CONCATENATION AS A BASIS FOR Q AND THE INTUITIONISTIC VARIANT OF NELSON'S CLASSIC RESULT

MSc Thesis (*Afstudeerscriptie*)

written by

Rachel Sterken
(born March 20, 1981 in London, Ontario, Canada)

under the supervision of **Albert Visser and Benedikt Löwe**, and submitted to the Board of Examiners in partial fulfillment of the requirements for the degree of

Master of Logic

at the *Universiteit van Amsterdam*.

Date of the public defense:	**Members of the Thesis Committee:**
October 17th, 2008	Albert Visser, Benedikt Löwe, Dick de Jongh, Peter van Emde Boas.

CONTENTS

Abstract

In [18], Visser shows that a first-order theory is sequential (has 'global coding') iff (roughly) it directly interprets a weak set theory, AS. The programme behind Visser's result is to find coordinate free ways of thinking about notions of coding. In this thesis, we add some results to Visser's programme for the case of 'local coding'.

Since Robinson's arithmetic, Q, is mutually interpretable (but not directly) with AS (see [14], [4], [8], [18]) and Q is in a sense the minimal arithmetical theory that yields enough coding to prove Gödel's Second Incompleteness Theorem, we propose whether a theory interprets Q as a characterization of the notion of 'local coding'.

We also investigate other candidates in place of Q. We show that a basic theory of strings, TC_{Q} interprets Q.

We, in addition, verify that the classical result of Nelson [10] works in the constructive case by showing that $i\mathsf{Q}$ interprets $iI\Delta_0 + \Omega_1$. This result entails that our characterization of 'local coding' also works in the constructive case.

1. Introduction

This Master's thesis is concerned with research at the junction of many distinct, yet connected, ideas and programmes in *meta*mathematics. Five of which are particularly important.

Weak theories. The first is the study of weak theories. The notion of weak theory is somewhat informal in the literature and in parlance amongst metamathematicians. It is not fully clear which theories are 'weak'. Nonetheless, the notion is robust and amenable to precise and independently motivated definition: Historically, the most significant of such theories is *Robinson's arithmetic*, Q. The theory Q is formulated in the language of arithmetic, $\{\overline{0}, \mathsf{S}, +, \cdot\}$, whose axiomatization consists of seven axioms: Three axioms stating that the successor symbol represents an injective function with a range containing all numbers except 0, and four other axioms about $+$ and $\cdot$, two stating how $+$ and $\cdot$ interact with $\overline{0}$ and two stating how the sum $x + \mathsf{S}y$ and product $x \cdot \mathsf{S}y$ intuitively interact with and are uniquely determined by the sum $x + y$ and the product $x \cdot y$. *Peano arithmetic*, PA, is an extension of Q formulated in the same language by adding the induction schema to the axioms of Q. Many treatments enrich Q by adding $\leq$ to the language and an additional axiom that defines it; by convention, this definitional extension retains the name Robinson's arithmetic and is denoted by Q. The presence of $\leq$ makes the definition possible of a *bounded formula* and fragments of PA, like $I\Delta_0$, where induction is restricted to bounded formulas. Aside from its historical significance, Q has many important metamathematical properties: First, Q is finitely axiomatizable. Second, Q is *essentially undecidable* — that is, each consistent extension of Q is undecidable. Third, Q is mathematically very weak — it does not even prove the commutativity and associativity of $+$. Lastly, despite its weakness, it is, strikingly, capable of *interpreting* many much stronger theories like $I\Delta_0$ and certain extensions thereof, like $I\Delta_0 + \Omega_1$. Visser, in [19], defines weak theories as those *mutually interpretable* with Q (or alternatively, those mutually locally interpretable with Q) and provides the following useful survey of such theories:

a. Arithmetical theories like Q, $I\Delta_0$, Buss's theory S^1_2 and $I\Delta_0 + \Omega_1$.

b. Various theories of concatenation like Szmielew and Tarski's theory F ([14], p.86) and Grzegorczyk's theory TC ([5]).

c. Theories of sequences, like the one introduced by Pavel Pudlák in [11].

d. Various weak set theories like adjunctive set theory AS, a set theory introduced by Pudlák in [11] (see also: [9]). Pudlák's theory is modulo some inessential details, the same as a weak set theory introduced and studied by Tarski and Szmielew, minus extensionality. See [14] and [15].

