Archive for Mathematical Logic (2024) 63:353–390
https://doi.org/10.1007/s00153-023-00898-y

Mathematical Logic

Weak essentially undecidable theories of concatenation, part II

Juvenal Murwanashyaka[1]

Received: 27 December 2021 / Accepted: 30 September 2023 / Published online: 2 November 2023
© The Author(s) 2023

Abstract
We show that we can interpret concatenation theories in arithmetical theories without coding sequences by identifying binary strings with 2×2 matrices with determinant 1.

Keywords Theory of concatenation · First-order arithmetic · Interpretability

Mathematics Subject Classification 03B25 · 03B30 · 03F25 · 03F30

1 Introduction

A computably enumerable first-order theory is called *essentially undecidable* if any consistent extension, in the same language, is undecidable (there is no algorithm for deciding whether an arbitrary sentence is a theorem). A computably enumerable first-order theory is called *essentially incomplete* if any recursively axiomatizable consistent extension is incomplete. Since a decidable consistent theory can be extended to a decidable complete consistent theory (see Chapter 1 of Tarski et al. [12]), a theory is essentially undecidable if and only if it is essentially incomplete. Two theories that are known to be essentially undecidable are Robinson arithmetic Q and the related theory R (see Fig. 1 for the axioms of R and Q). The essential undecidability of R and Q is proved in Chapter 2 of [12]. In Chapter 1 of [12], Tarski introduces interpretability as an indirect way of showing that first-order theories are essentially undecidable. The method is indirect because it reduces the problem of essential undecidability of a theory T to the problem of essentially undecidability of a theory S which is known to be essentially undecidable. Interpretability between theories is a reflexive and transitive relation and thus induces a degree structure on the class of computably enumerable essentially undecidable first-order theories.

✉ Juvenal Murwanashyaka
juvenalm@math.uio.no

1 Department of Mathematics, University of Oslo, Oslo, Norway

The Axioms of R

R_1 $\overline{n}+\overline{m}=\overline{n+m}$
R_2 $\overline{n}\times\overline{m}=\overline{n\times m}$
R_3 $\overline{n}\neq\overline{m}$ if $n\neq m$
R_4 $\forall x\;[\;x\leq\overline{n}\rightarrow\bigvee_{k\leq n}x=\overline{k}\;]$
R_5 $\forall x\;[\;x\leq\overline{n}\vee\overline{n}\leq x\;]$

The Axioms of Q

Q_1 $\forall xy\;[\;x\neq y\rightarrow \mathrm{S}x\neq\mathrm{S}y\;]$
Q_2 $\forall x\;[\;\mathrm{S}x\neq 0\;]$
Q_3 $\forall x\;[\;x=0\vee\exists y\;[\;x=\mathrm{S}y\;]\;]$
Q_4 $\forall x\;[\;x+0=x\;]$
Q_5 $\forall xy\;[\;x+\mathrm{S}y=\mathrm{S}(x+y)\;]$
Q_6 $\forall x\;[\;x\times 0=0\;]$
Q_7 $\forall xy\;[\;x\times\mathrm{S}y=x\times y+x\;]$

Fig. 1 Non-logical axioms of the first-order theories R, Q. The axioms of R are given by axiom schemes where n, m, k are natural numbers and $\overline{n}, \overline{m}, \overline{k}$ are their canonical names

Fig. 2 Non-logical axioms of the first-order theories WD, D. The axioms of WD are given by axiom schemes where α, β, γ are nonempty binary strings and $\overline{\alpha}, \overline{\beta}, \overline{\gamma}$ are their canonical names. $\mathsf{Pref}(\alpha)$ is the set of all nonempty prefixes of α

The Axioms of WD

WD_1 $\overline{\alpha}\;\overline{\beta}=\overline{\alpha\beta}$
WD_2 $\overline{\alpha}\neq\overline{\beta}$ if $\alpha\neq\beta$
WD_3 $\forall x\;[\;x\preceq\overline{\alpha}\leftrightarrow\bigvee_{\gamma\in\mathsf{Pref}(\alpha)}x=\overline{\gamma}\;]$

The Axioms of D

D_1 $\forall xyz\;[\;(xy)z=x(yz)\;]$
D_2 $\forall xy\;[\;x\neq y\rightarrow(\;x0\neq y0\wedge x1\neq y1\;)\;]$
D_3 $\forall xy\;[\;x0\neq y1\;]$
D_4 $\forall x\;[\;x\preceq 0\leftrightarrow x=0\;]$
D_5 $\forall x\;[\;x\preceq 1\leftrightarrow x=1\;]$
D_6 $\forall xy\;[\;x\preceq y0\leftrightarrow(\;x=y0\vee x\preceq y\;)\;]$
D_7 $\forall xy\;[\;x\preceq y1\leftrightarrow(\;x=y1\vee x\preceq y\;)\;]$

In [10], we introduce two theories of concatenation WD, D and show that they are respectively mutually interpretable with R and Q (see Fig. 2 for the axioms of WD and D). The language of WD and D is $\{0, 1, \circ, \preceq\}$ where 0 and 1 are constant symbols, $\circ$ is a binary function symbol and $\preceq$ is a binary relation symbol. The intended model of WD and D is the free semigroup generated by two letters extended with the prefix relation. Extending finitely generated free semigroups with the prefix relation allows us to introduce Σ_1-formulas which are expressive enough to encode computations by Turing machines (see Kristiansen and Murwanashyaka [6]). Σ_1-formulas are formulas on negation normal form where universal quantifiers occur bounded, i.e., they are of the form $\forall x \preceq t$. Axioms $\mathsf{D}_4-\mathsf{D}_7$ are essential for coding sequences in D since they allow us to work with Σ_0-formulas, formulas where all quantifiers are of the form $\exists x \preceq t$, $\forall x \preceq t$. In [10], we show that Q is interpretable in D by using especially axioms $\mathsf{D}_4-\mathsf{D}_7$ to restrict the universe of D to a domain K on which the analogue of Q_3 holds, that is, the sentence $\mathsf{Q}_3' \equiv \forall x\;[\;x=0\;\vee\;x=1\;\vee\;\exists y\preceq x\;[\;x=y0\;\vee\;x=y1\;]\;]$. To improve readability, we use juxtaposition instead of the binary function symbol $\circ$ of the formal language. Due to the existential quantifier in Q_3', we need to ensure that Σ_0-formulas are absolute for K.

Since D and Q are mutually interpretable, we can identify differences between these two theories by investigating the interpretability degrees of the theories we obtain by weakening axioms $\mathsf{D}_4 - \mathsf{D}_7$, Q_3 which are essential for coding sequences in D and Q. In addition to D and WD, we introduce in [10] two theories ID, ID^* (called C, BT, respectively, in [10]) and prove that their interpretability degrees are strictly between the degrees of WD and D. But we are not able to determine in [10] whether ID and ID^* are mutually interpretable. We obtain ID and ID^* from D by replacing axioms $\mathsf{D}_4 - \mathsf{D}_7$ with respectively the axiom schemas

$$\mathsf{ID}_4 \equiv \forall x \left[x \preceq \overline{\alpha} \leftrightarrow \bigvee_{\gamma \in \mathsf{Pref}(\alpha)} x = \overline{\gamma} \right], \quad \mathsf{ID}_4^* \equiv \forall x \left[x \sqsubseteq_{\mathsf{S}} \overline{\alpha} \rightarrow \bigvee_{\gamma \in \mathsf{Sub}(\alpha)} x = \overline{\gamma} \right]$$

where α is a nonempty binary string, $\overline{\alpha}$ is a canonical variable-free term that represents α, $\mathsf{Pref}(\alpha)$ denotes the set of all nonempty prefixes of α, $\mathsf{Sub}(\alpha)$ denotes the set of all nonempty substrings of α and $x \sqsubseteq_{\mathsf{S}} y$ is shorthand for

$$x = y \ \vee \ \exists uv \ [\ y = ux \ \vee \ y = xv \ \vee \ y = uxv\ ] .$$

In the standard model, $x \sqsubseteq_{\mathsf{S}} y$ holds if and only if $x \in \mathsf{Sub}(y)$. It is easy to interpret ID in ID^* while it is less obvious whether ID^* is interpretable in ID since the axiom schema ID_4^* puts strong constraints on the concatenation operator while any model of $\mathsf{D}_1 - \mathsf{D}_3$ can always be extended to a model of ID. In Sect. 3, we show that ID and ID^* are mutually interpretable.

Given mutually interpretability of ID and ID^*, a natural question is whether the arithmetical analogues of ID and ID^* are also mutually interpretable. We let IQ and IQ^* be the theories we obtain from Q by replacing axiom Q_3 with respectively the axiom schemas

$$\mathsf{IQ}_3 \equiv \forall x \left[x \leq \overline{n} \leftrightarrow \bigvee_{k \leq n} x = \overline{k} \right], \quad \mathsf{IQ}_3^* \equiv \forall x \left[x \leq_{\mathsf{l}} \overline{n} \rightarrow \bigvee_{k \leq n} x = \overline{k} \right]$$

where n is a natural number, $\overline{n}$ is a canonical variable-free term that represents n, $\leq$ is a fresh binary relation symbol that is realized as the less than or equal relation in the standard model and $x \leq_{\mathsf{l}} y \equiv \exists z\ [\ z + x = y\ ]$. In Sect. 4, we show that IQ and IQ^* are mutually interpretable.

We try to identify differences between concatenation theories and arithmetical theories by investigating the comparability of ID and IQ with respect to interpretability. In Sect. 5, we show that IQ is expressive enough to interpret the theory $\overline{\mathsf{ID}}$ we obtain by extending ID with the axioms

$$\forall xy\ [\ x \neq y \rightarrow (\ 0x \neq 0y \ \wedge \ 1x \neq 1y\ )\ ], \ \ \forall xy\ [\ 0x \neq 1y\ ].$$

Since IQ does not have enough resources for coding general sequences, the interpretation we give shows that we can think of concatenation theories as naturally contained in arithmetical theories. In Sect. 5.2, we show that the idea behind the interpretation of ID in IQ allows us to give a very simple interpretation of WD in R. In Sect. 6, we show

The Axioms of TC

TC_1 $\forall xyz\,[\,x(yz) = (xy)z\,]$
TC_2 $\forall xyzw\,[\,(\,xy = zw \rightarrow \big(\,(\,x = z \wedge y = w)\vee$
$\exists u\,[\,(\,z = xu \wedge uw = y\,) \vee (\,x = zu \wedge uy = w\,)\,]\,\big)\,]$
TC_3 $\forall xy\,[\,xy \neq 0\,]$
TC_4 $\forall xy\,[\,xy \neq 1\,]$
TC_5 $0 \neq 1$

Fig. 3 Non-logical axioms of the first-order theory TC

that our interpretation of ID in IQ extends in a natural way to an interpretation in Q of Grzegorczyk's theory of concatenation TC [3] (see Fig. 3 for the axioms of TC). We can think of D as a fragment of TC since TC proves all the axioms of D when we let $x \preceq y \equiv x = y \vee \exists z\,[\,y = xz\,]$. The intended model of TC is a finitely generated free semigroup with at least two generators. We have not been able to determine whether IQ is interpretable in $\overline{\mathsf{ID}}$ and whether $\overline{\mathsf{ID}}$ is interpretable in ID.

We summarize our results in the following theorem. We let $S \leq T$ mean that S is interpretable in T. We let $S < T$ mean $S \leq T \;\wedge\; T \not\leq S$. We let $S \cong T$ mean $S \leq T \;\wedge\; T \leq S$. We let $\overline{\mathsf{ID}}^*$ denote the theory we obtain from $\overline{\mathsf{ID}}$ by replacing ID_4 with ID_4^*.

Theorem 1

$$\mathsf{R} \cong \mathsf{WD} < \mathsf{ID} \cong \mathsf{ID}^* \leq \overline{\mathsf{ID}} \cong \overline{\mathsf{ID}}^* \leq \mathsf{IQ} \cong \mathsf{IQ}^* < \mathsf{Q} \cong \mathsf{D}.$$

It is not difficult to see that the two strict inequalities $\mathsf{WD} < \mathsf{ID}$, $\mathsf{IQ} < \mathsf{Q}$ hold. If ID were interpretable in WD, then $\mathsf{ID}_1 - \mathsf{ID}_3$ would be interpretable in a finite subtheory of WD. Since any model of $\mathsf{ID}_1 - \mathsf{ID}_3$ is infinite while any finite subtheory of WD has a finite model, ID is not interpretable in WD. Similarly, if Q were interpretable in IQ, it would be interpretable in a finite subtheory of IQ. But, any finite subtheory of IQ is interpretable in the first-order theory of the field of real numbers $(\mathbb{R}, 0, 1, +, \times)$, which was shown to be decidable by Tarski [11]. Since Q is essentially undecidable, it is not interpretable in IQ.

2 Preliminaries

In this section, we clarify a number of notions that we only glossed over in the previous section.

2.1 Notation and terminology

We consider the structures

$$\mathfrak{D}^- = (\{\mathbf{0},\mathbf{1}\}^+, \mathbf{0}, \mathbf{1}, ^\frown\,) \quad \text{and} \quad \mathfrak{D} = (\{\mathbf{0},\mathbf{1}\}^+, \mathbf{0}, \mathbf{1}, ^\frown, \preceq^{\mathfrak{D}})$$

where $\{\mathbf{0},\mathbf{1}\}^+$ is the set of all finite nonempty strings over the alphabet $\{\mathbf{0},\mathbf{1}\}$, the binary operator $\frown$ concatenates elements of $\{\mathbf{0},\mathbf{1}\}^+$ and $\preceq^{\mathfrak{D}}$ denotes the prefix relation, i.e., $x \preceq^{\mathfrak{D}} y$ if and only if $y = x$ or there exists $z \in \{\mathbf{0},\mathbf{1}\}^+$ such that $y = x^\frown z$. The structure $\mathfrak{D}^-$ is thus the free semigroup with two generators. We call elements of $\{\mathbf{0},\mathbf{1}\}^+$ *bit strings*. The structures $\mathfrak{D}^-$ and $\mathfrak{D}$ are first-order structures over the languages $\mathcal{L}_{\mathsf{BT}}^- = \{0, 1, \circ\}$ and $\mathcal{L}_{\mathsf{BT}} = \{0, 1, \circ, \preceq\}$, respectively.

The language of first-order arithmetic is $\mathcal{L}_{\mathsf{NT}} = \{0, \mathrm{S}, +, \times\}$ and we denote by $(\mathbb{N}, 0, \mathrm{S}, +, \times)$ the standard first-order structure. In first-order number theory, each natural number n is associated with a numeral $\overline{n}$ by recursion: $\overline{0} \equiv 0$ and $\overline{n+1} \equiv \mathrm{S}\overline{n}$. Each non-empty bit string $\alpha \in \{\mathbf{0},\mathbf{1}\}^+$ is associated by recursion with a unique $\mathcal{L}_{\mathsf{BT}}^-$-term $\overline{\alpha}$, called a *biteral*, as follows: $\overline{\mathbf{0}} \equiv 0$, $\overline{\mathbf{1}} \equiv 1$, $\overline{\alpha\mathbf{0}} \equiv (\overline{\alpha} \circ 0)$ and $\overline{\alpha\mathbf{1}} \equiv (\overline{\alpha} \circ 1)$. The biterals are important if we, for example, want to show that certain sets are definable since we then need to talk about elements of $\{\mathbf{0},\mathbf{1}\}^+$ in the formal theory.

A class is a formula with at least one free variable. Given a class I with n free variables, we write $(x_1, \dots, x_n) \in I$ for $I(x_1, \dots, x_n)$. If I has two free variables, we also write xIy for $I(x, y)$. We let $(\exists x_1, \dots, x_n) \in I \;\; [\, \phi \,]$ and $(\forall x_1, \dots, x_n) \in I \;\; [\, \phi \,]$ be shorthand for the formulas $\exists x_1, \dots, x_n \; [\; I(x_1, \dots, x_n) \;\; \wedge \;\; \phi \;]$ and $\forall x_1, \dots, x_n \; [\; I(x_1, \dots, x_n) \; \rightarrow \; \phi \;]$, respectively. We let $\{(x_1, \dots, x_n) \in I \; : \;\; \psi\}$ be shorthand for $I(x_1, \dots, x_n) \;\wedge\; \psi$.

