three lemmas is a plain technicality pertaining to **L**-derivations.

Lemma 3 *Let D be an **L**-derivation of $\Delta \vdash t \doteq s$. Let also A and B be two finite sets of variables that do not occur in Δ. There exists an **L**-derivation of $\Delta \wedge [A, B] \vdash t \doteq s$.*

PROOF: This is actually quite obvious. All that is needed is to replace Δ with $\Delta \wedge [A, B]$ everywhere[9]. It will also be necessary to insert an N6 between the premise and conclusion of any E5. Also, in the (supposedly rare) situation where $\Delta = \top$, it will be necessary to insert an E6 after any rule $R \in G$. □

Lemma 4 *Let D be a derivation of $\Gamma \vdash t \doteq s$ in ZP_{ax} and Δ a context that is exhaustive for t and s, and such that $\Delta \Rightarrow \Gamma$ holds.*

*There exists a context $\Delta' = [\varnothing, A]$ (where the variables in A do not occur in Δ) and an **L**-derivation of $\Delta \wedge \Delta' \vdash t \doteq s$.*

[9] Again, this need not apply to any part of the derivation above an E5.

Remark Since no hypothesis but finiteness is made about A we can safely ignore the case $\Delta = \top$, thanks to lemma 3.

PROOF: We proceed by structural induction on D, and distinguish cases according to the last rule used in this derivation. See appendix A.4. □

Lemma 5 *If $[\varnothing, \mathrm{Var}(t+s)] \vdash t \doteq s$ can be derived in ZP_{ax}, and if no 0 appears in either t or s, there exists a finite set of variables A (whose elements do not occur in $t+s$) and an **EL**-derivation of $\Delta' \vdash \Delta'(t) \doteq \Delta'(s)$ in ZP^+_{ax}, where $\Delta' = [\varnothing, \mathrm{Var}(t+s)] \wedge [\varnothing, A]$.*

PROOF: Proposition 4 yields us an **L**-derivation, call it D, of the statement $\Delta' \vdash t \doteq s$. The **EL**-derivation will be built by structural induction from D. Again we distinguish cases according to the last rule used in D, keeping in mind some structural properties about **L**-derivations. This is done in appendix A.5. □

We will now introduce a last evolution of our formal system before actually going to equality in $\langle \mathbb{N}, 1, +, \times, \uparrow \rangle$.

Definition 16 (The $P_{\mathbf{ax}}$ formal system). *P_{ax} is a sub-system of ZP^+_{ax} which includes the following rules :*

- *the axioms $\mathcal{A}^+_1, \ldots, \mathcal{A}^+_n$,*
- REFL, SYM, TRANS, CONT,
- E6.

Remarque Clearly any statement which can be derived in P_{ax} can also be derived in ZP_{ax}.

Corollary 6 *With the same hypotheses and notations as in lemma 5, there is a derivation of $[\varnothing, \mathrm{Var}(t+s)] \wedge [\varnothing, A] \vdash t \doteq s$ in P_{ax}. Moreover, no 0 occurs in the terms of this derivation at all.*

PROOF: Clearly the **EL**-derivation granted by lemma 5 is actually a derivation in P_{ax}. The terms of its conclusion have no zeros, and we will prove that if a rule in an **EL**-derivation has no 0 in its conclusion, it can have none in its premise(s).

$\mathcal{A}^+_i$, REFL Those rules have no premises.

SYM, CONT, E6 The terms in the premise are the same as (or subterms of) those in the conclusion.

TRANS A new term can appear in the premise, but since it is partially evaluated it is either syntactically positive or 0. But since it is derived to be equal to the terms of the conclusion, and since these are syntactically positive, the "new" term must also be syntactically positive. □

Theorem 7. *The equational therory of $\langle \mathbb{N}, 0, 1, +, \times, \uparrow \rangle$ cannot derive from a finite set of axioms.*

PROOF: As we said before, we reason *ad absurdum*. Let us then assume that such a finite set of axioms $\{\mathcal{A}_i\}_{i\in\{1,\ldots,n\}}$ exists.