Much of the focus in Visser's related work has been on theories in (c.) and (d.). In this Master's thesis, we will be focusing on theories like those in (a.) and (b.).

Interpretability. The notion of interpretability, developed extensively into refined concepts in the work of (most notably) Pudlák, Friedman and Visser, is central to the definition of weak theories and also their propitiousness as tools in metamathematics. Different concepts of interpretability provide metamathematicians different means of comparing theories (e.g., as a measure of relative mathematical strength) and formulating sufficient conditions in metamathematical theorems. More precisely, we define a basic notion of interpretability as follows: We first need the notions of a translation between formulas and a translation between symbols.[1] A *translation of formulas*,

[1] We use the definition of interpretation found in Svejdar [13].

F, from a theory U to formulas of a theory V is determined by a definitional extension V' of V, a translation of symbols and a domain. A *translation of symbols*, τ, is a function that maps each symbol in the language of U to a symbol of the same arity and kind in the language of the definitional extension V'. A *domain* is a formula $\delta(x)$ of V' with one free variable used to relativize quantifiers in the given translation of formulas: It translates $(\forall x\phi)^\tau$ as $\forall x(\delta(x) \to \phi^\tau)$ and $(\exists x\phi)^\tau$ as $\exists x(\delta(x) \wedge \phi^\tau)$. It is important to note that logical connectives are preserved under the translation F. Finally, we call a translation of formulas an *interpretation of* U *in* V if its domain $\delta(x)$ satisfies:

$$\mathsf{V}' \vdash \exists x\, \delta(x) \text{ and,}$$

$$\mathsf{V}' \vdash \forall x_1,...,x_n((\delta(x_1) \wedge ... \wedge \delta(x_n)) \to \exists y(\delta(y) \wedge \forall z(f^\tau(x_1,...,x_n,z) \leftrightarrow z =^\tau y))$$

for each function symbol f in the language of U — i.e., the domain is provably non-empty and closed under the interpreted functions. Moreover, V' must prove the translation of every axiom ϕ of U — that is:

$$\mathsf{V}' \vdash \phi^\tau \text{ for each axiom } \phi \text{ of } \mathsf{U}.$$

A theory U is interpretable in V if there exists an interpretation of U in V. We call an interpretation *unrelativized* if the domain formula is $\delta(x) :\leftrightarrow (x = x)$. Moreover, an interpretation has *absolute identity* if identity in U is mapped to identity in V. Finally, we call an interpretation *direct* if it is unrelativized and has absolute identity.

Incompleteness without arithmetization. The third item this Master's thesis is concerned with is a programme, taken up by Grzegorczyk [5] and seminal in the work of Szmielew and Tarski [14] and Quine [12], is to base the explanation of the phenomena of incompleteness and undecidability on axiomatic theories different from Q and PA. In particular, Grzegorczyk uses a weak theory of concatenation TC. Indeed, a theory of concatenation might be considered a more natural setting to place the explanation of such phenomena, especially given the special role off coding in the proofs of such metamathematical results. In [17], Visser highlights the supervenience of structured objects on strings, and how other theoretically important objects, e.g., sets, emerge out of our reasoning about strings and concatenation.