2.2 Translations and interpretations

We recall the method of relative interpretability introduced by Tarski [12] for showing that first-order theories are essentially undecidable. We restrict ourselves to many-dimensional parameter-free one-piece relative interpretations. Let $\mathcal{L}_1$ and $\mathcal{L}_2$ be computable first-order languages. A *relative translation* τ from $\mathcal{L}_1$ to $\mathcal{L}_2$ is a computable map given by:

1. An $\mathcal{L}_2$-formula $\delta(x_1, \dots, x_m)$ with exactly m free variable. The formula $\delta(x_1, \dots, x_m)$ is called a domain.
2. For each n-ary relation symbol R of $\mathcal{L}_1$, an $\mathcal{L}_2$-formula $\psi_R(\vec{x}_1, \dots, \vec{x}_n)$ with exactly mn free variables. The equality symbol $=$ is treated as a binary relation symbol.
3. For each n-ary function symbol f of $\mathcal{L}_1$, an $\mathcal{L}_2$-formula $\psi_f(\vec{x}_1, \dots, \vec{x}_n, \vec{y})$ with exactly $m(n+1)$ free variables.
4. For each constant symbol c of $\mathcal{L}_1$, an $\mathcal{L}_2$-formula $\psi_c(\vec{y})$ with exactly m free variables.

We extend τ to a translation of atomic $\mathcal{L}_1$-formulas by mapping an $\mathcal{L}_1$-term t to an $\mathcal{L}_2$-formula $(t)^{\tau,\vec{w}}$ with free variables $\vec{w}$ that denote the value of t:

5. For each n-ary relation symbol R of $\mathcal{L}_1$

$$\big(R(t_1, \dots, t_n)\big)^\tau \equiv \exists \vec{v}_1 \dots \vec{v}_n \left[\bigwedge_{i=1}^{n} \delta(\vec{v}_i) \;\wedge\; \bigwedge_{j=1}^{n} (t_j)^{\tau,\vec{v}_j} \;\wedge\; \psi_R(\vec{v}_1 \dots \vec{v}_n) \right]$$

where $\vec{v}_1 \dots \vec{v}_n$ are distinct variable symbols that do not occur in $t_1, \dots, t_n$ and

(a) for each variable symbol x of $\mathcal{L}_1$, $(x)^{\tau,\vec{w}} \equiv \bigwedge_{i=1}^{m} w_i = x_i$
(b) for each constant symbol c of $\mathcal{L}_1$, $(c)^{\tau,\vec{w}} \equiv \psi_c(\vec{w})$
(c) for each n-ary function symbol f of $\mathcal{L}_1$

$$\begin{aligned} &\big(f(t_1,\ldots,t_n)\big)^{\tau,\vec{w}} \\ &\equiv \exists \vec{w}_1 \ldots \vec{w}_n \left[\bigwedge_{i=1}^{n} \delta(\vec{w}_i) \ \wedge \ \bigwedge_{j=1}^{n} (t_j)^{\tau,\vec{w}_j} \ \wedge \ \psi_f(\vec{w}_1 \ldots \vec{w}_n, \vec{w}) \right] \end{aligned}$$

where $\vec{w}_1 \ldots \vec{w}_n$ are distinct variable symbols that do not occur in $\bigwedge_{j=1}^{n} (t_j)^{\tau,\vec{w}}$.

We extend τ to a translation of all $\mathcal{L}_1$-formulas as follows:

6. $(\neg\phi)^\tau \equiv \neg\phi^\tau$
7. $(\phi \oslash \psi)^\tau \equiv \phi^\tau \oslash \psi^\tau$ for $\oslash \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$
8. $(\exists x\ \phi)^\tau \equiv \exists\vec{x}\ [\ \delta(\vec{x}) \ \wedge\ \phi^\tau\ ]$
9. $(\forall x\ \phi)^\tau \equiv \forall\vec{x}\ [\ \delta(\vec{x}) \rightarrow \phi^\tau\ ]$.

Let S be an $\mathcal{L}_1$-theory and let T be an $\mathcal{L}_2$-theory. We say that S is *(relatively) interpretable* in T if there exists a relative translation τ such that

– $T \vdash \exists\mathbf{x}\ [\ \delta(\mathbf{x})\ ]$
– For each function symbol f of $\mathcal{L}_1$

$$T \vdash \bigwedge_{i=1}^{n} \delta(\mathbf{x}_i) \rightarrow \exists\mathbf{y}\ \big[\ \delta(\mathbf{y}) \wedge \psi_f(\mathbf{x}_1,\ldots,\mathbf{x}_n,\mathbf{y}) \wedge \forall\mathbf{z}\ \big[\ \delta(\mathbf{z}) \wedge \psi_f(\mathbf{x}_1,\ldots,\mathbf{x}_n,\mathbf{z}) \rightarrow \psi_=(\mathbf{y},\mathbf{z})\ \big]\ \big].$$

– For each constant symbol c of $\mathcal{L}_1$

$$T \vdash \exists\mathbf{y}\ \big[\ \delta(\mathbf{y}) \wedge \psi_c(\mathbf{y}) \wedge \forall\mathbf{z}\ \big[\ \delta(\mathbf{z}) \wedge \psi_c(\mathbf{z}) \rightarrow \psi_=(\mathbf{y},\mathbf{z})\ \big]\ \big].$$

– T proves ϕ^τ for each non-logical axiom ϕ of S. If equality is not translated as equality, then T must prove the translation of each equality axiom.

If S is relatively interpretable in T and T is relatively interpretable in S, we say that S and T are *mutually interpretable*.

The following proposition summarizes important properties of relative interpretability (see Tarski et al. [12] for the details).

Proposition 2 *Let S, T and U be computably enumerable first-order theories.*

1. *If S is interpretable in T and T is consistent, then S is consistent.*
2. *If S is interpretable in T and T is interpretable in U, then S is interpretable in U.*
3. *If S is interpretable in T and S is essentially undecidable, then T is essentially undecidable.*

3 Mutual interpretability of ID and ID*

In this section, we show that ID and ID* are mutually interpretable (see Fig. 4 for the axioms of ID and ID*). It is easy to see that ID is interpretable in ID*. We therefore need to focus on the more difficult task of proving that ID* is interpretable in ID. It is more difficult to interpret ID* in ID because the axiom schema ID_4^* puts strong constraints on the concatenation operator while it is always possible to extend any model of ID_1, ID_2, ID_3 to a model of ID. For example, we can have models of ID where there exist infinitely many pairs x, y such that $xy = \overline{\alpha}$ for each nonempty string α. Indeed, consider the model where the universe is the Cartesian product $\prod_{i<\omega}\{0, 1\}^*$, concatenation is componentwise and each binary string β is mapped to the constant sequence $(\beta)_{i<\omega}$.

To interpret ID* in ID, we need to use the axiom schema ID_4 in an essential way to define a function $\star$ that provably in ID satisfies the translation of each axiom of ID*. The idea is to observe that since we have the right cancellation law in the weak form of ID_2, if we had an axiom schema for the suffix relation, denoted $\preceq_{\mathsf{suff}}$, analogues to ID_4, we could try to define $\star$ by requiring that $x{\star}y = xy$ only if $y \preceq_{\mathsf{suff}} xy$. If xy is a variable-free term and $y \preceq_{\mathsf{suff}} xy$, then the axiom schema for the suffix relation gives us a finite number of possibilities for the value of y. If we also knew that 0 and 1 were atoms/ indecomposable, we would be able to use ID_2 and ID_3 to determine that x and y are also variable-free terms. To make this idea work, we need to ensure that $\star$ is associative. Our solution is to show that extending ID with an axiom schema for $\preceq_{\mathsf{suff}}$ and the axiom $\forall xy\ [\ y \preceq_{\mathsf{suff}} xy\ ]$ does not change the interpretability degree.

This section is organized as follows: In Sect. 3.1, we show that we can extend ID to a theory $\mathsf{ID}^{(2)}$ with the same interpretability degree where 0 and 1 are atoms. In Sect. 3.2, we show that we can extend $\mathsf{ID}^{(2)}$ to a theory $\mathsf{ID}^{(3)}$ with the same interpretability degree where we have an axiom schema for the suffix relation $\preceq_{\mathsf{suff}}$ analogues to the axiom schema ID_4. In Sect. 3.3, we extended $\mathsf{ID}^{(3)}$ to a theory $\mathsf{ID}^{(4)}$ with the same interpretability degree and where we have an axiom schema for the substring relation, analogues to ID_4. In Sect. 3.4, we use the axiom schema for the substring relation to extend $\mathsf{ID}^{(4)}$ to a theory $\mathsf{ID}^{(5)}$ with the same interpretability degree and where the suffix relation $\preceq_{\mathsf{suff}}$ satisfies additional properties. Finally, in Sect. 3.5, we show that ID* is interpretable in $\mathsf{ID}^{(5)}$.

Fig. 4 Non-logical axioms of the first-order theories ID and ID*. ID_4 and ID_4^* are axiom schemas where α is a nonempty binary string, $\mathsf{Pref}(\alpha)$ is the set of all nonempty prefixes of α and $\mathsf{Sub}(\alpha)$ is the set of all nonempty substrings of α. Furthermore, $x \sqsubseteq_{\mathsf{s}} y \equiv\ x = y\ \vee\ \exists uv\ [\ y = ux\ \vee\ y = xv\ \vee\ y = uxv\ ]$

The Axioms of ID

ID_1 $\forall xyz\ [\ (xy)z = x(yz)\ ]$
ID_2 $\forall xy\ [\ x \neq y \rightarrow (\ x0 \neq y0 \wedge x1 \neq y1\ )\ ]$
ID_3 $\forall xy\ [\ x0 \neq y1\ ]$
ID_4 $\forall x\ [\ x \preceq \overline{\alpha} \leftrightarrow \bigvee_{\gamma \in \mathsf{Pref}(\alpha)} x = \overline{\gamma}\ ]$

The Axioms of ID*

$\mathsf{ID}_1,\ \mathsf{ID}_2,\ \mathsf{ID}_3$
ID_4^* $\forall x[\ x \sqsubseteq_{\mathsf{s}} \overline{\alpha} \rightarrow \bigvee_{\gamma \in \mathsf{Sub}(\alpha)} x = \overline{\gamma}\ ]$

3.1 Atoms

It will prove useful later to know that 0 and 1 are atoms. So, let $\mathsf{ID}^{(2)}$ be ID extended with the axioms

$$\mathsf{AT0} \equiv \forall xy\ [\ xy \neq 0\ ], \quad \mathsf{AT1} \equiv \forall xy\ [\ xy \neq 1\ ].$$

Lemma 3 ID *and* $\mathsf{ID}^{(2)}$ *are mutually interpretable.*

Proof Since $\mathsf{ID}^{(2)}$ is an extension of ID, it suffices to show that $\mathsf{ID}^{(2)}$ is interpretable in ID. Since the axioms of ID are universal sentences, it suffices to relativize quantification to a domain K on which the sentences $\mathsf{AT0}$, $\mathsf{AT1}$ hold. We obtain K by successively restricting the universe to subclasses with nice properties.

Let

$$K_1 = \{x :\ x = 0\ \vee\ x = 1\ \vee\ \exists y\ [\ x = y0\ \vee\ x = y1\ ]\ \}.$$

Clearly, $0, 1 \in K_1$. Since concatenation is associative, K_1 is closed under concatenation.

Let

$$K_2 = \left\{ y \in K_1 :\ \forall x \in K_1 \left[\bigwedge_{a \in \{0,1\}} xy \neq a \right] \right\}.$$

We show that $0, 1 \in K_2$. Let $a, b \in \{0, 1\}$ and let $x \in K_1$. We need to show $xb \neq a$. Assume for the sake of a contradiction that $xb = a$. Since $x \in K_1$, let $c \in \{0, 1\}$ be such that $x = c$ or $x = uc$ for some u. Let $d \in \{0, 1\}\setminus\{c\}$. Then, $xb = a$ implies $ddxb = dda$. By ID_3 and ID_2, $ddx = dd$, which contradicts ID_3. Thus, $0, 1 \in K_2$.

We now show that K_2 is closed under the maps $x \mapsto x0$, $x \mapsto x1$. Let $y \in K_2$ and let $b \in \{0, 1\}$. We need to show that $yb \in K_2$. Since $y, b \in K_2 \subseteq K_1$ and K_1 is closed under concatenation, $yb \in K_1$. Now, let $a \in \{0, 1\}$ and let $x \in K_1$. We need to show $xyb \neq a$. Assume for the sake of a contradiction that $xyb = a$. Then, $axyb = aa$. By ID_3 and ID_2, we have $axy = a$, which contradicts $y \in K_2$ since $ax \in K_1$ as $a, x \in K_1$ and K_1 is closed under concatenation. Thus, K_2 is closed under the maps $x \mapsto x0$, $x \mapsto x1$.

The class K_2 is not a domain since it may not be closed under concatenation. We obtain K by restricting K_2 to a subclass that contains 0 and 1 and is closed under concatenation. Let

$$K = \{w \in K_2 :\ \forall z \in K_2\ [\ zw \in K_2\ ]\ \}.$$

We have $0, 1 \in K$ since K_2 contains $0, 1$ and is closed under the maps $x \mapsto x0$, $x \mapsto x1$. We now show that K is closed under concatenation. Let $w_0, w_1 \in K$. We need to show that $w_0w_1 \in K$. Since $w_0 \in K \subseteq K_2$ and $w_1 \in K$, we have $w_0w_1 \in K_2$. Now, let $z \in K_2$. We need to show that $zw_0w_1 \in K_2$. We do not worry about parentheses since ID_1 tells us that concatenation is associative. Since $w_0 \in K$, we have $zw_0 \in K_2$. Since $w_1 \in K$, we have $zw_0w_1 \in K_2$. Hence, $w_0w_1 \in K$. Thus, K is closed under concatenation. □

3.2 Suffix relation

In this section, we show that we can extend $\mathsf{ID}^{(2)}$ to a theory where we have an axiom schema for the suffix relation, analogues to ID_4, without changing the interpretability degree. We extend the language of $\mathsf{ID}^{(2)}$ with a fresh binary relation symbol $\preceq_{\mathsf{suff}}$. Given a nonempty binary string α, let $\mathsf{Suff}(\alpha)$ denote the set of all nonempty suffixes of α: $\gamma \in \mathsf{Suff}(\alpha)$ if and only if $\alpha = \gamma$ or $\exists \delta \in \{\mathbf{0}, \mathbf{1}\}^+ \ [\ \alpha = \delta\gamma \ \wedge \ \gamma \in \{\mathbf{0}, \mathbf{1}\}^+ \ ]$. Let $\mathsf{ID}^{(3)}$ be $\mathsf{ID}^{(2)}$ extended with the following axiom schema

$$\forall x \left[\ x \preceq_{\mathsf{suff}} \overline{\alpha} \leftrightarrow \bigvee_{\gamma \in \mathsf{Suff}(\alpha)} x = \overline{\gamma} \ \right].$$

Lemma 4 ID *and* $\mathsf{ID}^{(3)}$ *are mutually interpretable.*

Proof Since $\mathsf{ID}^{(3)}$ is an extension of ID, it suffices by Lemma 3 to show that the suffix relation is definable in $\mathsf{ID}^{(2)}$. We translate the suffix relation as follows: $x \preceq_{\mathsf{suff}} y$ if and only if

(1) $y = x \ \vee \ \exists u \, [\ y = ux\ ]$
(2) $\forall u \preceq x \left[\ u = 0 \ \vee \ u = 1 \ \vee \ \exists v \preceq u \, [\ u = v0 \ \vee \ u = v1\ ]\ \right]$
(3) $\preceq$ is reflexive and transitive on the class $I_x = \{z : z \preceq x\}$, $x \in I_x$ and $\forall z \in I_x \ \forall w \preceq z \, [\ w \in I_x\ ]$.