Let us also consider Th the equational theory of $\langle \mathbb{N}, 1, +, \times, \uparrow\rangle$ with the axioms $\{\mathcal{A}_i^+\}_{i\in\{1,\ldots,n\}}$ (as defined previously). Since these axioms are true in ZP_{ax} (which is by hypothesis equivalent to *ZP*), they are true in $\langle \mathbb{N}, 1, +, \times, \uparrow\rangle$ (see proposition 2). So Th only proves equalities that are true in $\langle \mathbb{N}, 1, +, \times, \uparrow\rangle$.

Let now t and s be two terms that are equal in $\langle \mathbb{N}, 1, +, \times, \uparrow\rangle$. They support the hypotheses of lemma 5, since $[\varnothing, \mathrm{Var}(t+s)] \vdash t \doteq s$ can be derived in *ZP* (using E0), thus in ZP_{ax}.

Corollary 6 then yields a derivation of $\Delta \vdash t \doteq s$ in P_{ax}, which contains no 0 in its terms.

If contexts are removed from this derivation, the E6 rules can be stripped as well (they become empty transitions), and we get a derivation in a formal system with $\{\mathcal{A}_i^+\}_{i\in\{1,\ldots,n\}}$ as axioms, and the usual transitivity, symmetry, reflexivity and context rules, which is equivalent to Th

Therefore any equality in $\langle \mathbb{N}, 1, +, \times, \uparrow\rangle$ can be derived in Th. Since it is known that equality in $\langle \mathbb{N}, 1, +, \times, \uparrow\rangle$ cannot derive from any finite set of axioms, we have a contradiction. □

5 Conclusions

We have proved that $\langle \mathbb{N}, 0, 1, +, \times, \uparrow\rangle$ has a decidable, but not finitely axiomatisable, equational theory, and clearly shown that the only difference between $\langle \mathbb{N}, 0, 1, +, \times, \uparrow\rangle$ and $\langle \mathbb{N}, 1, +, \times, \uparrow\rangle$ is given by the system $\mathfrak{Z}$ in figure 2.
As a consequence, the family of Gurevič's equalities does not collapse, and we also obtain the following additional result

Theorem 8. *The theory of type isomorphisms in Bi-Cartesian Closed Categories is not finitely axiomatisable*

that closes the long standing open problem of the finite axiomatisability of type isomorphisms for the lambda calculus with sums and the empty types [DC95].

By using the decidability result for $\langle \mathbb{N}, 0, 1, +, \times, \uparrow\rangle$ and the fact that all isomorphisms are equalities, we can reject all non-isomorphisms that are also non-arithmetical identities, but, due to the fact that some arithmetic identities are not isomorphisms of BiCCCs, it is left open whether such isomorphisms are indeed decidable.

Acknowledgements The first author would like to thank Claude Kirchner, Vincent Balat and Christophe Calves for interesting discussions on these subjects.

References

[BDCF02] Vincent Balat, Roberto Di Cosmo, and Marcelo Fiore. Remarks on isomorphisms in typed lambda calculi with empty and sum type. In *LICS*. IEEE, July 2002.

[BDCF04] Vincent Balat, Roberto Di Cosmo, and Marcelo Fiore. Extensional normalisation and type-directed partial evaluation for typed lamda calculus with sums. In *31st Ann. ACM Symp. on Principles of Programming Languages (POPL)*, pages 64–76. ACM, 2004.

[DC95] Roberto Di Cosmo. *Isomorphisms of types: from λ-calculus to information retrieval and language design*. Birkhauser, 1995.

[D97] Kosta Dosen and Zoran Petric. Isomorphic objects in symmetric monoidal closed categories. *Mathematical Structures in Computer Science*, 7(6):639–662, 1997.

[DT69] J. Doner and Alfred Tarski. An extended arithmetic of ordinal numbers. *Fundamenta Mathematica*, 65:95–127, 1969.

[Gur85] R. Gurevič. Equational theory of positive numbers with exponentiation. *Proceedings of the American Mathematical Society*, 94(1):135–141, 1985.

[Gur90] R. Gurevič. Equational theory of positive numbers with exponentiation is not finitely axiomatizable. *Annals of Pure and Applied Logic*, 49:1–30, 1990.

[Hen77] Leon Henkin. The logic of equality. *American Mathematical Monthly*, 84:597–612, October 1977.