Nelson's programme. The fourth is Nelson's programme. Nelson in [10] uses Q as a basis for his philosophy of mathematics and predicative arithmetic. Buss in [3] characterizes, we think accurately, Nelson's philosophy of mathematics as a combination of *formalism* and *radical constructivism*. Nelson is a formalist in the sense that he doubts the existence of platonic mathematical objects, in particular the existence of the set of all integers; further, he is a radical constructivist since the method he innovated to build up his predicative arithmetic from Q is rather constructive: Nelson objects to the fact that on the one hand, the set of integers is defined as the set of numbers for which induction is valid, and on the other hand, the formulas for which induction must hold involve quantification over the set of all integers. Instead, Nelson's predicative arithmetic avoids the platonic assumption about the existence of an infinite set of integers that satisfy induction. It does so by starting with a pre theoretic notion of an infinite set of integers which satisfy the axioms of Q, what Buss [3] and Burgess [1] call the set of *proto-integers*. The set of proto-integers is then refined into more refined notions of integer by taking subsets of the proto-integers that satisfy more and more properties of the integers, starting with basic properties such as the commutativity and associativity of $+$ and eventually working up to induction for bounded formulas. This technique is known as Solovay's method of *shortening cuts* (also known as *inductive cuts*). Using these techniques to their limit, Nelson showed that Q interprets $I\Delta_0+\Omega_1$.

Aside from being philosophically interesting, this result is also metamathematically significant from a methodological point of view since it says that Q interprets the mathematically stronger theory $I\Delta_0+\Omega_1$. This result means that we can use interpretability in Q as a reasonably simple sufficient condition to satisfy in many metamathematical theorems while at the same time we have $I\Delta_0+\Omega_1$ at our disposal in doing the grunt work for establishing such metamathematical theorems. In this sense, Nelson's theorem is what Visser calls a *bridging theorem* in [19].

Visser's programme. Lastly, we outline Visser's programme which interestingly incorporates many of the insights of the ideas and programmes mentioned above (cf. [18] and [19]). Visser's programme is to find *coordinate-free* ways of defining the notions of coding needed in order to yield the associated metamathematical results. By coordinate-free, we mean independent of the choice of signature. In [19] and [18], Visser shows (roughly) that if a theory U *directly interprets* an appropriate weak set theory or sequential theory (cf. (c.) and (d.) above), then:

(i) U has enough coding abilities to prove the incompleteness theorems for any choice of domain for U and,

(ii) U has enough coding abilities to prove its own restricted consistency statements.

We call this coding ability, *global coding*. The theories in (a.) and (b.) do not directly interpret the theory AS that Visser proposes and hence, do not characterize *global coding*. However, the theories in (a.) and (b.) do provide us with another characterization of coding — *local coding*: Roughly, if a theory U interprets Q, then U has enough coding abilities to prove the incompleteness theorems for some choice of domain for U.

In what follows, we will propose a weak theory of strings, TC_{Q} as an analogue of Q, and show that TC_{Q} interprets Q. This result contributes to Grzegorczyk's programme and Visser's programme by providing a simple theory in the language of concatenation that, effectively, yields the same metamathmatical benefits as Q. That is, as a corollary of the mutual interpretability of TC_{Q} and Q, we can now use TC_{Q} as a base theory to show that any theory interpreting TC_{Q} has certain welcome coding capabilities — i.e., has local coding.

In addition, we verify that the classical result of Nelson [10] works in the constructive case by showing that $i\mathsf{Q}$ interprets $iI\Delta_0+\Omega_1$. This result entails that our characterization of local coding also works in the constructive case.

This Master's thesis is structured as follows: In section 2, we present a constructive proof of Nelson's classic result that Q interprets $I\Delta_0+\Omega_1$. In section 3, we show that the weak theory of concatenation TC_{Q} interprets Q.

The techniques used in this Master's thesis, as far as the author is aware, are due primarily to the following: Tarski, Mostowski and Robinson [15], unpublished work of Solovay, Nelson [10], Hájek and Pudlák [7], and Visser [19].

Acknowledgements: I would like to especially thank my supervisor Albert Visser for his generous help, hospitality and patience without which this thesis would not have been written. I would

also like to thank the *ILLC* and the great people there that make it all happen — especially, of course, Benedikt Löwe and Tanja Kassenaar. Finally, it would be impossible to withhold thanks to Marcello Di Bello for his continuous support and companionship during my time in Amsterdam.