Given a nonempty binary string α, we need to show that

$$\mathsf{ID}^{(2)} \vdash \forall x \left[\ x \preceq_{\mathsf{suff}} \overline{\alpha} \leftrightarrow \bigvee_{\gamma \in \mathsf{Suff}(\alpha)} x = \overline{\gamma} \ \right].$$

($\Leftarrow$)
We show that

$$\mathsf{ID}^{(2)} \vdash \forall x \left[\ \Big(\bigvee_{\gamma \in \mathsf{Suff}(\alpha)} x = \overline{\gamma} \ \Big) \to x \preceq_{\mathsf{suff}} \overline{\alpha} \ \right].$$

Let $\gamma \in \mathsf{Suff}(\alpha)$. We need to show that $\overline{\gamma} \preceq_{\mathsf{suff}} \overline{\alpha}$ holds. That is, we need to show that $\overline{\gamma}$ and $\overline{\alpha}$ satisfy (1)–(3). It is easy to prove by induction on the length of binary strings that

$$\mathsf{ID} \vdash \overline{\delta} \ \overline{\zeta} = \overline{\delta\zeta} \quad \text{for all } \delta, \zeta \in \{\mathbf{0}, \mathbf{1}\}^+ . \qquad (*)$$

By (*), $\overline{\alpha} = \overline{\gamma}$ or $\overline{\alpha} = \overline{\delta}\ \overline{\gamma}$ where δ is a prefix of α. Hence, (1) holds. By (*) and the axiom schema ID_4 for the prefix relation, $\overline{\gamma}$ satisfies (2)–(3). Thus, $\overline{\gamma} \preceq_{\mathsf{suff}} \overline{\alpha}$ holds.
($\Rightarrow$)

We need to show that

$$\mathsf{ID}^{(2)} \vdash \forall x \left[x \preceq_{\mathsf{suff}} \overline{\alpha} \rightarrow \bigvee_{\gamma \in \mathsf{Suff}(\alpha)} x = \overline{\gamma} \right]. \qquad (**)$$

We prove (**) by induction on the length of α. Assume $\alpha \in \{\mathbf{0}, \mathbf{1}\}$ and $x \preceq_{\mathsf{suff}} \overline{\alpha}$ holds. By (1), $x = \overline{\alpha}$ or there exist u such that $\overline{\alpha} = ux$. By $\mathsf{AT0}$ and $\mathsf{AT1}$, we have $x = \overline{\alpha}$. Thus, (**) holds when $\alpha \in \{\mathbf{0}, \mathbf{1}\}$.

We consider the inductive case. Assume $\alpha = \beta a$ where $a \in \{\mathbf{0}, \mathbf{1}\}$, $\beta \in \{\mathbf{0}, \mathbf{1}\}^+$ and

$$\mathsf{ID}^{(2)} \vdash \forall x \left[x \preceq_{\mathsf{suff}} \overline{\beta} \rightarrow \bigvee_{\gamma \in \mathsf{Suff}(\beta)} x = \overline{\gamma} \right]. \qquad (***)$$

By definition, $\overline{\alpha} = \overline{\beta a} = \overline{\beta}\,\overline{a}$. Assume $x \preceq_{\mathsf{suff}} \overline{\alpha}$ holds. By (1), $x = \overline{\alpha}$ or there exist u such that $\overline{\alpha} = ux$. If $x = \overline{\alpha}$, we are done. So, assume $\overline{\alpha} = ux$. By (3), we have $x \preceq x$. Then, by (2), we have one of the following cases: (i) there exists $b \in \{0, 1\}$ such that $b = x$, (ii) there exist $w \preceq x$ and $c \in \{0, 1\}$ such that $x = wc$. Assume (i) holds. We have $\overline{\beta}\,\overline{a} = \overline{\alpha} = ux = ub$. By ID_3, we have $\overline{a} = b = x$. Thus, $x = \overline{\gamma}$ where $\gamma \in \mathsf{Suff}(\alpha)$.

Assume (ii) holds. Then, $\overline{\beta}\,\overline{a} = \overline{\alpha} = ux = uwc$. By ID_3, we have $\overline{a} = c$. By ID_2, we have $\overline{\beta} = uw$. Furthermore

- $\forall u \preceq w\ \big[\ u = 0\ \vee\ u = 1\ \vee\ \exists v \preceq u\ [\ u = v0\ \vee\ u = v1\ ]\ \big]$ since $u \preceq w\ \wedge\ w \preceq x$ implies $u \preceq x$ by (3)
- since $w \preceq x$ and (3) holds, $\preceq$ is reflexive and transitive on the class $I_w = \{z : z \preceq w\}$, $w \in I_w$ and $\forall z \in I_w\ \forall w \preceq z\ [\ w \in I_w\ ]$.

Thus, $w \preceq_{\mathsf{suff}} \overline{\beta}$ holds. By (***), $w = \overline{\delta}$ where δ is a suffix of β. Then, $x = w\overline{a} = \overline{\delta}\,\overline{a} = \overline{\delta a}$ and δa is a suffix of α. Thus, α satisfies (**).

Thus, by induction, (**) holds for all nonempty binary strings α. □

3.3 Substring relation

In this section, we show that we can extend $\mathsf{ID}^{(3)}$ to a theory where we have an axiom schema for the substring relation, analogues to ID_4, without changing the interpretability degree. We extend the language of $\mathsf{ID}^{(3)}$ with a fresh binary relation symbol $\preceq_{\mathsf{sub}}$. Given a nonempty binary string α, let $\mathsf{Sub}(\alpha)$ denote the set of all nonempty substrings of α: $\beta \in \mathsf{Sub}(\alpha)$ if and only if $\alpha = \beta$ or there exist $\gamma, \delta \in \{\mathbf{0}, \mathbf{1}\}^+$ such that $\beta \in \{\mathbf{0}, \mathbf{1}\}^+$ and $\alpha = \gamma\beta\ \vee\ \alpha = \beta\delta\ \vee\ \alpha = \gamma\beta\delta$. Let $\mathsf{ID}^{(4)}$ be $\mathsf{ID}^{(3)}$ extended with the following axiom schema

$$\forall x \left[x \preceq_{\mathsf{sub}} \overline{\alpha} \leftrightarrow \bigvee_{\gamma \in \mathsf{Sub}(\alpha)} x = \overline{\gamma} \right].$$

Lemma 5 ID *and* $\mathsf{ID}^{(4)}$ *are mutually interpretable.*

Proof By Lemma 4, it suffices to show that the substring relation is definable in $\mathsf{ID}^{(3)}$. We translate the substring relation as follows

$$x \preceq_{\mathsf{sub}} y \equiv \; x \preceq y \;\vee\; x \preceq_{\mathsf{suff}} y \;\vee\; \exists u \preceq y \; [\, x \preceq_{\mathsf{suff}} u \,].$$

By the axiom schema for the prefix relation and the axiom schema for the suffix relation, it is easy to see that $\mathsf{ID}^{(3)}$ proves $\forall x \; [\, x \preceq_{\mathsf{sub}} \overline{\alpha} \leftrightarrow \bigvee_{\gamma \in \mathsf{Sub}(\alpha)} x = \overline{\gamma} \,]$ for each nonempty binary string α. □

3.4 Suffix relation II

We are finally ready to equip the suffix relation with two very important properties. Let $\mathsf{ID}^{(5)}$ be $\mathsf{ID}^{(4)}$ extended with the following axioms

$$\forall x \left[\bigwedge_{a \in \{0,1\}} a \preceq_{\mathsf{suff}} xa \right], \quad \forall xy \left[x \preceq_{\mathsf{suff}} y \rightarrow \bigwedge_{a \in \{0,1\}} xa \preceq_{\mathsf{suff}} ya \right].$$

To show that $\mathsf{ID}^{(5)}$ and ID are mutually interpretable, we need the following lemma. Recall that a class is a formula with at least one free variable and that if I is a class with one free variable we occasionally write $x \in I$ for $I(x)$.

Lemma 6 *There exists a class J with the following properties:*

(1) $\mathsf{ID}^{(4)} \vdash t \in J$ *for each variable-free term* t
(2) $\mathsf{ID}^{(4)} \vdash \forall x \, \forall z \in J \; \big[\; \bigwedge_{a \in \{0,1\}} (\, z = xa \rightarrow a \preceq_{\mathsf{suff}} z \,) \, \big]$
(3) $\mathsf{ID}^{(4)} \vdash \forall xy \, \forall z \in J \; \big[\; \bigwedge_{a \in \{0,1\}} \big(\, (\, z = ya \;\wedge\; x \preceq_{\mathsf{suff}} y \,) \rightarrow (\, xa \preceq_{\mathsf{suff}} z \,) \, \big) \big]$
(4) $\mathsf{ID}^{(4)} \vdash \forall z \in J \; \big[\, z = 0 \;\vee\; z = 1 \;\vee\; \exists u \preceq_{\mathsf{sub}} z \, [\, z = u0 \;\vee\; z = u1 \,] \, \big]$
(5) $\mathsf{ID}^{(4)} \vdash \forall z \in J \; \forall u \, \big[\, u \preceq_{\mathsf{sub}} z \rightarrow u \in J \, \big]$.

Proof We define J as follows: $u \in J$ if and only if

(i) $u \preceq_{\mathsf{sub}} u$
(ii) $\forall w \preceq_{\mathsf{sub}} u \; [\, w \preceq_{\mathsf{sub}} w \,]$
(iii) $\forall w \preceq_{\mathsf{sub}} u \; \forall v_0 \preceq_{\mathsf{sub}} w \; \forall v_1 \preceq_{\mathsf{sub}} v_0 \; [\, v_1 \preceq_{\mathsf{sub}} w \,]$

(A) $\forall w \preceq_{\mathsf{sub}} u \; [\, w = 0 \;\vee\; w = 1 \;\vee\; \exists v \preceq_{\mathsf{sub}} w \; [\, w = v0 \;\vee\; w = v1 \,] \,]$.
(B) $\forall w \preceq_{\mathsf{sub}} u \; \forall x \; [\, w = x0 \rightarrow 0 \preceq_{\mathsf{suff}} w \,]$
(C) $\forall w \preceq_{\mathsf{sub}} u \; \forall x \; [\, w = x1 \rightarrow 1 \preceq_{\mathsf{suff}} w \,]$

(D) $\forall w \preceq_{\mathsf{sub}} u \, \forall xy \, [\, (\, w = y0 \, \wedge \, x \preceq_{\mathsf{suff}} y \,) \rightarrow x0 \preceq_{\mathsf{sub}} w \,]$
(E) $\forall w \preceq_{\mathsf{sub}} u \, \forall xy \, [\, (\, w = y1 \, \wedge \, x \preceq_{\mathsf{suff}} y \,) \rightarrow x1 \preceq_{\mathsf{sub}} w \,]$.

It follows straight from the definition that J satisfies clauses (2)–(4). By the axiom schema for the substring relation, the axiom schema for the suffix relation, $\mathsf{AT0}$, $\mathsf{AT1}$, ID_2 and ID_3, J satisfies Clause (1). It remains to show that J also satisfies Clause (5). That is, we need to show that J is downward closed under $\preceq_{\mathsf{sub}}$. So, assume $u' \preceq_{\mathsf{sub}} u \in J$. We need to show that $u' \in J$. That is, we need to show that u' satisfies (i)–(iii) and (A)–(E). We show that u' satisfies (i). Since u satisfies (ii), $u' \preceq_{\mathsf{sub}} u$ implies $u' \preceq_{\mathsf{sub}} u'$. Thus, u' satisfies (i).

We show that u' satisfies (ii)–(iii) and (A)–(E). Consider one of these clauses. It is of the form $\forall w \preceq_{\mathsf{sub}} u' \, \phi(w)$. We need to show that $\forall w \preceq_{\mathsf{sub}} u' \, \phi(w)$ holds. Since $u \in J$, we know that $\forall w \preceq_{\mathsf{sub}} u \, \phi(w)$ holds. Let $w \preceq_{\mathsf{sub}} u'$. We need to show that $\phi(w)$ holds. Since $\forall w \preceq_{\mathsf{sub}} u \, \phi(w)$ holds, it suffices to show that $w \preceq_{\mathsf{sub}} u$ holds. By assumption

$$w \preceq_{\mathsf{sub}} u' \preceq_{\mathsf{sub}} u .$$

Since u satisfies (i)

$$w \preceq_{\mathsf{sub}} u' \preceq_{\mathsf{sub}} u \preceq_{\mathsf{sub}} u .$$

Then, $w \preceq_{\mathsf{sub}} u$ since u satisfies (iii). Hence, $\forall w \preceq_{\mathsf{sub}} u' \, \phi(w)$ holds. Thus, u' satisfies clauses (ii)–(iii), (A)–(E).

Since u' satisfies (i)–(iii) and (A)–(E), $u' \in J$. Thus, J is downward closed under $\preceq_{\mathsf{sub}}$. □

Lemma 7 ID *and* $\mathsf{ID}^{(5)}$ *are mutually interpretable.*

Proof By Lemma 5, it suffices to show that $\mathsf{ID}^{(5)}$ is interpretable in $\mathsf{ID}^{(4)}$. Let J be the class given by Lemma 6. To interpret $\mathsf{ID}^{(5)}$ in $\mathsf{ID}^{(4)}$ it suffices to translate the suffix relation as follows

$$x \preceq^{\tau}_{\mathsf{suff}} y \equiv \, (\, y \in J \, \wedge \, x \preceq_{\mathsf{suff}} y \,) \, \vee \, (\, y \notin J \, \wedge \, x = x \,).$$

We need show that the translation of each instance of the axiom schema for the suffix relation is a theorem of $\mathsf{ID}^{(4)}$. Let α be a nonempty binary string. We need to show that

$$\forall x \left[\, x \preceq^{\tau}_{\mathsf{suff}} \overline{\alpha} \leftrightarrow \bigvee_{\gamma \in \mathsf{Suff}(\alpha)} x = \overline{\gamma} \, \right] \tag{A}$$

holds. By Clause (1) of Lemma 6, $\overline{\alpha} \in J$. Hence, by the definition of $\preceq^{\tau}_{\mathsf{suff}}$, (A) holds if and only if

$$\forall x \left[x \preceq_{\mathsf{suff}} \overline{\alpha} \leftrightarrow \bigvee_{\gamma \in \mathsf{Suff}(\alpha)} x = \overline{\gamma} \right] \tag{B}$$

holds. Observe that (B) is an instance of the axiom schema for the suffix relation. Thus, the translation of each instance of the axiom schema for the suffix relation is a theorem of $\mathsf{ID}^{(4)}$.

We need to show that the translation of the axiom

$$\forall x \left[\bigwedge_{a \in \{0,1\}} a \preceq_{\mathsf{suff}} xa \right] \tag{C}$$

is a theorem of $\mathsf{ID}^{(4)}$. Let x be arbitrary and let $a \in \{0, 1\}$. We need to show that $a \preceq^{\tau}_{\mathsf{suff}} xa$ holds. Assume $xa \in J$. Then, $a \preceq^{\tau}_{\mathsf{suff}} xa$ holds if and only if $a \preceq_{\mathsf{suff}} xa$ holds. By Clause (2) of Lemma 6, $a \preceq_{\mathsf{suff}} xa$ holds. Hence, $a \preceq^{\tau}_{\mathsf{suff}} xa$ holds when $xa \in J$. Assume now $xa \notin J$. Then, $a \preceq^{\tau}_{\mathsf{suff}} xa$ holds by the second disjunct in the definition of $\preceq^{\tau}_{\mathsf{suff}}$. Thus, the translation of (C) is a theorem of $\mathsf{ID}^{(4)}$.

We need to show that the translation of the axiom

$$\forall xy \left[x \preceq_{\mathsf{suff}} y \to \bigwedge_{a \in \{0,1\}} xa \preceq_{\mathsf{suff}} ya \right] \tag{D}$$

is a theorem of $\mathsf{ID}^{(4)}$. Let $a \in \{0, 1\}$ and assume $x \preceq^{\tau}_{\mathsf{suff}} y$. We need to show that $xa \preceq^{\tau}_{\mathsf{suff}} ya$ holds. Assume first $ya \notin J$. Then, $xa \preceq^{\tau}_{\mathsf{suff}} ya$ holds by the second disjunct in the definition of $\preceq^{\tau}_{\mathsf{suff}}$. Assume next $ya \in J$. Then, by Clause (4) of Lemma 6, $ya \in \{0, 1\}$ or there exist $u \preceq_{\mathsf{sub}} ya$ and $b \in \{0, 1\}$ such that $ya = ub$. By $\mathsf{AT0}$, $\mathsf{AT1}$ and ID_3, we have $ya = ua$ where $u \preceq_{\mathsf{sub}} ya$. By ID_2, we have $y = u$. Hence, $y \preceq_{\mathsf{sub}} ya$. By Clause (5) of Lemma 6, $y \in J$. Thus, since $x \preceq^{\tau}_{\mathsf{suff}} y$ holds and $y \in J$, we have $x \preceq_{\mathsf{suff}} y$ by the definition of $\preceq^{\tau}_{\mathsf{suff}}$. Then, by Clause (3) of Lemma 6, $xa \preceq_{\mathsf{suff}} ya$ holds. Thus, the translation of (D) is a theorem of $\mathsf{ID}^{(4)}$. □

3.5 Interpretation of ID* in ID

We are finally ready to show that ID^* and ID are mutually interpretable.