[HR84] C. W. Henson and L. A. Rubel. Some applications of Nevanlinna theory to mathematical logic: Identities of exponential functions. *Trans. Am. Math. Soc.*, 282(1):1–32, March 1984.

[Mac81] A. Macintyre. The laws of exponentiation. In C. Berline, K. McAloon, and J.-P. Ressayre, editors, *Model Theory and Arithmetic*, volume 890 of *Lecture Notes in Mathematics*, pages 185–197. Springer-Verlag, 1981.

[Mar72] Charles F. Martin. Axiomatic bases for equational theories of natural numbers. *Notices of the Am. Math. Soc.*, 19(7):778, 1972.

[Rit90] Mikael Rittri. *Searching program libraries by type and proving compiler correctness by bisimulation*. PhD thesis, University of Göteborg, Göteborg, Sweden, 1990.

[Rog88] Hartley Rogers, Jr. *Theory of Recursive Functions and Effective Computability*. The MIT Press, Cambridge, Massachusetts; London, England, second edition, 1988.

[Sol93] Sergei V. Soloviev. A complete axiom system for isomorphism of types in closed categories. In A. Voronkov, editor, *Logic Programming and Automated Reasoning, 4th International Conference*, volume 698 of *Lecture Notes in Artificial Intelligence (subseries of LNCS)*, pages 360–371, St. Petersburg, Russia, 1993. Springer-Verlag.

[Wil81] A. J. Wilkie. On exponentiation — A solution to Tarski's high school algebra problem. Math. Inst. Oxford University (preprint), 1981.

[ZGC03] Yoav Zibin, Joseph (Yossi) Gil, and Jeffrey Considine. Efficient algorithms for isomorphisms of simple types. In *Proceedings of the 30th ACM SIGPLAN-SIGACT symposium on Principles of programming languages*, pages 160–171. ACM Press, 2003.

A Appendix

A.1 Proof of proposition 1

Let $H(t) = \#_0(t) + 2 \times \sum_{x/\Gamma \Rightarrow x=0} \#_x(t)$, where $\#_s(t)$ is the number of times s occurs in t. We proceed by induction in lexicographical order on $(S(t), H(t))$ where $S(t)$ is the size of t[10].

If $H(t) = 0$ or $t = 0$, taking $t' = t$ is OK.

Otherwise, i.e. if $t \neq 0$ and $H(t) > 0$, t matches one of the following patterns:

[10] This is the size in the usual meaning: the number of nodes in the syntax tree of t.

1. $C[0 \times s]$ or $C[s \times 0]$,
2. $C[0 + s]$ or $C[s + 0]$,
3. $C[s^0]$,
4. $C[x]$ where $\Gamma \Rightarrow x = 0$,
5. $C[0^s]$ where s is syntactically positive.

($C[\cdot]$ denotes a context with only one placeholder.)

1. The induction hypothesis yields a derivation D of $\Gamma \vdash C[0] \doteq t'$ where t' is 0 or syntactically positive, hence the following derivation:

$$\dfrac{\dfrac{\dfrac{}{\top \vdash s \times 0 \doteq 0}}{\Gamma \vdash s \times 0 \doteq 0} \qquad \dfrac{(D)}{\Gamma \vdash C[0] \doteq t'}}{\Gamma \vdash t \doteq t'}$$

   We proceed similarly when $t = C[0 \times s]$, using the rule E3' instead of E3.
2. The induction hypothesis again yields a derivation D of $\Gamma \vdash C[s] \doteq t'$ where t' is 0 or syntactically positive, and we build the following derivation.

$$\dfrac{\dfrac{\dfrac{}{\top \vdash s + 0 \doteq s}}{\Gamma \vdash s + 0 \doteq s} \qquad \dfrac{(D)}{\Gamma \vdash C[s] \doteq t'}}{\Gamma \vdash t \doteq t'}$$

   We proceed similarly when $t = C[0 + s]$, using the rule E2' instead of E2.
3. By induction there is a derivation D of $\Gamma \vdash C[1] \doteq t'$ with a suitable t', and we derive:

$$\dfrac{\dfrac{\dfrac{}{\top \vdash s^0 \doteq 1}}{\Gamma \vdash s^0 \doteq 1} \qquad \dfrac{(D)}{\Gamma \vdash C[1] \doteq t'}}{\Gamma \vdash t \doteq t'}$$