2. CONSIDERING CONSTRUCTIVITY: $i\mathsf{Q}$ INTERPRETS $iI\Delta_0 + \Omega_1$

In this section, we begin by presenting a slightly altered version of Q needed in order for the constructive proof of Nelson's result to go through. In the first subsection, we attempt to independently motivate this alteration by considerations about the decidability of identity and equality with $\overline{0}$ in the intuitionistic case. Next, in the second subsection, we present what is essentially Nelson's original proof that Q interprets $I\Delta_0$, however in, we hope, a more intuitive format (along similar lines as [7] with a few crucial corrections — cf. Lemma 6). Recall the method of shortening cuts mentioned in association with Nelson in the introduction, it will be used extensively throughout. Finally, at the end of the section, we outline the coding of the function ω_1 and claim that the proofs found in Nelson [10] and Hájek and Pudlák [7] go through constructively. This yields the result of the final subsection: $i\mathsf{Q}$ interprets $I\Delta_0 + \Omega_1$.

2.1. A BETTER VERSION OF Q

The theory Q, well-known as *Robinson's arithmetic*, is a theory in the language of arithmetic with the following axioms:

q1. $\mathsf{S}x = \mathsf{S}y \to x = y$

q2. $\mathsf{S}x \neq \overline{0}$

q3. $x \neq \overline{0} \to \exists y(x = \mathsf{S}y)$

q4. $x + \overline{0} = x$

q5. $x + \mathsf{S}y = \mathsf{S}(x+y)$

q6. $x \cdot \overline{0} = \overline{0}$

q7. $x \cdot \mathsf{S}y = x \cdot y + x$

Moreover, we define:

q8. $x \leq y :\leftrightarrow \exists u(u + x = y)$

Let $I(x)$ be a formula. We treat $\{x : I(x)\}$ as a virtual class and write I for $\{x : I(x)\}$. In this way, we can use a simple virtual class notation (e.g., $\in, \subseteq$) to aid in presentation. We assume the reader is aware of the simple relationship between the two notations (e.g., $x \in I$ is virtual class notation for $I(x)$, $J \cap I$ for $(J(x) \wedge I(x))$). (Note that we will use a mixture of the two notations according to their intuitive roles in use.)

I is an *initial segment* if I is closed under $\overline{0}, \mathsf{S}$ and downwards closed under $\leq$.

$i\mathsf{Q}$ is the usual axiomatization of Q with the intuitionistic predicate calculus as the underlying logic. Let IDENTITY:$= \{x : \forall y(x = y \vee x \neq y)\}$ and ZERO:$= \{x : x = \overline{0} \vee x \neq \overline{0}\}$. That is, let IDENTITY be the property that identity for x is decidable and ZERO be the property that identity for $\overline{0}$ is decidable. We conjecture that ZERO(x) and hence, IDENTITY(x) are not provably instantiated on any initial segment of $i\mathsf{Q}$, but that they are provable under a slightly different axiomatization of $i\mathsf{Q}$. We term this new axiomatization, the *constructive* or *disjunctive version of Q*, and write $i\mathsf{Q}_\mathsf{d}$. More precisely, $i\mathsf{Q}_\mathsf{d}$ will be taken to be Q plus the following classically equivalent, but intuitionistically stronger formula replacing (q3):

q3*. $x = \overline{0} \vee \exists y(x = \mathsf{S}y)$.

Conjecture 1. $\textsc{Zero}(x)$ *and* $\textsc{Identity}(x)$ *are not provably instantiated in* $i\mathsf{Q}$ *on any initial segment.*

Proof. We leave the crucial part of the proof — namely, that $\textsc{Zero}(x)$ is not provably instantiated in $i\mathsf{Q}$ as an open question. That $\textsc{Identity}(x)$ is not provably instantiated in $i\mathsf{Q}$ is a corollary of the former conjecture: Suppose $i\mathsf{Q} \vdash I(x) \to \textsc{Identity}(x)$. We have that $i\mathsf{Q} \vdash \textsc{Identity}(x) \to \textsc{Zero}(x)$ by universal instantiation. Moreover, by intuitionistic logic, we have that:

$$i\mathsf{Q} \vdash (I(x) \to \textsc{Identity}(x)) \to ((\textsc{Identity}(x) \to \textsc{Zero}(x)) \to (I(x) \to \textsc{Zero}(x)).$$