Theorem 8 *The theories* ID, ID^* *are mutually interpretable.*

Proof To interpret ID in ID^*, it suffices to translate $\preceq$ as follows

$$x \preceq y \equiv \; y = x \; \vee \; \exists z \, [\, y = xz \,].$$

Given a nonempty binary string α, we have

$$\begin{aligned} x \preceq \overline{\alpha} &\Leftrightarrow \overline{\alpha} = x \vee \exists z \, [\, \overline{\alpha} = xz \,] \\ &\Leftrightarrow \overline{\alpha} = x \vee \\ &\quad \exists z \, [\, x \sqsubseteq_{\mathsf{s}} \overline{\alpha} \ \wedge \ z \sqsubseteq_{\mathsf{s}} \overline{\alpha} \ \wedge \ \overline{\alpha} = xz \,] \qquad (\text{def. of } \sqsubseteq_{\mathsf{s}}\,) \\ &\Leftrightarrow \overline{\alpha} = x \vee \\ &\quad \bigvee_{\beta,\gamma \in \mathsf{Sub}(\alpha)} (\, x = \overline{\beta} \wedge z = \overline{\gamma} \wedge \overline{\beta}\,\overline{\gamma} = \overline{\alpha}\,) \qquad (\mathsf{ID}_4^*) \\ &\Leftrightarrow \bigvee_{\beta \in \mathsf{Pref}(\alpha)} x = \overline{\beta} \qquad (\mathsf{ID}_1 - \mathsf{ID}_3). \end{aligned}$$

This shows that the translation of each instance of the axiom schema ID_4 is a theorem of ID^*. Thus, ID is interpretable in ID^*.

Next, we show that ID^* is interpretable in ID. By Lemma 7, it suffices to show that ID^* is interpretable in $\mathsf{ID}^{(5)}$. Since the axioms of ID^* are universal sentences or sentences where existential quantifiers occur in the antecedent (instances of ID_4^*), to interpret ID^* in $\mathsf{ID}^{(5)}$ it suffices to relativize quantification to a suitable domain K.

We start by defining an auxiliary class K_1 (this is why we extended $\mathsf{ID}^{(4)}$ to $\mathsf{ID}^{(5)}$). Let

$$K_1 = \{u : \ \forall x \, [\, u \preceq_{\mathsf{suff}} xu \,] \,\}.$$

By the axiom $\forall x \, [\, \bigwedge_{a \in \{0,1\}} a \preceq_{\mathsf{suff}} xa \,]$, we have $0, 1 \in J$. We show that K_1 is closed under the maps $u \mapsto u0, \ u \mapsto u1$. Let $b \in \{0, 1\}$ and let $u \in K_1$. We need to show that $ub \in K_1$. That is, we need to show that $ub \preceq_{\mathsf{suff}} xub$ for all x. Since $u \in K_1$, we know that

$$\forall x \, [\, u \preceq_{\mathsf{suff}} xu \,] \qquad (*)$$

holds. Then, by (*) and the axiom

$$\forall xy \left[\, x \preceq_{\mathsf{suff}} y \to \bigwedge_{a \in \{0,1\}} xa \preceq_{\mathsf{suff}} ya \, \right]$$

we have

$$\forall x \, [\, ub \preceq_{\mathsf{suff}} xub \,].$$

Hence, $ub \in K_1$. Thus, K_1 is closed under the maps $u \mapsto u0, \ u \mapsto u1$.

The class K_1 is not a domain since it may not be closed under concatenation. We let

$$K = \{u \in K_1 : \ \forall v \in K_1 \, [\, vu \in K_1 \,] \,\}.$$

Since K_1 contains 0 and 1 and is closed under the maps $x \mapsto x0,\ x \mapsto x1$, we have $0, 1 \in K$. We show that K is closed under concatenation. Let $u_0, u_1 \in K$. We need to show that $u_0u_1 \in K$. We start by showing that $u_0u_1 \in K_1$. We have $u_0 \in K \subseteq K_1$. Hence, $u_0u_1 \in K_1$ since $u_1 \in K$. Next, we need to show that $\forall v \in K_1[\ vu_0u_1 \in K_1\ ]$. We do not need to worry about parentheses since ID_1 tells us that concatenation is associative. Let $v \in K_1$. We need to show that $vu_0u_1 \in K_1$. Since $u_0 \in K$, we have $vu_0 \in K_1$. Since $u_1 \in K$, we have $vu_0u_1 \in K_1$. Hence, $u_0u_1 \in K$. Thus, K is closed under concatenation and therefore satisfies the domain conditions.

Since the axioms ID_1, ID_2, ID_3 are universal sentences, their restrictions to K are theorems of $\mathsf{ID}^{(5)}$. It remains to show that the restriction to K of each instance of

$$\mathsf{ID}_4^* \equiv \forall x \left[\ x \sqsubseteq_{\mathsf{s}} \overline{\alpha} \rightarrow \bigvee_{\gamma \in \mathsf{Sub}(\alpha)} x = \overline{\gamma}\ \right]$$

is a theorem of $\mathsf{ID}^{(5)}$. It suffices to show that for each nonempty binary string α

$$\forall x, y \in K\big[\ xy = \overline{\alpha}\ \rightarrow \bigvee_{\beta,\gamma \in \mathsf{Sub}(\alpha)} (\ x = \overline{\gamma}\ \wedge\ y = \overline{\beta}\ )\ \big]. \qquad (**)$$

So, let $x, y \in K$ and assume $xy = \overline{\alpha}$. Since $y \in K \subseteq K_1$, we know that $y \preceq_{\mathsf{suff}} xy = \overline{\alpha}$. By the axiom schema for the suffix relation, $y = \overline{\beta}$ where β is a nonempty suffix of α. So, $x\overline{\beta} = \overline{\alpha}$. By ID_1, ID_2, ID_3, $\mathsf{AT0}$, $\mathsf{AT1}$, we have that $x = \overline{\gamma}$ where γ is a nonempty prefix of α such that $\alpha = \gamma\beta$. Thus, (**) hols for all nonempty binary strings α. Thus, the translation of each instance of ID_4^* is a theorem of $\mathsf{ID}^{(5)}$. $\square$

3.6 The theories $\overline{\mathsf{ID}}$, $\overline{\mathsf{ID}}^*$

The axioms ID_1, ID_2, ID_3 describe a right cancellative semigroup. It is also natural to consider semigroups that are also left cancellative, for example $(\{\mathbf{0}, \mathbf{1}\}^+, \mathbf{0}, \mathbf{1}, ^\frown)$. Let $\overline{\mathsf{ID}}$ and $\overline{\mathsf{ID}}^*$ be ID and ID^*, respectively, extended with the axioms

$$\forall xy\ [\ x \neq y \rightarrow (\ 0x \neq 0y\ \wedge\ 1x \neq 1y\ )\ ],\ \ \forall xy\ [\ 0x \neq 1y\ ].$$

It is not difficult to see that TC proves each axiom of $\overline{\mathsf{ID}}^*$. It is easily seen that our interpretation of ID^* in ID is also an interpretation of $\overline{\mathsf{ID}}^*$ in $\overline{\mathsf{ID}}$. Thus, $\overline{\mathsf{ID}}$ and $\overline{\mathsf{ID}}^*$ are mutually interpretable. We have not been able to determine whether $\overline{\mathsf{ID}}$ is interpretable in ID.

Theorem 9 $\overline{\mathsf{ID}}$ *and* $\overline{\mathsf{ID}}^*$ *are mutually interpretable.*

Open Problem 10 *Is* $\overline{\mathsf{ID}}$ *interpretable in* ID*?*

4 Mutual interpretability of IQ and IQ*

In this section, we show that IQ and IQ^* are also mutually interpretable. Recall that IQ^* is the theory we obtain from IQ by removing $\leq$ from the language and replacing the axiom schema IQ_3 with the axiom schema

$$\mathsf{IQ}_3^* \equiv \forall x \left[\, x \leq_{\mathsf{I}} \overline{n} \rightarrow \bigvee_{k \leq n} x = \overline{k} \, \right]$$

where $x \leq_{\mathsf{I}} y \equiv \exists z \, [\, z + x = y \,]$.

Theorem 11 IQ *and* IQ^* *are mutually interpretable.*

The proof strategy is similar to the one we used to interpret ID^* in ID. Since we obtain an interpretation of IQ in IQ^* by translating $\leq$ as $\leq_{\mathsf{I}}$, we just need to focus on proving that IQ^* is interpretable in IQ. The proof is structured as follows: In Sect. 4.1, we extend IQ to a theory IQ^+ which proves that for each inductive class there exists a an inductive subclass that is closed under addition and multiplication. A class is inductive if it contains 0 and is closed under the successor function. In Sect. 4.2, we extend IQ^+ to a theory IQ^{++} with the same interpretability degree as IQ^+ and where the ordering relation $\leq$ satisfies additional properties. In Sect. 4.3, we show that IQ^* is interpretable in IQ^+. Finally, in Sect. 7, we show that IQ is mutually interpretable with a theory $\mathsf{IQ}^{(2)}$ that is an extension of IQ^+.

4.1 Closure under addition and multiplication

A class X is called inductive if $0 \in X$ and $\forall x \in X \, [\, Sx \in X \,]$. A class X is called a cut if it is inductive and $\forall x \in X \, \forall y \, [\, y \leq_{\mathsf{I}} x \rightarrow y \in X \,]$. Let IQ^+ and Q^+ be respectively IQ and Q extended with the following axioms

- Associativity of addition $\forall xyz \, [\, (x + y) + z = x + (y + z) \,]$
- Left distributive law $\forall xyz \, [\, x(y + z) = xy + xz \,]$
- Associativity of multiplication $\forall xyz \, [\, (xy)z = x(yz) \,]$.

Lemma V.5.10 of Hajek and Pudlak [4] says that Q^+ proves that any inductive class has a subclass that is a cut and is closed under $+$ and $\times$. The proof of that lemma shows that IQ^+ proves that any inductive class has an inductive subclass that is closed under $+$ and $\times$ (see also Sect. 7).

Lemma 12 *Let X be an inductive class. Then,* IQ^+ *proves that there exists an inductive subclass Y that is closed under $+$ and $\times$.*

4.2 Ordering relation

Let IQ^{++} be IQ^+ extended with the following axioms

$$\forall x \, [\, 0 \leq x \,], \quad \forall xy \, [\, x \leq y \rightarrow Sx \leq Sy \,]$$

Using the ideas of Sect. 3.4, we prove the following lemma.

Lemma 13 IQ^+ *and* IQ^{++} *are mutually interpretable.*

Proof Since IQ^{++} is an extension of IQ^+, it suffices to show that IQ^{++} is interpretable in IQ^+. Furthermore, it suffices to show that we can translate $\leq$ in such a way that IQ^+ proves the translation of each instance of IQ_3 and the translation of $\forall x\ [\ 0 \leq x\ ]$ and $\forall xy\ [\ x \leq y \rightarrow Sx \leq Sy\ ]$.

Let $u \in G$ if and only if

(1) $u \leq u$
(2) $\forall w \leq u\ [\ w \leq w\ ]$
(3) $\forall w \leq u\ \forall v_0 \leq w\ \forall v_1 \leq v_0\ [\ v_1 \leq w\ ]$

(A) $\forall w \leq u\ [\ w = 0\ \vee\ \exists v \leq w\ [\ w = \mathrm{S}v\ ]$
(B) $\forall w \leq u\ \forall x\ [\ w = \mathrm{S}x \rightarrow 0 \leq w\ ]$
(C) $\forall w \leq u\ \forall xy\ [\ (\ w = \mathrm{S}y\ \wedge\ x \leq y\ ) \rightarrow \mathrm{S}x \leq w\ ]$.

It can be verified that IQ proves that $t \in G$ for each variable-free term t and that G is downward closed under $\leq$.

We translate $\leq$ as follows

$$x \leq^{\tau} y \equiv\ (\ y \in G\ \wedge\ x \leq y\ )\ \vee\ (\ y \notin G\ \wedge\ x = x\ ).$$

Since $t \in G$ for each variable-free term t, the translation of each instance of the axiom schema IQ_3 is a theorem of IQ^+.

We show that IQ^+ proves the translation of $\forall x\ [\ 0 \leq x\ ]$. Choose an arbitrary x. If $x \notin G$, then $0 \leq^{\tau} x$ holds by the second disjunct in the definition of $\leq^{\tau}$. Otherwise, $x \in G$. We need to show that $0 \leq x$ holds. If $x = 0$, then $0 \leq x$ holds by IQ_3. Otherwise, by (A), there exists $v \leq x$ such that $x = \mathrm{S}v$. Then, by (B), $0 \leq x$ holds. Thus, $\mathsf{IQ}^+ \vdash \forall x\ [\ 0 \leq^{\tau} x\ ]$.

We show that IQ^+ proves the translation of $\forall xy\ [\ x \leq y \rightarrow \mathrm{S}x \leq \mathrm{S}y\ ]$. Assume $x \leq y$ holds. If $\mathrm{S}y \notin G$, then $\mathrm{S}x \leq^{\tau} \mathrm{S}y$ holds by the second disjunct in the definition of $\leq^{\tau}$. Otherwise, $\mathrm{S}y \in G$. We need to show that $\mathrm{S}x \leq \mathrm{S}y$ holds. By Q_2, $\mathrm{S}y \neq 0$. Hence, by (A), there exists $v \leq \mathrm{S}y$ such that $\mathrm{S}y = \mathrm{S}v$. By Q_1, $y = v$. Hence, $y \leq \mathrm{S}y$. Since G is downward closed under $\leq$, we have $y \in G$. Then, by (C), $\mathrm{S}x \leq \mathrm{S}y$ holds. Thus, $\mathsf{IQ}^+ \vdash \forall xy\ [\ x \leq^{\tau} y \rightarrow \mathrm{S}x \leq^{\tau} \mathrm{S}y\ ]$. □

4.3 Interpretation of IQ* in IQ$^+$

Lemma 14 IQ^* *is interpretable in* IQ^+.

Proof By Lemma 13, it suffices to show that IQ^* is interpretable in IQ^{++}. We interpret IQ^* in IQ^{++} by simply restricting the universe of IQ^{++} to an inductive subclass K that is closed under $+$, $\times$ and which is such that IQ^{++} proves that $\forall x, u \in K\ [\ u \leq x + u\ ]$.

Let

$$K_1 = \{u :\ \forall x\ [\ u \leq x + u\ ]\ \}$$

We have $0 \in K_1$ by the axiom $\forall x\ [\ 0 \leq x\ ]$ and Q_4. We show that K_1 is closed under S. Let $u \in K_1$. We need to show that $\mathrm{S}u \in K_1$. That is, we need to show that

$\mathrm{S}u \leq x + \mathrm{S}u$. Since $u \in K_1$, we have $u \leq x + u$. Then, $\mathrm{S}u \leq \mathrm{S}(x + u)$ by the axiom $\forall xy\ [\ x \leq y \rightarrow \mathrm{S}x \leq \mathrm{S}y\ ]$. By Q_5, we have

$$\mathrm{S}u \leq \mathrm{S}(x + u) = x + \mathrm{S}u.$$

Hence, $\mathrm{S}u \in K_1$. Thus, K_1 contains 0 and is closed under S. By Lemma 12, there exists an inductive subclass K of K_1 that is closed under $+$ and $\times$.