4. By induction there is a derivation D of $\Gamma \vdash C[0] \doteq t'$ with a suitable t', and we derive:

$$\dfrac{\dfrac{\dfrac{}{x = 0 \vdash x \doteq 0}}{\Gamma \vdash x \doteq 0} \qquad \dfrac{(D)}{\Gamma \vdash C[0] \doteq t'}}{\Gamma \vdash t \doteq t'}$$

5. By induction there is a derivation D of $\Gamma \vdash C[0] \doteq t'$ with a suitable t', and we derive:

$$\dfrac{\dfrac{\dfrac{(D')}{\Gamma \vdash s \text{ positive}}}{\Gamma \vdash 0^s \doteq 0} \qquad \dfrac{(D)}{\Gamma \vdash C[0] \doteq t'}}{\Gamma \vdash t \doteq t'}$$

   Here, we will need the lemma 1 pertaining to the relationship between the "$\Gamma \vdash t$ positive" statement and being syntactically positive, in order to provide the derivation D'.

A.2 Proof of proposition 2 (1)

Depending on the last rule used in this derivation, we have:

REFL, E1 to E4 These are trivial cases.
SYM, TRANS, CONT, E5 These are also obvious, using the induction hypothesis.
E0 Thanks to the (†) condition, $\forall\varphi$ such that $\forall x\ \varphi(x) \neq 0$, $[\![t]\!]_\varphi = [\![s]\!]_\varphi$.
Let ψ be a valuation satisfying Γ; since t and s are syntactically positive in context Γ, necessarily $\forall x \in \mathrm{Var}(t+s)\ \psi(x) \neq 0$, and there exists a valuation φ as above such that $[\![t]\!]_\varphi = [\![t]\!]_\psi$, and $[\![s]\!]_\varphi = [\![s]\!]_\psi$. Thus $[\![t]\!]_\psi = [\![s]\!]_\psi$ holds.
E6 By induction : $\forall\varphi$ satisfying Γ, $[\![t]\!]_\varphi = [\![s]\!]_\varphi$. Since $\Delta \Rightarrow \Gamma$ it is clear that any valuation φ satisfying Δ also satisfies Γ, hence $\forall\varphi$ satisfying Δ, $[\![t]\!]_\varphi = [\![s]\!]_\varphi$.
E7 As well as with E6, any valuation φ satisfying $\Gamma \vee \Delta$ satisfies either Γ or Δ.
N0 and N1 Are also trivial cases.
N2 to N5 The induction hypothesis obviously allows to conclude.
N6 This case is treated like E6.
N7 Like E7.

A.3 Proof of proposition 2 (2)

We let Γ be such that $\forall\varphi$ satisfying Γ, $[\![t]\!]_\varphi = [\![s]\!]_\varphi$.

Fact 1 Γ has a logically equivalent form that is written

$$([A_1, B] \wedge \Delta_1) \vee \cdots \vee ([A_n, B] \wedge \Delta_n)$$

where

- $B = \mathrm{Var}(t+s)$,
- $\forall i\ A_i \subset B$,
- $\forall i\ \Delta_i$ is a $\wedge$-formula in which no variable in $\mathrm{Var}(t+s)$ appears.

To draft a proof, let us say that one needs to put Γ in a normal disjunctive form, call it Γ', which is in turn equivalent to $\Gamma' \wedge \bigwedge_{x\in\mathrm{Var}(t+s)}(x = 0 \vee \neg x = 0)$. What remains to be done is distributing this expression, taking out the antilogic conjunctive clauses, and grouping the atoms in each clause.

Fact 2 $\forall\psi$ satisfying $[A_i, B]$, there is a φ satisfying $[A_i, B] \wedge \Delta_i$ (thus satisfying Γ), such that $[\![t]\!]_\psi = [\![t]\!]_\varphi$, and $[\![s]\!]_\psi = [\![s]\!]_\varphi$.

All that is needed is to "change the values of ψ so that it satisfies Δ_i", which can assuredly be done without modifying the value of $\psi(x)$ for any $x \in \mathrm{Var}(t+s)$.