But this is a contradiction since by implication elimination we have that $i\mathsf{Q} \vdash I(x) \to \textsc{Zero}(x)$ and if $\textsc{Zero}(x)$ is not provably instantiated in $i\mathsf{Q}$, we have that $i\mathsf{Q} \nvdash I(x) \to \textsc{Zero}(x)$ and hence, $i\mathsf{Q} \nvdash I(x) \to \textsc{Identity}(x)$ too.

□

Proposition 1. $\textsc{Zero}(x)$ *is provable in* $i\mathsf{Q}_\mathsf{d}$.

Proof. Reason in $i\mathsf{Q}_\mathsf{d}$. By (q3*), $x = \overline{0} \vee \exists y(x = \mathsf{S}y)$. If $x = \overline{0}$, then $x = \overline{0} \vee x \neq \overline{0}$. If $x = \mathsf{S}y$ for some y, then by (q1) we have that $x \neq \overline{0}$. Whence, $x = \overline{0} \vee x \neq \overline{0}$. Thus, $i\mathsf{Q}_\mathsf{d} \vdash x = \overline{0} \vee x \neq \overline{0}$. This means precisely that $\textsc{Zero}$ is decidable in $i\mathsf{Q}_\mathsf{d}$.

□

Proposition 2. $\textsc{Identity}(x)$ *is provably instantiated in* $i\mathsf{Q}_\mathsf{d}$ *on an initial segment.*

Proof. We postpone the proof until Section 3.2, Corollary 9.

□

Henceforth, we will refer to $i\mathsf{Q}_\mathsf{d}$ by simply $i\mathsf{Q}$. Next, we go on to the main result of section 3.

2.2. $i\mathsf{Q}$ INTERPRETS $iI\Delta_0$

The schema for bounded induction under the signature of Q is as follows:

$$(\phi(\overline{0}) \wedge \forall y \leq x(\phi(y) \to \phi(\mathsf{S}y))) \to \phi(x)$$

where ϕ is a bounded formula of the language of arithmetic.

Define $I\Delta_0$ to be Q together with the schema of bounded induction. $iI\Delta_0$ is the usual axiomatization of $I\Delta_0$ where the underlying logic is the intuitionistic predicate calculus.

First, we present the proof of a lemma needed in the proof of Theorem 15 at the end of this section. We follow Burgess [1] in calling this lemma the *absoluteness principle* and follow Nelson [10] in giving its proof by induction on the complexity of ϕ.

Lemma 3 (Nelson [10])**.** *Suppose* U *is a theory with the binary predicate symbol* $\leq$ *and* I *is provably downwards closed under* $\leq$ *and provably closed under the functions of* U*. Let* $\phi(\vec{z})$ *be a bounded formula of* U*. Then* U *proves:*

$$\vec{z} : I \rightarrow (\phi(\vec{z}) \leftrightarrow \phi(\vec{z})^I).$$

Proof. Call a U-formula ϕ *absolute* if U proves:

$$\vec{z} : I \rightarrow (\phi(\vec{z}) \leftrightarrow \phi(\vec{z})^I).$$

Atomic formulas are absolute since if ϕ is atomic, then ϕ^I is just ϕ so that $I \rightarrow (\phi \leftrightarrow \phi^I)$ is a tautology.

Next, suppose ϕ is absolute, then since ϕ and $\neg\phi$ have the same free variables and relativizations, we have that $\neg\phi$ is absolute.

Suppose ϕ_1 and ϕ_2 are absolute. We have that the free variables of $\phi_1 \vee \phi_2$ are precisely those of ϕ_1 and ϕ_2. Moreover, $(\phi_1 \vee \phi_2)^I$ is just $\phi_1^I \vee \phi_2^I$. Thus, $\phi_1 \vee \phi_2$ is absolute.