We interpret IQ^* in IQ^{++} by relativizing quantification to K. The translation of each one of the axioms $\mathsf{Q}_1 - \mathsf{Q}_2$, $\mathsf{Q}_4 - \mathsf{Q}_7$ is a theorem of IQ^{++} since universal sentences are absolute for K. It remains to show that each instance of IQ_3^* is a theorem of IQ^{++}. Choose a natural number n. We need to show that

$$\mathsf{IQ}^{++} \vdash \forall x, y \in K \left[x + y = \overline{n} \rightarrow \bigvee_{k \leq n} y = \overline{k} \right].$$

Assume $x, y \in K$ and $x + y = \overline{n}$. Since $y \in K \subseteq K_1$, we have $y \leq \overline{n}$. By the axiom schema IQ_3, there exists $k \leq n$ such that $y = \overline{k}$. Thus, IQ^{++} proves the translation of each instance of IQ_3^*. □

5 Interpretability of $\overline{\mathsf{ID}}$ in IQ

In this section, we show that $\overline{\mathsf{ID}}$ is interpretable in IQ (see Fig. 5 for the axioms of $\overline{\mathsf{ID}}$ and IQ). The most intuitive way to interpret concatenation theories in arithmetical theories is to construct a formula $\phi_\circ(x, y, z)$ that given x and y defines an object that encodes a

Fig. 5 Non-logical axioms of the first-order theories $\overline{\mathsf{ID}}$ and IQ

The Axioms of $\overline{\mathsf{ID}}$

ID_1 $\forall xyz\ [\ (xy)z = x(yz)\ ]$
ID_2 $\forall xy\ [\ x \neq y \rightarrow (\ x0 \neq y0 \wedge x1 \neq y1\ )\ ]$
ID_3 $\forall xy\ [\ x0 \neq y1\ ]$
ID_4 $\forall x\ [\ x \preceq \overline{\alpha} \leftrightarrow \bigvee_{\gamma \in \mathsf{Pref}(\alpha)} x = \overline{\gamma}\ ]$
$\overline{\mathsf{ID}}_5$ $\forall xy\ [\ x \neq y \rightarrow (\ 0x \neq 0y \wedge 1x \neq 1y\ )\ ]$
$\overline{\mathsf{ID}}_6$ $\forall xy\ [\ 0x \neq 1y\ ]$

The Axioms of IQ

Q_1 $\forall xy\ [\ x \neq y \rightarrow \mathrm{S}x \neq \mathrm{S}y\ ]$
Q_2 $\forall x\ [\ \mathrm{S}x \neq 0\ ]$
Q_4 $\forall x\ [\ x + 0 = x\ ]$
Q_5 $\forall xy\ [\ x + \mathrm{S}y = \mathrm{S}(x + y)\ ]$
Q_6 $\forall x\ [\ x \times 0 = 0\ ]$
Q_7 $\forall xy\ [\ x \times \mathrm{S}y = x \times y + x\ ]$
IQ_3 $\forall x\ [\ x \leq \overline{n} \leftrightarrow \bigvee_{k \leq n} x = \overline{k}\ ]$

computation of $x \circ y$. Unfortunately, IQ does not have the resources necessary to prove that we can find a domain I on which $\phi_\circ(x, y, z)$ defines a function that satisfies ID_1, ID_2, ID_3, $\overline{\mathsf{ID}}_5$, $\overline{\mathsf{ID}}_6$. To prove correctness of recursive definition in Robinson Arithmetic Q, we rely on the axiom $\mathsf{Q}_3 \equiv \forall x\ [\ x = 0\ \vee\ \exists y\ [\ x = Sy\ ]\ ]$. The axiom schema $\mathsf{IQ}_3 \equiv \forall x\ [\ x \leq \overline{n} \leftrightarrow \bigvee_{k \leq n} x = \overline{k}\ ]$ can only allow us to verify that $\phi_\circ(x, y, z)$ gives a correct value z when x and y represent variable-free terms. Thus, to interpret $\overline{\mathsf{ID}}$ in IQ, we need a conception of strings as numbers that allows us to translate concatenation without coding sequences. The translation needs to also be simple enough that we can prove its correctness in IQ. In Lemma 4 of [2], Ganea explains how we can translate concatenation as a Δ_0-formula in strong theories such as Peano Arithmetic PA and $\mathsf{I}\Delta_0$.

Although we show that $\overline{\mathsf{ID}}$ is interpretable in IQ, we have not been able to determine whether the converse holds.

Open Problem 15 *Is* IQ *interpretable in* $\overline{\mathsf{ID}}$*?*

As mentioned, the main result of this section is the following theorem.

Theorem 16 $\overline{\mathsf{ID}}$ *is interpretable in* IQ.

The proof of the theorem is structured as follows: In Sect. 5.1, we explain how we intend to interpret $\overline{\mathsf{ID}}$ in IQ. In Sect. 5.2, we use this idea to give a simple interpretation of WD in R. In Sect. 5.3, we show that we can interpret $\overline{\mathsf{ID}}$ in an extension of IQ which we denote $\mathsf{IQ}^{(2)}$. Finally, in Sect. 7, we show that IQ and $\mathsf{IQ}^{(2)}$ are mutually interpretable.

5.1 Strings as matrices

The idea is to think of strings as 2×2 matrices and to translate concatenation as matrix multiplication. Let us first see how we can use this idea to give a 4-dimensional interpretation of $(\{\mathbf{0}, \mathbf{1}\}^*, \varepsilon, \mathbf{0}, \mathbf{1}, ^\frown)$ in $(\mathbb{N}, 0, 1, +, \times)$, where ε denotes the empty string and $\{\mathbf{0}, \mathbf{1}\}^* = \{\mathbf{0}, \mathbf{1}\}^+ \cup \{\varepsilon\}$. Let

$$\varepsilon^\tau := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \mathbf{0}^\tau := \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \qquad \mathbf{1}^\tau := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Let $\mathbf{SL}_2(\mathbb{N})$ denote the monoid generated by $\mathbf{0}^\tau$ and $\mathbf{1}^\tau$ under matrix multiplication. The monoid $\mathbf{SL}_2(\mathbb{N})$ is a substructure of the special linear group $\mathbf{SL}_2(\mathbb{Z})$ of 2×2 matrices with integer coefficients and determinant 1; the two matrices $\mathbf{0}^\tau$ and $\mathbf{1}^\tau$ generate $\mathbf{SL}_2(\mathbb{Z})$. Let $\times$ denote matrix multiplication. Then, $(\{\mathbf{0}, \mathbf{1}\}^*, \varepsilon, \mathbf{0}, \mathbf{1}, ^\frown)$ is isomorphic to $(\mathbf{SL}_2(\mathbb{N}), \varepsilon^\tau, \mathbf{0}^\tau, \mathbf{1}^\tau, \times)$. Since $\mathbf{SL}_2(\mathbb{N})$ is the set of 2×2 matrices with natural number coefficients and determinant 1, the isomorphism defines a 4-dimensional interpretation of $(\{\mathbf{0}, \mathbf{1}\}^*, \varepsilon, \mathbf{0}, \mathbf{1}, ^\frown)$ in $(\mathbb{N}, 0, 1, +, \times)$. The idea is to specify an interpretation of $\overline{\mathsf{ID}}$ in IQ by building on this interpretation of $(\{\mathbf{0}, \mathbf{1}\}^*, \varepsilon, \mathbf{0}, \mathbf{1}, ^\frown)$ in $(\mathbb{N}, 0, 1, +, \times)$. But we need to be careful since the axioms $\mathsf{IQ}_1 - \mathsf{IQ}_2$, $\mathsf{IQ}_4 - \mathsf{IQ}_7$ have many models.

In Lemma 11 of [10], we use this idea of associating strings with matrices to prove that $\mathsf{ID}_1 - \mathsf{ID}_3$ has a decidable model. We prove this result by giving a 4-dimensional interpretation of $\mathsf{ID}_1 - \mathsf{ID}_3$ in the first-order theory of the real closed

(I)	Left distributivity	$\forall xyz\ [\ x(y+z) = xy + xz\ ]$
(II)	Associativity of $+$	$\forall xyz\ [\ (x+y)+z = x+(y+z)\ ]$
(III)	Associativity of $\times$	$\forall xyz\ [\ (xy)z = x(yz)\ ]$
(IV)	Commutativity of $+$	$\forall xy\ [\ x+y = y+x\ ]$
(V)	Commutativity of $\times$	$\forall xy\ [\ xy = yx\ ]$
(VI)	Right cancellation	$\forall xyz\ [\ x+z = y+z \rightarrow x = y\ ]$
(VII)	Nonnegative Elements	$\forall xy\ [\ x+y = 0 \rightarrow (\ x = 0\ \wedge\ y = 0\ )\ ]$
(VIII)	No Zero Divisors	$\forall xy\ [\ xy = 0 \rightarrow (\ x = 0\ \vee\ y = 0\ )\ ]$.

Fig. 6 Algebraic properties we need in order to interpret $\overline{\mathsf{ID}}$ in IQ

field $(\mathbb{R}, 0, 1, +, \times, \leq)$, which is decidable (see Tarski [11]). At the time, we were investigating whether it is possible to remove some of the axioms of D and obtain a theory that is essentially undecidable. The possibility of interpreting $\overline{\mathsf{ID}}$ in IQ resulted from a careful investigation of the algebraic properties of $(\mathbb{R}, 0, 1, +, \times, \leq)$ we need to interpret $\mathsf{ID}_1 - \mathsf{ID}_3$. Properties (I)–(VIII) in Fig. 6 are sufficient to interpret $\overline{\mathsf{ID}}$ in IQ. Extending IQ with (I)–(VIII) allows us to reason about natural numbers in the standard way. In the rest of the paper, we use the Roman numerals (I)–(VIII) to refer exclusively to axioms (I)–(VIII) in Fig. 6.

The 4-dimensional interpretation of $(\{\mathbf{0}, \mathbf{1}\}^*, \varepsilon, \mathbf{0}, \mathbf{1}, ^\frown)$ in $(\mathbb{N}, 0, 1, +, \times)$ we described is a many-to-one reduction that maps existential sentences to existential sentences. This means that unsolvability of equations over $(\{\mathbf{0}, \mathbf{1}\}^*, \varepsilon, \mathbf{0}, \mathbf{1}, ^\frown)$ implies unsolvability of equations over $(\mathbb{N}, 0, 1, +, \times)$. The idea of associating $(\{\mathbf{0}, \mathbf{1}\}^*, \varepsilon, \mathbf{0}, \mathbf{1}, ^\frown)$ with $\mathbf{SL}_2(\mathbb{N})$ dates back to Markov [9]. According to Lothaire [7] (see p. 387), in the 1950s, A. A. Markov hoped that Hilbert‘s 10th Problem could be solved by proving unsolvability of word equations, that is, equations over finitely generated free semigroups. In 1970, Yuri Matiyasevich proved that Hilbert‘s 10th Problem is undecidable using a completely different method (see for example Davis [1]). In 1977, Makanin [8] proved that the existential theory of a finitely generated free semigroup is decidable.

5.2 Interpretation of WD in R

In this section, we show that the isomorphism between $(\{\mathbf{0}, \mathbf{1}\}^*, \varepsilon, \mathbf{0}, \mathbf{1}, ^\frown)$ and $\mathbf{SL}_2(\mathbb{N})$ defines a very simple interpretation of WD in R.

Lemma 17 *Let τ be the 4-dimensional translation of $\{0, 1, \circ\}$ in $\{0, \mathrm{S}, +, \times\}$ defined as follows*

– *0 and* 1 *are translated as* $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, *respectively*
– $\circ$ *is translated as matrix multiplication*
– *the domain is the class of all* 2×2 *matrices* $\begin{pmatrix} x & y \\ z & w \end{pmatrix}$.

Then, τ *extends to a translation of* $\{0, 1, \circ, \preceq\}$ *in* $\{0, \mathrm{S}, +, \times, \leq\}$ *that defines a* 4*-dimensional interpretation of* WD *in* R.

Proof By the axiom schemas $\mathsf{R}_1 \equiv \overline{n} + \overline{m} = \overline{n+m}$, $\mathsf{R}_2 \equiv \overline{n} \times \overline{m} = \overline{n \times m}$, R proves the translation of each instance of $\mathsf{WD}_1 \equiv \overline{\alpha}\ \overline{\beta} = \overline{\alpha\beta}$. By the axiom schema R_3, R proves the translation of each instance of WD_2. It remains to give a translation of $\preceq$ that provably satisfies the axiom schema

$$\mathsf{WD}_3 \equiv \forall x \left[x \preceq \overline{\alpha} \leftrightarrow \bigvee_{\gamma \in \mathsf{Pref}(\alpha)} x = \overline{\gamma} \right].$$

This is where we use the axiom schema $\mathsf{IQ}_3 \equiv \forall x\ [\ x \leq \overline{n} \leftrightarrow \bigvee_{k \leq n} x = \overline{k}\ ]$, which is a theorem of R.

Let

$$K = \left\{ \begin{pmatrix} x & y \\ z & w \end{pmatrix} :\ \begin{pmatrix} x & y \\ z & w \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\ \wedge\ xw = 1 + yz \right\}.$$

Let

$$A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}.$$

Let $A \preceq B$ if and only if $A, B \in K$ and there exists a largest element $m(B) \in \{b_1, b_2, b_3, b_4\}$ with respect to $\leq$ such that

(1) $A = B$ or
(2) there exists $C \in K$ such that $a_i, c_i \leq m(B)$ for all $1 \leq i \leq 4$ and $AC = B$.

Let $\mathsf{SL}_2(\mathbb{N})^+$ denote $\mathsf{SL}_2(\mathbb{N})$ minus the identity matrix. Assume B is the translation of a variable-free $\mathcal{L}_{\mathsf{BT}}$-term. Then, $B \in \mathsf{SL}_2(\mathbb{N})^+$. The bound in (2) tells that $A, C \in \mathsf{SL}_2(\mathbb{N})^+$. It is straightforward to verify that if $A, B, C \in \mathsf{SL}_2(\mathbb{N})^+$ are such that $AC = B$, then a bound such as the one in (2) holds. It is then clear that (1)–(2) capture what it means for a finite string to be a prefix of another string. Thus, R proves the translation of each instance of WD_3. $\square$

5.3 Interpretation of $\overline{\mathsf{ID}}$ in $\mathsf{IQ}^{(2)}$

Let $\mathsf{IQ}^{(2)}$ be IQ extended with axioms (I)–(VIII) in Fig. 6. We can reason in $\mathsf{IQ}^{(2)}$ about natural numbers in the standard way and will therefore occasionally not refer explicitly to the axioms of $\mathsf{IQ}^{(2)}$ we use. In this section, we show that $\overline{\mathsf{ID}}$ is interpretable in $\mathsf{IQ}^{(2)}$.

We start by making a few simple observations:

- Axiom (IV) tells us that addition is commutative. Hence, by Q_4, 0 is an additive identity. That is, $\mathsf{IQ}^{(2)} \vdash \forall x\ [\ 0 + x = x\ \wedge\ x + 0 = x\ ]$.
- Recall that $1 = \mathrm{S}0$. By Q_7 and Q_6

$$x1 = x0 + x = 0 + x = x.$$

  Since axiom (V) tells us that multiplication is commutative, 1 is a multiplicative identity. That is, $\mathsf{IQ}^{(2)} \vdash \forall x\ [\ 1x = x\ \wedge\ x1 = x\ ]$.
- Axiom (VI) tells us that addition is right-cancellative. Since addition is commutative, it is also left-cancellative. That is

$$\mathsf{IQ}^{(2)} \vdash \forall xyz\ [\ z + x = z + y \rightarrow x = y\ ].$$

- By Q_6 and (V), $\mathsf{IQ}^{(2)} \vdash \forall x\ [\ x0 = 0\ \wedge\ 0x = 0\ ]$.

Lemma 18 *Let τ be the 4-dimensional translation of $\{0, 1, \circ\}$ in $\{0, \mathrm{S}, +, \times\}$ defined as follows*

- *0 and 1 are translated as $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, respectively*
- *$\circ$ is translated as matrix multiplication*
- *the domain J is the class of all 2×2 matrices $\begin{pmatrix} x & y \\ z & w \end{pmatrix}$ where $x \neq 0$.*

Then, τ extends to a translation of $\{0, 1, \circ, \preceq\}$ in $\{0, \mathrm{S}, +, \times, \leq\}$ that defines a 4-dimensional interpretation of $\overline{\mathsf{ID}}$ in $\mathsf{IQ}^{(2)}$.

Proof We verify that J satisfies the domain condition. It is clear that $0^\tau, 1^\tau \in J$. It remains to verify that J is closed under matrix multiplication. Let

$$A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}, \quad B = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}, \quad AB = \begin{pmatrix} a_1b_1 + a_2b_3 & a_1b_2 + a_2b_4 \\ a_3b_1 + a_4b_3 & a_3b_2 + a_4b_4 \end{pmatrix}$$

where $a_1, b_1 \neq 0$. We need to show that $a_1b_1 + a_2b_3 \neq 0$. Axiom (VIII) tells us that models of $\mathsf{IQ}^{(2)}$ do not have zero divisors. Hence, $a_1b_1 \neq 0$. Axiom (VII) tells us that 0 is the only element with an additive inverse. Hence, $a_1b_1 + a_2b_3 \neq 0$, which implies $AB \in J$. Thus, J is closed under matrix multiplication.

It is straightforward to verify that (I)–(V) suffice to prove that matrix multiplication is associative. Thus, $\mathsf{IQ}^{(2)}$ proves the translation of ID_1.