Fact 3 ($\forall\varphi$ satisfying Γ $[\![t]\!]_\varphi = [\![s]\!]_\varphi$) $\Rightarrow \forall i$ ($\forall\psi$ satisfying $[A_i, B]$ $[\![t]\!]_\psi = [\![s]\!]_\psi$)
This is obvious thanks to fact 2.

Fact 4 $(\forall i\ [A_i, B] \vdash t \doteq s) \Rightarrow \Gamma \vdash t \doteq s$.
One needs only use rules E6 (to bring in the Δ_is) and E7.

A.4 Proof of lemma 4

$\mathbf{R} \in \mathbf{G}$ Follow with an E6, with Δ as new context.

E5 Insert an N6 with Δ as new context between the premise and conclusion of this E5.

E6 D has the following form :

$$\dfrac{\dfrac{(D')}{\Gamma' \vdash t \doteq s}}{\Gamma \vdash t \doteq s}$$

where $\Gamma \Rightarrow \Gamma'$. Thus $\Delta \Rightarrow \Gamma'$ and the induction hypothesis applies to the derivation of $\Gamma' \vdash t \doteq s$, yielding the wanted **L**-derivation.

E7 D has the following form :

$$\dfrac{\dfrac{(D')}{\Gamma' \vdash t \doteq s} \qquad \dfrac{(D'')}{\Gamma'' \vdash t \doteq s}}{\Gamma' \vee \Gamma'' \vdash t \doteq s}$$

Since Δ is exhaustive for t and s, it is a $\wedge$-formula and either $\Delta \Rightarrow \Gamma'$ or $\Delta \Rightarrow \Gamma''$ holds. If for example , $\Delta \Rightarrow \Gamma'$ holds, the induction hypothesis can be applied to the derivation of $\Gamma' \vdash t \doteq s$, yielding the wanted **L**-derivation.

SYM, CONT Trivial.

TRANS By induction hypothesis we have **L**-derivations of $\Delta \wedge \Delta_0 \vdash t \doteq s$ and $\Delta \wedge \Delta_1 \vdash s \doteq u$. By letting $\Delta' = \Delta_0 \wedge \Delta_1$, and summoning lemma 3 we get **L**-derivations of $\Delta \wedge \Delta' \vdash t \doteq s$ and $\Delta \wedge \Delta' \vdash s \doteq u$. All that is left is to apply TRANS again.

A.5 Proof of lemma 5

$\mathcal{A}_i$ followed by E6 Use $\mathcal{A}_i^+$, then E6.

$\mathbf{R} \in \mathbf{G_0}$ followed by E6 For any rule in G_0, when its conclusion is written $\Gamma \vdash l \doteq r$ we have $\Delta' \Rightarrow \Gamma$ (see **L2**, **L4**), and $\Delta'(l) = \Delta'(r)$ (checking this is easy). The **EL**-derivation we want is a suitable use of REFL followed by E6.

E5 Idem.

SYM Immediate induction step.

CONT In this case, the **L**-derivation (D) looks like this:

$$\dfrac{\dfrac{(D')}{\Delta' \vdash t \doteq s}}{\Delta' \vdash C[t] \doteq C[s]}$$

By induction we have an **EL**-derivation of $\Delta' \vdash \Delta'(t) \doteq \Delta'(s)$, and one of two things happens:

- Either $\Delta'(t) = \Delta'(s) = 0$, and $\Delta'(C[t]) = \Delta'(C[s])$ – both are $\Delta'(C[0])$, which can be derived by REFL + E6.
- Or $\Delta'(t)$ and $\Delta'(s)$ are syntactically positive in context Δ', and $\Delta'(C[t]) = \Delta'(C[\cdot])[\Delta'(t)]$ (*mutatis mutandis* s). So we just have to apply CONT again, with context $\Delta'(C[\cdot])$, to get the desired **EL**-derivation.

TRANS As SYM, relying on **L2** to summon the induction hypothesis.

Properties **L1** to **L4** are clearly preserved, **EL0** clearly holds, and **EL1** as well since $\Gamma(\Gamma(t)) = \Gamma(t)$ whenever $\Gamma(t)$ is defined.