Suppose ϕ_1 and ϕ_2 are absolute. We have that the free variables of $\phi_1 \wedge \phi_2$ are precisely those of ϕ_1 and ϕ_2. Moreover, $(\phi_1 \wedge \phi_2)^I$ is just $\phi_1^I \wedge \phi_2^I$. Thus, $\phi_1 \wedge \phi_2$ is absolute.

Suppose $\phi(\vec{z})$ is absolute and ψ is $\exists x(x \leq t \wedge \phi)$ where x does not occur free in t. Then the free variables of ψ are those free in t (call these $\vec{y}$) and those free in ϕ. Since I is closed under all the function symbols of U, we have that U proves:

$$\vec{y} : I \wedge \vec{z} : I \rightarrow I[t].$$

Moreover, since I is downwards closed under $\leq$, we have that U proves:

$$\vec{y} : I \wedge \vec{z} : I \rightarrow (\exists x(x \leq t \wedge \phi(\vec{z})) \leftrightarrow \exists x(I(x) \wedge x \leq t \wedge \phi(\vec{z}))).$$

Since ϕ is absolute and $(\vec{y} : I \wedge \vec{z} : I \wedge I(x)) \rightarrow \vec{z} : I$ is a tautology, we have that U proves:

$$\vec{y} : I \wedge \vec{z} : I \rightarrow (\exists x(x \leq t \wedge \phi(\vec{z})) \leftrightarrow \exists x(I(x) \wedge x \leq t \wedge \phi(\vec{z})^I))$$

which is precisely the condition for ψ's absoluteness. Ergo, ψ is absolute.

Suppose $\phi(\vec{z})$ is absolute and ψ is $\forall x(x \leq t \rightarrow \phi)$ where x does not occur free in t. Then the free variables of ψ are those free in t (call these $\vec{y}$) and those free in ϕ. Since I is closed under all the function symbols of U, we have that U proves:

$$\vec{y} : I \wedge \vec{z} : I \rightarrow I[t].$$

Moreover, since I is downwards closed under $\leq$, we have that U proves:

$$\vec{y} : I \wedge \vec{z} : I \rightarrow (\forall x(x \leq t \rightarrow \phi(\vec{z})) \leftrightarrow \forall x(I(x) \wedge x \leq t \rightarrow \phi(\vec{z}))).$$

Since ϕ is absolute and $(\vec{y} : I \wedge \vec{z} : I \wedge I(x)) \rightarrow \vec{z} : I$ is a tautology, we have that U proves:

$$\vec{y} : I \wedge \vec{z} : I \rightarrow (\forall x(x \leq t \rightarrow \phi(\vec{z})) \leftrightarrow \forall x(I(x) \wedge x \leq t \rightarrow \phi(\vec{z})^I))$$

which is precisely the condition for ψ's absoluteness. Ergo, ψ is absolute.

This completes the induction and hence we have established the absoluteness principle for U.

□

Now, we go on to prove the remainder of the lemmas needed for Theorem 15.

A number x is *L-successive*[1] iff $\forall y \forall z(y+z=x \rightarrow \mathsf{S}y+z=\mathsf{S}x)$. We call the class of L-successive numbers $\mathfrak{I}_0$.

Lemma 4 (in $i\mathsf{Q}$**).** *The class* $\mathfrak{I}_0$ *is closed under* $\overline{0}$ *and* S.

Proof. We first show that $x+y=\overline{0} \rightarrow x=y=\overline{0}$ is a theorem of $i\mathsf{Q}$. If $y=\overline{0}$, then $x+\overline{0}=\overline{0} \rightarrow x=y=\overline{0}$ by $(\mathsf{q}4)$. If $y=\mathsf{S}u$ for some u, then $x+\mathsf{S}u=\mathsf{S}(x+u)\neq\overline{0}$ by $(\mathsf{q}5)$ and $(\mathsf{q}1)$. But this is a contradiction, so we have that $y\neq\mathsf{S}u$ which implies by $(\mathsf{q}3^*)$ that $y=\overline{0}$.