Next, we show that the translation of ID_2 and $\overline{\mathsf{ID}}_5$ are theorems of $\mathsf{IQ}^{(2)}$. We need to show that

(1) $\forall A, B \in J\ [\ (\ A0^\tau = B0^\tau\ \vee\ 0^\tau A = 0^\tau B\ ) \rightarrow A = B\ ]$
(2) $\forall A, B \in J\ [\ (\ A1^\tau = B1^\tau\ \vee\ 1^\tau A = 1^\tau B\ ) \rightarrow A = B\ ]$.

We verify (1). First, we show that $\forall A, B \in J\ [\ A0^\tau = B0^\tau \rightarrow A = B\ ]$. Assume $x, a \neq 0$ and

$$\begin{pmatrix} x + y & y \\ z + w & w \end{pmatrix} = \begin{pmatrix} x & y \\ z & w \end{pmatrix} 0^\tau = \begin{pmatrix} a & b \\ c & d \end{pmatrix} 0^\tau = \begin{pmatrix} a + b & b \\ c + d & d \end{pmatrix}.$$

We need to show that $x = a$ and $z = c$. We have

$$x + b = x + y = a + b \ \wedge \ z + d = z + w = c + d.$$

Since addition is right-cancellative, $x = a$ and $z = c$. Thus, for all $A, B \in J$, if $A0^\tau = B0^\tau$, then $A = B$.

We show that $\forall A, B \in J\ [\ 0^\tau A = 0^\tau B \to A = B\ ]$. Assume $x, a \neq 0$ and

$$\begin{pmatrix} x & y \\ x+z & y+w \end{pmatrix} = 0^\tau \begin{pmatrix} x & y \\ z & w \end{pmatrix} = 0^\tau \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ a+c & b+d \end{pmatrix}.$$

We need to show that $z = c$ and $w = d$. We have

$$a + z = x + z = a + c \ \wedge \ b + w = y + w = b + d.$$

Since addition is left-cancellative, $z = c$ and $w = d$. Thus, for all $A, B \in J$, if $0^\tau A = 0^\tau B$, then $A = B$. Hence, (1) holds. By similar reasoning, (2) holds. Thus, $\mathsf{IQ}^{(2)}$ proves the translation of ID_2 and $\overline{\mathsf{ID}}_5$.

We show that the translation of ID_3 is a theorem of $\mathsf{IQ}^{(2)}$. We need to show that $\forall A, B \in J\ [\ A0^\tau \neq B1^\tau\ ]$. Assume for the sake of a contradiction $x, a \neq 0$ and

$$\begin{pmatrix} x+y & y \\ z+w & w \end{pmatrix} = \begin{pmatrix} x & y \\ z & w \end{pmatrix} 0^\tau = \begin{pmatrix} a & b \\ c & d \end{pmatrix} 1^\tau = \begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix}.$$

Then

$$a = x + y = x + a + b$$

where we have omitted parentheses since addition is associative. Since 0 is an additive identity and addition is commutative, $0 + a = x + b + a$. Since addition is right-cancellative, $0 = x + b$. Since 0 is the only element with an addititive inverse, $x = 0$, which contradicts the assumption that $x \neq 0$. Thus, $\mathsf{IQ}^{(2)}$ proves the translation of ID_3.

We show that the translation of $\overline{\mathsf{ID}}_6$ is a theorem of $\mathsf{IQ}^{(2)}$. We need to show that $\forall A, B \in J\ [\ 0^\tau A \neq 1^\tau B\ ]$. Assume for the sake of a contradiction $x, a \neq 0$ and

$$\begin{pmatrix} x & y \\ x+z & y+w \end{pmatrix} = 0^\tau \begin{pmatrix} x & y \\ z & w \end{pmatrix} = 1^\tau \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix}.$$

Then, $x = a + c = a + x + z$. Hence, $0 = a + z$. Since 0 is the only element with an addititive inverse, $a = 0$, which contradicts the assumption that $a \neq 0$. Thus, $\mathsf{IQ}^{(2)}$ proves the translation of $\overline{\mathsf{ID}}_6$.

Finally, we translate $\preceq$ as in the proof of Lemma 17. □

6 Interpretation of TC in Q

In this section, we show that our interpretation of $\overline{\mathsf{ID}}$ in IQ extends in a natural way to an interpretation of TC in Q. Instead of interpreting TC, we interpret the variant $\mathsf{TC}^{\varepsilon}$ where we extend the language of TC with a constant symbol ε for the identity element. See Fig. 7 for the axioms of $\mathsf{TC}^{\varepsilon}$. We choose to work with $\mathsf{TC}^{\varepsilon}$ because the identity matrix is naturally present in our interpretation of $\overline{\mathsf{ID}}$ in IQ and because we get a more compact form of the editor axiom (TC_2 and $\mathsf{TC}_3^{\varepsilon}$). The interpretation we give can be turned into an interpretation of TC by simply removing the identity matrix from the domain (see Appendix A of Visser [13] for mutual interpretability of TC and $\mathsf{TC}^{\varepsilon}$).

Recall that $x \leq_{\mathsf{I}} y \equiv \exists r \, [\, r + x = y \,]$. Let $x <_{\mathsf{I}} y \equiv \exists r \, [\, r \neq 0 \;\wedge\; r + x = y \,]$. Let $\mathsf{Q}^{(2)}$ be Q extended with axioms (I)–(VI) in Fig. 6 and the trichotomy law

$$\forall xy \, [\, x <_{\mathsf{I}} y \;\vee\; x = y \;\vee\; y <_{\mathsf{I}} x \,].$$

We make a few simple observations:

- Axiom (VII) $\forall xy \, [\, x + y = 0 \rightarrow (\, x = 0 \;\wedge\; y = 0 \,)\,]$ is a theorem of $\mathsf{Q}^{(2)}$. Indeed, assume $x + y = 0$. If $y = 0$, then $x = 0$ by Q_4. Thus, it suffices to show that $y = 0$. Assume for the sake of a contradiction that $y \neq 0$. Then, by Q_3, there exists v such that $y = \mathrm{S}v$. By Q_5

$$0 = x + y = x + \mathrm{S}v = \mathrm{S}(x + v)$$

  which contradicts Q_2. Thus, $x + y = 0$ implies $x = y = 0$.
- Axiom (VIII) $\forall xy \, [\, xy = 0 \rightarrow (\, x = 0 \;\vee\; y = 0 \,)\,]$ is a theorem of $\mathsf{Q}^{(2)}$. Indeed, assume $xy = 0$ and $y \neq 0$. By Q_3, there exists v such that $y = \mathrm{S}v$. By Q_7

$$0 = xy = xv + x$$

  which implies $x = 0$. Thus, $xy = 0$ implies $x = 0 \;\vee\; y = 0$.
- $\mathsf{Q}^{(2)}$ proves that 1 is the only element with a multiplicative inverse. Indeed, assume $xy = 1$. By commutativity of multiplication, Q_2 and Q_5, we have $x, y \neq 0$.

The Axioms of $\mathsf{TC}^{\varepsilon}$

$\mathsf{TC}_1^{\varepsilon}$ $\forall x \, [\, \varepsilon x = x \;\wedge\; x\varepsilon = x \,]$
$\mathsf{TC}_2^{\varepsilon}$ $\forall xyz \, [\, x(yz) = (xy)z \,]$
$\mathsf{TC}_3^{\varepsilon}$ $\forall xyzw \, [\; xy = zw \rightarrow \exists u \, [\, (\, z = xu \wedge uw = y \,) \vee (\, x = zu \wedge uy = w \,)\,]\,]$
$\mathsf{TC}_4^{\varepsilon}$ $0 \neq \varepsilon$
$\mathsf{TC}_5^{\varepsilon}$ $\forall xy \, [\, xy = 0 \rightarrow (\, x = \varepsilon \;\vee\; y = \varepsilon \,)\,]$
$\mathsf{TC}_6^{\varepsilon}$ $1 \neq \varepsilon$
$\mathsf{TC}_7^{\varepsilon}$ $\forall xy \, [\, xy = 1 \rightarrow (\, x = \varepsilon \;\vee\; y = \varepsilon \,)\,]$
$\mathsf{TC}_8^{\varepsilon}$ $0 \neq 1$

Fig. 7 Non-logical axioms of the first-order theory $\mathsf{TC}^{\varepsilon}$

Hence, by Q_3, there exist u, v such that $x = \mathsf{S}u$ and $y = \mathsf{S}v$. By commutativity of multiplication, Q_7 and Q_5

$$1 = xy = xv + x = \mathsf{S}(xv + u) \ \wedge\ 1 = yx = yu + y = \mathsf{S}(yu + v).$$

By Q_1

$$0 = xv + u \ \wedge\ 0 = yu + v$$

which implies $u = v = 0$. Hence, $x = y = 1$. Thus, $xy = 1$ implies $x = y = 1$.

This section as structured as follows: In Sect. 6.1, we show that that if we modify our interpretation of $\overline{\mathsf{ID}}$ in $\mathsf{IQ}^{(2)}$ by choosing as the domain the class K of all 2×2 matrices with determinant 1, we obtain an interpretation in $\mathsf{Q}^{(2)}$ of the theory we obtain from $\mathsf{TC}^{\varepsilon}$ by replacing the editor axiom $\mathsf{TC}_2^{\varepsilon}$ with the axioms D_2, D_3, $\overline{\mathsf{ID}}_5$, $\overline{\mathsf{ID}}_6$, $\forall x\ [\ x = \varepsilon\ \vee\ \exists y\ [\ x = y0\ \vee\ x = y1\ ]$. In Sect. 6.2, we extend our interpretation of $\overline{\mathsf{ID}}$ in $\mathsf{IQ}^{(2)}$ to an interpretation of $\mathsf{TC}^{\varepsilon}$ in $\mathsf{Q}^{(2)}$ by restricting K to a subclass on which the editor axiom holds. Finally, in Sect. 8, we show that we can interpret $\mathsf{Q}^{(2)}$ in Q by restricting the universe of Q to a suitable subclass.

6.1 Atoms and predecessors

Let K denote the class all 2×2 matrices with determinant 1. That is

$$K = \left\{ \begin{pmatrix} x & y \\ z & w \end{pmatrix} \ :\ xw = 1 + yz \right\}.$$

It is not difficult to verify that $\mathsf{Q}^{(2)}$ proves that $\det(AB) = 1$ if $\det(A) = \det(B) = 1$. We thus have the following lemma.

Lemma 19 $\mathsf{Q}^{(2)}$ *proves that* K *is closed under* $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ *and matrix multiplication.*

Let us say that $A \in K$ is an atom in K if for all $B, C \in K$, $A = BC$ implies that one of B and C is the identity matrix. The proof of the following lemma is straightforward.

Lemma 20 $\mathsf{Q}^{(2)}$ *proves that* $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ *and* $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ *are atoms in* K.

In [10], we introduce a theory BTQ and show that D interprets Q by showing that it interprets BTQ. We obtain BTQ from ID by replacing ID_4 with the axiom $\forall x\ [\ x = 0\ \vee\ x = 1\ \vee\ \exists y\ [\ x = y0\ \vee\ x = y1\ ]$. The next lemma shows that if we modify the translation in Lemma 18 by choosing as the domain the class of all elements in K distinct from the identity matrix, we obtain an interpretation of BTQ in $\mathsf{Q}^{(2)}$.

Lemma 21 *Let* $A \in K$. *Then,* $\mathsf{Q}^{(2)}$ *proves that* A *is the identity matrix or that there exist* $B, C \in K$ *such that* $A = BC$ *and* C *is one of* $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Proof Let $K \ni A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. By the trichotomy law, we have the following cases

- (1a) $a = b \ \wedge \ c <_{\mathsf{l}} d$, (1b) $a = b \ \wedge \ c = d$, (1c) $a = b \ \wedge \ d <_{\mathsf{l}} c$
- (2a) $a <_{\mathsf{l}} b \ \wedge \ c = d$, (2b) $b <_{\mathsf{l}} a \ \wedge \ c = d$
- (3a) $b <_{\mathsf{l}} a \ \wedge \ c <_{\mathsf{l}} d$, (3b) $a <_{\mathsf{l}} b \ \wedge \ d <_{\mathsf{l}} c$, (3c) $b <_{\mathsf{l}} a \ \wedge \ d <_{\mathsf{l}} c$, (3d) $a <_{\mathsf{l}} b \ \wedge \ c <_{\mathsf{l}} d$.

We consider Case (1a). Since $a = b \ \wedge \ c <_{\mathsf{l}} d$, let $d = r + c$ where $r \neq 0$. Since $ad = 1 + bc$ as $A \in K$, we have

$$ar + ac = a(r + c) = ad = 1 + bc = 1 + ac$$

Since addition is right-cancellative, $ar = 1$, which implies $a = r = 1$. Thus

$$A = \begin{pmatrix} 1 & 1 \\ c & 1 + c \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

We consider Case (1b). Since $a = b \ \wedge \ c = d$ and $A \in K$, we have

$$ad = 1 + bc = 1 + ad.$$

Since 0 is an additive identity and addition is right-cancellative, $0 = 1$ which contradicts Q_2.

We consider Case (1c). Since $a = b \ \wedge \ d <_{\mathsf{l}} c$, let $c = s + d$ where $s \neq 0$. We have

$$ad = 1 + bc = 1 + a(s + d) = 1 + as + ad.$$

Hence, $0 = 1 + as$. Since addition is commutative, $0 = \mathrm{S}(as + 0)$ by Q_5, which contradicts Q_2.

We consider Case (2a). Since $a <_{\mathsf{l}} b \ \wedge \ c = d$, let $b = r + a$ where $r \neq 0$. We have

$$ad = 1 + bc = 1 + (r + a)d = 1 + rd + ad.$$

Hence, $0 = 1 + rd$ which contradicts Q_2.

We consider Case (2b). Since $b <_{\mathsf{l}} a \ \wedge \ c = d$, let $a = s + b$ where $s \neq 0$. We have

$$sd + bd = (s + b)d = ad = 1 + bc = 1 + bd.$$

Hence, $sd = 1$ which implies $s = d = 1$. Thus

$$A = \begin{pmatrix} 1 + b & b \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

We consider Case (3a). Since $b <_{\mathsf{I}} a \ \wedge\ c <_{\mathsf{I}} d$, there exist $r, s \neq 0$ such that $a = r + b$ and $d = s + c$. Since $ad = 1 + bc$, we have

$$rs + rc + bs + bc = (r + b)(s + c) = ad = 1 + bc$$

which implies

$$rs + rc + bs = 1.$$

Since $r, s \neq 0$, we conclude that $r = s = 1$ and $b = c = 0$. Thus, $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

We consider Case (3b). Since $a <_{\mathsf{I}} b \ \wedge\ d <_{\mathsf{I}} c$, there exist $p, q \neq 0$ such that $b = p + a$ and $c = q + d$. Since $ad = 1 + bc$, we have

$$ad = 1 + bc = 1 + (p + a)(q + d) = 1 + pq + pd + aq + ad.$$

Hence, $0 = 1 + pq + pd + aq$ which contradicts Q_2.

We consider Case (3c). Since $b <_{\mathsf{I}} a \ \wedge\ d <_{\mathsf{I}} c$,

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = E \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \quad \text{where } E = \begin{pmatrix} a - b & b \\ c - d & d \end{pmatrix}.$$

Since addition is right-cancellative in $\mathsf{Q}^{(2)}$, we write $a - b$ and $c - d$ for the unique elements r, s such that $a = r + b$ and $c = s + d$. We need to show that $E \in K$. That is, we need to show that $\det(E) = 1$. First, observe that

$$(x - y)z = xy - yz \ \text{ and } \ (1 + xz) - yz = 1 + (xz - yz)$$

since

$$(x - y)z + yz = \big((x - y) + y\big)z = xz \ \text{ and } \ 1 + (xz - yz) + yz = 1 + xz.$$

Since $\det(A) = 1$, we have

$$(a - b)d = ad - bd = (1 + bc) - bd = 1 + b(c - d).$$

Thus, $E \in K$.