Suppose $y+z=\overline{0}$, then $y=z=\overline{0}$ by the theorem just proved in $i\mathsf{Q}$. Moreover, $\mathsf{S}y+z=\mathsf{S}\overline{0}+\overline{0}=\mathsf{S}\overline{0}$. Ergo, $\overline{0}\in\mathfrak{I}_0$.

Suppose $y+z=\mathsf{S}x$ and x is L-successive. We want to show that $\mathsf{S}y+z=\mathsf{S}\mathsf{S}x$. If $z=\overline{0}$, then we find that $y=\mathsf{S}x$ and hence $\mathsf{S}y+\overline{0}=\mathsf{S}y=\mathsf{S}\mathsf{S}x$ by $(\mathsf{q}4)$. If $z=\mathsf{S}u$ for some u, then $y+\mathsf{S}u=\mathsf{S}x$. Ergo, $\mathsf{S}(y+u)=\mathsf{S}x$ by $(\mathsf{q}5)$. This means that $y+u=x$ by $(\mathsf{q}2)$ and so since x is L-successive, we have $\mathsf{S}y+u=\mathsf{S}x$. Finally, by the functionality of S, we have that $\mathsf{S}(\mathsf{S}y+u)=\mathsf{S}\mathsf{S}x$ so that $\mathsf{S}y+\mathsf{S}u=\mathsf{S}\mathsf{S}x$ by $(\mathsf{q}5)$. We conclude that $\mathsf{S}x\in\mathfrak{I}_0$.

□

A number x is an *o-commutator*[2] iff $\forall y \forall z(y+z=x \rightarrow z+y=x)$. A number x is a *strong o-commutator* iff x is L-successive and x is an o-commutator. We call the class of strong o-commutators $\mathfrak{I}_1$.

Lemma 5 (in $i\mathsf{Q}$**).** *The class* $\mathfrak{I}_1$ *is closed under* $\overline{0}$ *and* S.

Proof. We already showed that $\overline{0}$ is L-successive. Hence, suppose $y+z=\overline{0}$, then $y=z=\overline{0}$ by the theorem of $i\mathsf{Q}$ proved above. Ergo, we have that $\overline{0}=\overline{0}+\overline{0}=z+y$ by $(\mathsf{q}4)$ so that $\overline{0}$ is also an o-commutator.

Suppose x is a strong o-commutator. By the argument in Lemma 4, $\mathsf{S}x$ is L-successive. Suppose $y+z=\mathsf{S}x$. If $z=\overline{0}$, then $y=y+\overline{0}=\mathsf{S}x$. Hence, we need to show that $\overline{0}+\mathsf{S}x=\mathsf{S}x$. By $(\mathsf{q}4)$, we have that $x+\overline{0}=x$. Since x is an o-commutator, we find that $\overline{0}+x=x$ and hence that $\overline{0}+\mathsf{S}x=\mathsf{S}x$ by the functionality of S. Now, if $z=\mathsf{S}u$ for some u, then we have that $y+\mathsf{S}u=\mathsf{S}x$. Moreover, we have that $y+u=x$ by $(\mathsf{q}5)$ and $(\mathsf{q}2)$. Since x is an o-commutator, we find that $u+y=x$ and hence since x is also L-successive, $\mathsf{S}u+y=\mathsf{S}x$.

□

Proposition 6 (in $i\mathsf{Q}$, **Visser [16]).** *Suppose the elements of an initial segment I are all o-commutators. Then I verifies* $(\mathsf{q}3^*)$ *and* $(\mathsf{q}8)$.

[1] Note that the ‘L’ is mnemonic for “left”. We will use similar mnemonics throughout to mitigate confusion.

[2] Note that the ‘o’ is mnemonic for “output”.

Proof. Suppose $\mathsf{S}x \in I$. We have that $x+\mathsf{S}\overline{0}=\mathsf{S}x$ by (q4) and (q5). Thus, since x is an o-commutator, we have that $x \leq \mathsf{S}x$. Hence, $x \in I$. This means that any non-zero number in I has a predecessor in I, whence (q3*) holds.