We consider Case (3d). Since $a <_{\mathsf{I}} b \ \wedge\ c <_{\mathsf{I}} d$

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = G \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{where } G = \begin{pmatrix} a & b - a \\ c & d - c \end{pmatrix}$$

We need to show that $G \in K$. That is, we need to show that $\det(G) = 1$. Since $\det(A) = 1$, we have

$$a(d-c) = ad - ac = 1 + bc - ac = 1 + (b-a)c.$$

Thus, $G \in K$. $\square$

By similar reasoning, $\mathsf{Q}^{(2)}$ proves that left predecessors also exist: if $A \in K$ is not the identity, then there exist $B, C \in K$ such that $A = CB$ and C is one of $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Since modified subtraction makes sense in $\mathsf{Q}^{(2)}$, we also get that the cancellation laws hold: if $A, B, C \in K$ and $AC = BC \vee CA = CB$, then $A = B$. In particular, in any model of $\mathsf{Q}^{(2)}$, K defines a model of the theory F of Szmielew and Tarski (see Tarski et al. [12, p. 86]). The theory F is given by the following non-logical axioms: concatenation is associative, every element is both left cancellative and right cancellative, the two maps $x \mapsto x0$ and $y \mapsto y1$ have disjoint images, every element different from 0 and 1 is in the image of one of the two maps $x \mapsto x0$ and $y \mapsto y1$. The intended model is the free semigroup with two generators.

6.2 Interpretation of $\mathsf{TC}^{\varepsilon}$

We are finally ready to extend our interpretation of $\overline{\mathsf{ID}}$ in $\mathsf{IQ}^{(2)}$ to an interpretation of $\mathsf{TC}^{\varepsilon}$ in $\mathsf{Q}^{(2)}$. All we need to do is to restrict the class K to a subclass on which the editor axiom holds.

Theorem 22 *There exists a class I such that the 4-dimensional translation of $\{\varepsilon, 0, 1, \circ\}$ in $\{0, 1, S, +, \times\}$ defined by*

- *ε, 0 and 1 are translated as $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, respectively*
- *$\circ$ is translated as matrix multiplication*
- *the domain is I*

defines a 4-dimensional interpretation of $\mathsf{TC}^{\varepsilon}$ in $\mathsf{Q}^{(2)}$.

Proof Let

$$K = \left\{ \begin{pmatrix} x & y \\ z & w \end{pmatrix} : \ xw = 1 + yz \right\}.$$

Lemmas 18 and 20 tell us that the restriction of axioms $\mathsf{TC}_1^{\varepsilon} - \mathsf{TC}_2^{\varepsilon}, \mathsf{TC}_4^{\varepsilon} - \mathsf{TC}_8^{\varepsilon}$ to K are theorems of $\mathsf{Q}^{(2)}$. Since $\mathsf{TC}_1^{\varepsilon} - \mathsf{TC}_2^{\varepsilon}, \mathsf{TC}_4^{\varepsilon} - \mathsf{TC}_8^{\varepsilon}$ are universal sentences, to interpret $\mathsf{TC}^{\varepsilon}$ in $\mathsf{Q}^{(2)}$, it suffices to restrict the class K to a subclass I on which the editor axiom $\mathsf{TC}_2^{\varepsilon}$ holds. We need the following three properties that are given by Lemmas 18 and 21

$$\mathsf{DJ}\ \forall A, B \in K \left[\ A\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix} \neq B\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\ \right]$$

$$\mathsf{RC}\ \forall A, B \in K \Bigg[A \neq B \rightarrow \left(A\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix} \neq B\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix} \ \wedge\ A\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} \neq B\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\right) \Bigg]$$

$$\mathsf{PD}\ \forall A \in K \left[\ A = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \vee \exists B \in K \left[\ A = B\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix} \ \vee\ A = B\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\ \right]\right]$$

Let

$$H = \Big\{ W \in K :\ \forall XZ\ \forall Y \in K\big[\ XY = ZW \rightarrow \exists U \in K\ [\ (\ Z = XU\ \wedge\ UW = Y) \vee (\ X = ZU\ \wedge\ UY = W)\ ]\big] \Big\}.$$

It follows from DJ, RC, PD and associativity of matrix multiplication that $\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$, $\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}$, $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$ are elements of H. We show that H is closed under matrix multiplication. So, assume $W_0, W_1 \in H$. We need to show that $W_0W_1 \in H$. First, we observe that $W_0W_1 \in K$ since K is closed under matrix multiplication and $H \subseteq K$. Now, let X, Y, Z be such that $XY = ZW_0W_1$ and $Y \in K$. Since $W_1 \in H$, we have the following two cases for some $U_1 \in K$

$$(1)\ X = ZW_0U_1\ \wedge\ U_1Y = W_1, \quad (2)\ ZW_0 = XU_1\ \wedge\ U_1W_1 = Y.$$

We consider (1). Since K is closed under matrix multiplication and $H \subseteq K$, we have

$$X = ZW_0U_1\ \wedge\ W_0U_1Y = W_0W_1\ \wedge\ W_0U_1 \in K\ . \qquad (*)$$

We consider (2). Since $W_0 \in H$ and $U_1 \in K$, we have one of the following two cases for some $U_0 \in K$

$$\begin{aligned} &(2a)\ \ Z = XU_0\ \wedge\ U_0W_0 = U_1\ \wedge\ U_1W_1 = Y,\\ &(2b)\ \ X = ZU_0\ \wedge\ U_0U_1 = W_0\ \wedge\ U_1W_1 = Y. \end{aligned}$$

In case of (2a), we have

$$Z = XU_0\ \wedge\ U_0W_0W_1 = U_1W_1 = Y\ \wedge\ U_0 \in K\ . \qquad (**)$$

In case of (2b), we have

$$X = ZU_0 \ \wedge \ W_0W_1 = U_0U_1W_1 = U_0Y \ \wedge \ U_0 \in K. \qquad (***)$$

By (*), (**) and (***), we have $W_0W_1 \in H$. Thus, H is closed under matrix multiplication.

We are finally ready to specify the class I. Let

$$I = \{A \in H : \forall B \, [\, B \preceq_K A \rightarrow B \in H \,]\,\}$$

where

$$B \preceq_K A \equiv \exists C \in K \, [\, A = BC \,].$$

It follows from Lemma 20 that $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ are elements of I. To show that I defines a model of $\mathsf{TC}^{\varepsilon}$, it suffices to show that I is closed under matrix multiplication and downward closed under $\preceq_K$, where the latter ensures that the editor axiom holds restricted to I.

We show that I is closed under matrix multiplication. Assume $A_0, A_1 \in I$. We need to show that $A_0A_1 \in I$. So, assume $BC = A_0A_1$ where $C \in K$. We need to show that $B \in H$. Since $A_1 \in I \subseteq H$ and $C \in K$, we have one of the following cases for some $U \in K$

$$\text{(i)} \ \ A_0 = BU \ \wedge \ UA_1 = C \ , \quad \text{(ii)} \ \ B = A_0U \ \wedge \ UC = A_1.$$

In case of (i) we have $B \preceq_K A_0$ which implies $B \in H$ since $A_0 \in I$. In case of (ii) we have $U \preceq_K A_1$ which implies $U \in H$ since $A_1 \in I$. Since H is closed under matrix multiplication and $A_0 \in I \subseteq H$, we have $B = A_0U \in H$. Hence, $A_0A_1 \in I$. Thus, I is closed under matrix multiplication.

We show that I is downward closed under $\preceq_K$. So, assume $B \preceq_K A$ where $A \in I$. We need to show that $B \in I$. That is, we need to show that $B \in H$ and $\forall D \preceq_K B \, [\, D \in H \,]$. Since $A \in I$ and $B \preceq_K A$, it follows from the definition of I that $B \in H$. Assume now $B = DC$ where $C \in K$. We need to show that $D \in H$. Since $B \preceq_K A$, there exists $E \in K$ such that $A = BE$. Hence, $DCE = BE = A$. Since $C, E \in K$ and K is closed under matrix multiplication, $CE \in K$. Hence, $D \preceq_K A$. Then, $D \in H$ since $A \in I$. Thus, I is downward closed under $\preceq_K$. $\square$

7 Commutative semirings I

We complete our proof of interpretability of $\overline{\mathsf{ID}}$ in IQ by showing that IQ and $\mathsf{IQ}^{(2)}$ are mutually interpretable.

Theorem 23 IQ *and* $\mathsf{IQ}^{(2)}$ *are mutually interpretable.*

Proof Since $\mathsf{IQ}^{(2)}$ is an extension of IQ, we only need to show that $\mathsf{IQ}^{(2)}$ is interpretable in IQ. Our strategy is to first restrict the universe of IQ to an inductive class N_2 which is such that each of the axioms (I)–(VIII) in Fig. 6 holds on N_2 when we restrict quantification to N_2 and treat addition and multiplication as partial functions. Recall that a class X is inductive if $0 \in X$ and $\forall x \in X\ [\ \mathrm{S}x \in X\ ]$. Now, since the axioms of $\mathsf{IQ}^{(2)}$ are all universal sentences, to interpret $\mathsf{IQ}^{(2)}$ in IQ, it suffices to relativize quantification to a subclass N of N_2 that is closed under $0, \mathrm{S}, +, \times$.

We start by restricting the universe of IQ to a subclass N_0 where 0 is the only element with an additive inverse, and addition is associative and right-cancellative. Let $u \in N_0$ if and only if

(1) $0 + u = u$
(2) $\forall x\ [\ x + u = 0 \rightarrow (\ x = 0\ \wedge\ u = 0)\ ]$
(3) $\forall x\ [\ \mathrm{S}x + u = \mathrm{S}(x + u)\ ]$
(4) $\forall xy\ [\ (x + y) + u = x + (y + u)\ ]$
(5) $\forall xy\ [\ x + u = y + u \rightarrow x = y\ ]$
(6) $0u = 0$.

We verify that $0 \in N_0$. We need to show that 0 satisfies (1)–(6). By $\mathsf{Q}_4 \equiv \forall x\ [\ x + 0 = x\ ]$, 0 satisfies (1)–(5). By $\mathsf{Q}_6 \equiv \forall x\ [\ x0 = 0\ ]$, 0 satisfies (6). Thus, $0 \in N_0$.

We verify that N_0 is closed under S. Let $u \in N_0$. We need to show that $\mathrm{S}u \in N_0$. That is, we need to show that $\mathrm{S}u$ satisfies (1)–(6). We have

$$0 + \mathrm{S}u = \mathrm{S}(0 + u) = \mathrm{S}u = \mathrm{S}u + 0$$

where the first equality holds by $\mathsf{Q}_5 \equiv \forall xy\ [\ x + \mathrm{S}y = \mathrm{S}(x + y)\ ]$, the second equality holds since u satisfies (1) and the last equality holds by Q_4. Thus, $\mathrm{S}u$ satisfies (1).

By Q_5 and $\mathsf{Q}_2 \equiv \forall x\ [\ \mathrm{S}x \neq 0\ ]$

$$x + \mathrm{S}u = \mathrm{S}(x + u) \neq 0.$$

Thus, $\mathrm{S}u$ satisfies (2).

We have

$$\mathrm{S}x + \mathrm{S}u = \mathrm{S}(\mathrm{S}x + u) = \mathrm{SS}(x + u) = \mathrm{S}(x + \mathrm{S}u)$$

where the first equality holds by Q_5, the second equality holds since u satisfies (3) and the last equality holds by Q_5. Thus, $\mathrm{S}u$ satisfies (3).

We have

$$(x + y) + \mathrm{S}u = \mathrm{S}((x + y) + u) = \mathrm{S}(x + (y + u)) = x + (y + \mathrm{S}u)$$

where the first equality holds by Q_5, the second equality holds since u satisfies (4), and the last equality holds by Q_5. Thus, $\mathrm{S}u$ satisfies (4).

We have

$$\mathrm{S}(x + u) = x + \mathrm{S}u = y + \mathrm{S}u = \mathrm{S}(y + u)\ \Rightarrow\ x + u = y + u\ \Rightarrow\ x + y$$

where the first implication follows from $\mathsf{Q}_1 \equiv \forall xy\ [\ \mathrm{S}x = \mathrm{S}y \rightarrow x = y\ ]$, and the last implication follows from the assumption that u satisfies (5). Thus, $\mathrm{S}u$ satisfies (5).

By $\mathsf{Q}_7 \equiv \forall xy\ [\ x \times \mathrm{S}y = x \times y + x\ ]$

$$0 \times \mathrm{S}u = 0u + 0 = 0 + 0 = 0$$

where the second equality follows from the assumption that u satisfies (6) and the last equality holds by Q_4. Thus, $\mathrm{S}u$ satisfies (6).

Since Su satisfies (1)–(6), $\mathrm{S}u \in N_0$. Thus, N_0 is closed under S. Since N_0 contains 0 and is closed under S, the class N_0 is inductive.

We restrict N_0 to a subclass N_1 where addition is commutative, the left distributive law holds, and there are no zero divisors. Let $u \in N_1$ if and only if $u \in N_0$ and

(7) $\forall x \in N_0\ [\ x + u = u + x\ ]$
(8) $\forall x \in N_0\ \forall y\ [\ x(y + u) = xy + xu\ ]$
(9) $\forall x \in N_0\ [\ xu = 0 \rightarrow (\ x = 0\ \vee\ u = 0)\ ]$
(10) $\forall x \in N_0\ [\ \mathrm{S}x \times u = xu + u\ ]$.

Verify that N_1 contains 0. We need to show that $0 \in N_0$ and that 0 satisfies (7)–(10). Since N_0 is inductive, $0 \in N_0$. By Q_4 and (1), 0 satisfies (7). By Q_4 and Q_6, 0 satisfies (8). It is obvious that 0 satisfies (9). By Q_6 and Q_4, 0 satisfies (10). Since 0 is an element of N_0 and satisfies (7)–(10), $0 \in N_1$.

We verify that N_1 is closed under S. Let $u \in N_1$. We need to show that $\mathrm{S}u \in N_0$ and that $\mathrm{S}u$ satisfies (7)–(10). Since N_0 is inductive and $u \in N_1 \subseteq N_0$, $\mathrm{S}u \in N_0$. We verify that $\mathrm{S}u$ satisfies (7). Let $x \in N_0$. Then

$$x + \mathrm{S}u = \mathrm{S}(x + u) = \mathrm{S}(u + x) = \mathrm{S}u + x$$

where the first equality holds by Q_5, the second equality holds since u satisfies (7), and the last equality holds since x satisfies (3). Thus, $\mathrm{S}u$ satisfies (7).

We verify that $\mathrm{S}u$ satisfies (8). Let $x \in N_0$. We have

$$\begin{aligned} x(y + \mathrm{S}u) &= x \times \mathrm{S}(y + u) \quad (\mathsf{Q}_5) \\ &= x(y + u) + x \quad (\mathsf{Q}_7) \\ &= (xy + xu) + x \quad (u \text{ satisfies } (8)) \\ &= xy + (xu + x) \quad (x \text{ satisfies } (4)) \\ &= xy + (x \times \mathrm{S}u) \quad (\mathsf{Q}_7). \end{aligned}$$

Thus, $\mathrm{S}u$ satisfies (8).

We verify that $\mathrm{S}u$ satisfies (9). Let $x \in N_0$ and assume $x \times \mathrm{S}u = 0$. By Q_7, $xu + x = 0$. Since x satisfies (2), $x = 0$. Thus, $\mathrm{S}u$ satisfies (9).

Finally, we verify that Su satisfies (10). Let $x \in N_0$. We have

$$
\begin{aligned}
\mathrm{S}x \times \mathrm{S}u &= (\mathrm{S}x \times u) + \mathrm{S}x && (\mathsf{Q}_7)\\
&= (xu + u) + \mathrm{S}x && (u \text{ satisfies } (10))\\
&= xu + (u + \mathrm{S}x) && (\mathrm{S}x \in N_0 \text{ satisfies } (4))\\
&= xu + \mathrm{S}(u + x) && (\mathsf{Q}_5)\\
&= xu + \mathrm{S}(x + u) && (x \in N_0 \text{ and } u \text{ satisfies } (7))\\
&= xu + (x + \mathrm{S}u) && (\mathsf{Q}_5)\\
&= (xu + x) + \mathrm{S}u && (\mathrm{S}u \in N_0 \text{ satisfies } (4))\\
&= (x \times \mathrm{S}u) + \mathrm{S}u && (\mathsf{Q}_7).
\end{aligned}
$$

Thus, Su satisfies (10).

Since Su is an element of N_0 and satisfies (7)–(10), S$u \in N_1$. Thus, N_1 is closed under S. Since N_1 contains 0 and is closed under S, the class N_1 is inductive.

We restrict N_1 to a subclass N_2 where multiplication is associative and commutative. Let $u \in N_2$ if and only if $u \in N_1$ and

(11) $\forall x, y \in N_1$ [$(xy)u = x(yu)$]
(12) $\forall x \in N_1$ [$xu = ux$] .

We verify that $0 \in N_2$. We need to show that $0 \in N_1$ and that 0 satisfies (11)–(12). Since N_1 is inductive, $0 \in N_1$. By Q_6, 0 satisfies (11). By Q_6 and (6), 0 satisfies (12). Thus, $0 \in N_2$.

We verify that N_2 is closed under S. Let $u \in N_2$. We need to show that S$u \in N_1$ and that Su satisfies (11)–(12). Since $N_2 \subseteq N_1$ and N_1 is inductive, S$u \in N_1$. We verify that Su satisfies (11). Let $x, y \in N_1$. We have

$$
\begin{aligned}
(xy) \times \mathrm{S}u &= (xy)u + xy && (\mathsf{Q}_7)\\
&= x(yu) + xy && (u \text{ satisfies } (11))\\
&= x(yu + y) && (x \in N_0 \text{ and } y \in N_1 \text{ satisfies } (8))\\
&= x(y \times \mathrm{S}u) && (\mathsf{Q}_7).
\end{aligned}
$$

Thus, Su satisfies (11).

We verify that Su satisfies (12). Let $x \in N_1$. We have

$$
\begin{aligned}
x \times \mathrm{S}u &= xu + x && (\mathsf{Q}_7)\\
&= ux + x && (u \text{ satisfies } (12)\ )\\
&= \mathrm{S}u \times x && (u \in N_0 \text{ and } x \in N_1 \text{ satisfies } (10)).
\end{aligned}
$$

Thus, Su satisfies (12).

Since Su is an element of N_1 and satisfies (11)–(12), S$u \in N_2$. Thus, N_2 is closed under S. Since N_2 contains 0 and is closed under S, the class N_2 is inductive.

We are almost done. All that remains is to restrict N_2 to an inductive class that is closed under addition and multiplication. We start by ensuring closure under addition.

Let

$$N_3 = \{u \in N_2 :\ \forall x \in N_2\ [\ x + u \in N_2\ ]\ \}.$$

By Q_4, $0 \in N_3$. We show that that N_3 is closed under S. Let $u \in N_3$. Since N_2 is inductive and $u \in N_3 \subseteq N_2$, $\mathrm{S}u \in N_2$. By Q_5, given $x \in N_2$, we have $x + \mathrm{S}u = \mathrm{S}(x + u)$. Since $u \in N_3$, $x + u \in N_2$. Since N_2 is inductive, $\mathrm{S}(x + u) \in N_2$. Hence, $\mathrm{S}u \in N_3$. Thus, N_3 is closed under S.

We verify that N_3 is closed under $+$. Let $u, v \in N_3$. We need to show that $u+v \in N_2$ and $\forall x \in N_2[\ x + (u + v) \in N_2\ ]$. Since $u \in N_2$ and $v \in N_3$, $u + v \in N_2$. Now, let $x \in N_2$. Since $u \in N_3$, $x + u \in N_2$. Since $v \in N_3$, $(x + u) + v \in N_2$. Since $v \in N_2 \subseteq N_0$ satisfies (4), $(x + u) + v = x + (u + v)$. Hence, $u + v \in N_3$ Thus, N_3 is closed under $+$.

Let

$$N = \{u \in N_3 :\ \forall x \in N_3\ [\ xu \in N_3\ ]\ \}.$$

We show that N is an inductive class that is closed under $+$ and $\times$. We show that $0 \in N$. Since N_3 is inductive, $0 \in N_3$. Let $x \in N_3$. By Q_6, $x0 = 0 \in N_3$. Thus, $0 \in N$.

We show that N is closed under S. Let $u \in N$. We need to show that $\mathrm{S}u \in N$. Since $u \in N_3$ and N_3 is inductive, $\mathrm{S}u \in N_3$. Let $x \in N_3$. By Q_7, $x \times \mathrm{S}u = xu + x$. Since $u \in N$, $xu \in N$. Since N_3 is closed under addition, $xu + x \in N_3$. Hence, $\mathrm{S}u \in N$. Thus, N is closed under S.

We show that N is closed under $+$. Let $u, v \in N \subseteq N_3$. Since N_3 is closed under addition, $u + v \in N_3$. Let $x \in N_3$. Since $u, v \in N$, $xu, xv \in N_3$. Since N_3 is closed under addition, $xu + xv \in N_3$. Since $x \in N_3 \subseteq N_0$ and $v \in N_3 \subseteq N_1$, $xu + xv = x(u + v)$. Hence, $u + v \in N$. Thus, N is closed under $+$.

We show that N is closed under $\times$. Let $u, v \in N \subseteq N_3$. Since $u \in N_3$ and $v \in N$, $uv \in N_3$. Let $x \in N_3$. Since $u \in N$, $xu \in N_3$. Since $v \in N$, $(xu)v \in N_3$. Since $x, u \in N_3 \subseteq N_1$ and $v \in N_3 \subseteq N_2$ satisfies (11), $(xu)v = x(uv)$. Hence, $uv \in N$. Thus, N is closed under $\times$.

Since N satisfies the domain conditions and all the axioms of $\mathsf{IQ}^{(2)}$ hold restricted to N as they are universal sentences, $\mathsf{IQ}^{(2)}$ is interpretable in IQ. Since $\mathsf{IQ}^{(2)}$ is an extension of IQ, it follows that IQ and $\mathsf{IQ}^{(2)}$ are mutually interpretable. □

8 Commutative semirings II

It is clear that $\mathsf{Q}^{(2)}$ is interpretable in Q since each axiom of $\mathsf{Q}^{(2)}$ is provable in $I\Delta_0$, which is Q extended with an induction schema for Σ_0-formulas, and $I\Delta_0$ is interpretable in Q (see Section V.5c of Hájek and Pudlák [4]). Lemma V.5.11 of [4] shows that we can interpret any finite subtheory of $I\Delta_0$ in Q by restricting the universe of Q to a suitable subclass. It then follows that our interpretation of $\mathsf{TC}^{\varepsilon}$ in $\mathsf{Q}^{(2)}$ really extends to a recursion-free interpretation of $\mathsf{TC}^{\varepsilon}$ in Q. For the benefit of the reader, we show that we can also prove this by building on the proof of Theorem 23.

Given a sentence ϕ and a class M, let ϕ^M denote the sentence we obtain by restricting quantification to M.

Theorem 24 *There exists a class M such that $\mathsf{Q} \vdash \phi^M$ for each axiom ϕ of $\mathsf{Q}^{(2)}$.*

Proof Let N be the class in the proof of Theorem 23. Let

$$u \leq_N v \equiv \exists r \in N\ [\ u + r = v\ ].$$

We restrict N to an inductive subclass M_0 that is downward closed under $\leq_N$. Let

$$M_0 = \big\{ u \in N :\ \forall v \leq_N u\ [\ v \in N\ ]\ \wedge\ \forall x, y \leq_N u\ [\ x \leq_N y\ \vee\ y \leq_N x\ ]\big\}.$$

We show that $0 \in M_0$. Assume $v + r = 0$. If $r = 0$, then $v = 0$ by Q_4. If $r \neq 0$, then by Q_3 there exists t such $r = \mathrm{S}t$. Then, by Q_5, $0 = v + r = \mathrm{S}(v + t)$ which contradicts Q_2. Thus, since $0 \in N$ and $0 + 0 = 0$, we have $0 \in M_0$.

We show that M_0 is closed under S. Let $u \in M_0$. We need to show that $\mathrm{S}u \in M_0$. Since $u \in M_0 \subseteq N$ and N is inductive, $\mathrm{S}u \in N$. We show that $\forall v \leq_N \mathrm{S}u\ [\ v \in N\ ]$. Assume $r \in N$ and $v + r = \mathrm{S}u$. We need to show that $v \in N$. If $v = 0$, then $v \in N$ since N is an inductive class. Otherwise, by Q_3, there exists w such that $\mathrm{S}w = v$. By Clause (3) in the proof of Theorem 23

$$\mathrm{S}u = v + r = \mathrm{S}w + r = \mathrm{S}(w + r).$$

By Q_1, $w + r = u$. Hence, $w \leq_N u$. Since $u \in M_0$, we have $w \in N$. Since N is an inductive class, $v = \mathrm{S}w \in N$. Thus, $\forall v \leq_N \mathrm{S}u\ [\ v \in N\ ]$.

We show that $\forall x, y \leq_N \mathrm{S}u\ [\ x \leq_N y\ \vee\ y \leq_N x\ ]$. Assume $x, y \leq_N \mathrm{S}u$. By what we have just shown, $x, y \in N$. If $x = \mathrm{S}u$ or $y = \mathrm{S}u$, then x and y are comparable with respect to $\leq_N$ since $x, y \leq_N \mathrm{S}u$. Otherwise, by Q_4

$$\mathrm{S}u = x + r\ \ \wedge\ \ \mathrm{S}u = y + t \quad \text{where } r, t \in N \setminus \{0\}.$$

Since $x, y, r, t \in N$, we have

$$\mathrm{S}u = x + r = r + x\ \ \wedge\ \ \mathrm{S}u = y + t = t + y$$

by Clause (7) in the proof of Theorem 23. By Q_3, there exist r_0, t_0 such that $r = \mathrm{S}r_0$ and $t = \mathrm{S}t_0$. Hence

$$\mathrm{S}u = \mathrm{S}r_0 + x = \mathrm{S}(r_0 + x)\ \ \wedge\ \ \mathrm{S}u = \mathrm{S}t_0 + y = \mathrm{S}(t_0 + y)$$

by Clause (3) in the proof of Theorem 23. By Q_1, $u = r_0 + x$ and $u = t_0 + y$. Hence, $r_0, t_0 \leq_N u$ which implies $r_0, t_0 \in N$ since $u \in M_0$. Then

$$u = r_0 + x = x + r_0\ \ \wedge\ \ u = t_0 + y = y + t_0$$

by Clause (7) in the proof of Theorem 23. Hence, $x, y \leq_N u$ which implies that x and y are comparable with respect to $\leq_N$ since $u \in M_0$. Thus, we have $\forall x, y \leq_N \mathrm{S}u\ [\ x \leq_N y \ \vee\ y \leq_N x\ ]$. It then follows that $\mathrm{S}u \in M_0$.

Since $\leq_N$ is transitive, M_0 is downward closed under $\leq_N$. Indeed, assume $w \leq_N v$ and $v \leq_N u$. Then, there exist $r, t \in N$ such that $v = w + r$ and $u = v + t$. Hence, $u = (w + r) + t$. Since $t \in N \subseteq N_0$, we have

$$u = (w + r) + t = w + (r + t)$$

by Clause (4) in the proof of Theorem 23. Since $r, t \in N$ and N is closed under addition, $r + t \in N$. Hence, $w \leq_N u$. Thus, $\leq_N$ is transitive.

We restrict M_0 to a subclass M_1 that is closed under addition. Let

$$M_1 = \left\{u \in M_0 :\ \forall x \in M_0\ [\ x + u \in M_0\ ]\right\}.$$

The class M_1 is shown to be closed under 0, S and $+$ just as in the proof of Theorem 23. We show that M_1 is downward closed under $\leq_N$. Assume $u \in M_1$ and $u = v + r$ where $r \in N$. We need to show that $v \in M_1$. So, let $x \in M_0$. We need to show that $x + v \in M_0$. We have

$$M_0 \ni x + u = x + (v + r) = (x + v) + r$$

by Clause (4) in the proof of Theorem 23. Then

$$x + v \leq_N x + u \in M_0.$$

Since M_0 is downward closed under $\leq_N$, we have $x + v \in M_0$. Hence, $v \in M_1$. Thus, M_1 is downward closed under $\leq_N$.

Finally, we restrict M_1 to a domain M. Let

$$M = \left\{u \in M_1 :\ \forall x \in M_1\ [\ xu \in M_1\ ]\right\}.$$

The class M is shown to be closed under 0, S, $+$, $\times$ just as in the proof of Theorem 23. We show that M_1 is downward closed under $\leq_N$. Assume $u \in M$ and $u = v + r$ where $r \in N$. We need to show that $v \in M$. So, let $x \in M_1$. We need to show that $xv \in M_1$. We have

$$M_1 \ni xu = x(v + r) = xv + xr$$

by Clause (8) in the proof of Theorem 23. Since $v \leq_N u$, $u \in M \subseteq M_1$ and M_1 is downward closed under $\leq_N$, we have $v \in M_1$. Then, by Clause (7) in the proof of Theorem 23

$$u = v + r = r + v.$$

Hence, $r \leq_N u$ which implies $r \in M_1$. Since $x, r \in M_1$ and M_1 is closed under $\times$, we have $xr \in M_1 \subseteq N$. Then, $xu = xv + xr$ implies $xv \leq_N xu$. Since $xu \in M_1$ and M_1 is downward closed under $\leq_N$, we have $xv \in M_1$. Hence, $v \in M$. Thus, M is downward closed under $\leq_N$.

Axioms (I)–(VIII) in Fig. 6 and the axioms of Q that are universal sentences hold on M when we restrict quantification to M since they hold on N when we restrict quantification to N. We show that $\mathsf{Q}_3 \equiv \forall x \left[\, x = 0 \ \vee \ \exists y \, [\, x = \mathrm{S}y \,] \,\right]$ holds on M. Assume $x \in M \backslash \{0\}$. By Q_3, there exists y such that $x = \mathrm{S}y$. We need to show that $y \in M$. By Q_4 and Q_5, we have

$$x = \mathrm{S}y = \mathrm{S}y + 0 = \mathrm{S}(y + 0) = y + \mathrm{S}0.$$

Since M is an inductive class, $\mathrm{S}0 \in M \subseteq N$. Hence, $y \leq_N x$. Since M is downward closed under $\leq_N$, we have $y \in M$. Thus, Q_3 holds restricted to M.

Finally, we show the trichotomy law $\forall xy \, [\, x <_{\mathsf{l}} y \ \vee \ x = y \ \vee \ y <_{\mathsf{l}} x \,]$ holds restricted to M. Recall that $x <_{\mathsf{l}} y \equiv \exists r \, [\, r \neq 0 \wedge r + x = y \,]$. Let $x, y \in M$. Since M is closed under addition and addition on M is commutative

$$y + x = x + y \in M.$$

Then, $x, y \leq_N x + y$. Since $M \subseteq M_0$, we have

$$x \leq_N y \ \vee \ y \leq_N x.$$

Assume $y = x + r$ where $r \in N$. By Clause (7) in the proof of Theorem 23, $y = x + r = r + x$. Hence, $r \leq_N y$ which implies $r \in M$. Similarly, if $x = y + t$ where $t \in N$, then $t \in M$. Hence, since $x \leq_N y \ \vee \ y \leq_N x$ holds

$$\exists r, t \in M \, [\, y = x + r \ \vee \ x = y + t \,].$$

Thus, the trichotomy law holds restricted to M. □

Funding Open access funding provided by University of Oslo (incl Oslo University Hospital).

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

1. Davis, M.: Hilbert's tenth problem is unsolvable. Am. Math. Mon. **80**(3), 233–269 (1973)
2. Ganea, M.: Arithmetic on semigroups. J. Symb. Log. **74**, 265–278 (2009)

3. Grzegorczyk, A.: Undecidability without arithmetization. Stud. Log. **79**, 163–230 (2005)
4. Hájek, P., Pudlák, P.: Metamathematics of First-Order Arithmetic. Cambridge University Press, Cambridge (2017)
5. Hodges, W.: Model Theory. Cambridge University Press, Cambridge (1993)
6. Kristiansen, L., Murwanashyaka, J.: First-order concatenation theory with bounded quantifiers. Arch. Math. Log. **60**, 77–104 (2021)
7. Lothaire, M.: Algebraic Combinatorics on Words. Cambridge University Press, Cambridge (2002)
8. Makanin, G.S.: The problem of solvability of equations in a free semigroup. Math. USSR Sb. **32**(2), 129–198 (1977)
9. Markov, A.: Theory of algorithms. In: Proceedings of the Steklov Institute of Mathematics, vol. 42, Moscow (1954)
10. Murwanashyaka, J.: Weak essentially undecidable theories of concatenation. Arch. Math. Log. **61**, 939–976 (2022)
11. Tarski, A.: A Decision Method for Elementary Algebra and Geometry. RAND Corporation, Santa Monica (1948)
12. Tarski, A., Mostowski, A., Robinson, R.M.: Undecidable Theories. North-Holland, Amsterdam (1953)
13. Visser, A.: Growing commas. A study of sequentiality and concatenation. Notre Dame J Form. Log. **50**, 61–85 (2009)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.