Suppose $x \leq y$ and $y \in I$, then for some z, $z+x=y$. Since y is a o-commutator, we find $x+z=y$, and so $z \leq y$. Thus, $z \in I$. □

A number x is an *o-associator* iff $\forall w \forall y \forall z(w+(y+z)=x \leftrightarrow (w+y)+z=x)$. Let the class of o-associators be $\mathfrak{I}_2$.

Lemma 7 (in *i*Q**).** *The class $\mathfrak{I}_2$ is closed under $\overline{0}$ and* S.

Proof. It is easy to see that $\overline{0}$ is an o-associator by the theorem of *i*Q proved in Lemma 4:

$$\begin{aligned} w+(y+z)=\overline{0} &\leftrightarrow w=y+z=\overline{0} \\ &\leftrightarrow w=y=z=\overline{0} \\ &\leftrightarrow w+y=z=\overline{0} \\ &\leftrightarrow (w+y)+z=\overline{0}. \end{aligned}$$

Suppose x is an o-associator. In case $z=\overline{0}$, we find that $w+(y+\overline{0})=w+y=(w+y)+\overline{0}$ by (q4). So, we have that $w+(y+\overline{0})=\mathsf{S}x \leftrightarrow (w+y)+\overline{0}=\mathsf{S}x$. Now, in case $z=\mathsf{S}u$ for some u, we have by (q5), (q2) and the functionality of S that:

$$\begin{aligned} w+(y+\mathsf{S}u)=\mathsf{S}x &\leftrightarrow \mathsf{S}(w+(y+u))=\mathsf{S}x \\ &\leftrightarrow w+(y+u)=x \\ &\leftrightarrow (w+y)+u=x \\ &\leftrightarrow \mathsf{S}((w+y)+u)=\mathsf{S}x \\ &\leftrightarrow (w+y)+\mathsf{S}u=\mathsf{S}x. \end{aligned}$$

□

Proposition 8 (in *i*Q**).** *Suppose $I \subseteq \mathfrak{I}_2$ and I is closed under $\overline{0}$ and* S. *Let:*

$$J := \{x \in I \mid \forall y \leq x(y \in I)\}.$$

Then J is an initial segment.

Proof. Let I be as specified.

We first show that $x \leq \overline{0} \rightarrow x=\overline{0}$ is a theorem of *i*Q. Suppose $x \leq \overline{0}$, then for some z, $z+x=\overline{0}$. Hence, by the theorem of *i*Q proved in Lemma 4, we have that $x=\overline{0}$.

Now, since I is closed under $\overline{0}$, we have that $\overline{0} \in I$. Moreover, since $\forall y \leq \overline{0}(y \in I)$ is equivalent to $\overline{0} \in I$ by the theorem of *i*Q just proved, we have J is closed under $\overline{0}$.

Suppose $x \in J$ and $y \leq \mathsf{S}x$, then for some u, $u+y=\mathsf{S}x$. In case $y=\overline{0}$, then $y \in I$ since we assume I is closed under $\overline{0}$. In case $y=\mathsf{S}v$ for some v, we have $\mathsf{S}(u+v)=\mathsf{S}x$ by (q5) and hence, $u+v=x$ by (q2). Ergo, $v \leq x$ and hence $v \in I$. Finally, since I is closed under S, we have that $\mathsf{S}v=y \in I$.

We conclude that J is closed under S.

We want to show that $(x \in J \wedge y \leq x) \to y \in J$. Hence, suppose $x \in J$, $y \leq x$ and $z \leq y$, then there are u, v such that $u + y = x$ and $v + z = y$ by (q8). Hence, $u + (v + z) = x$. Since x is an o-associator (since $J \subseteq I \subseteq \mathfrak{I}_2$ and $x \in J$), we have that $(u + v) + z = x$. Ergo, $z \leq x$ and $z \in I$. Thus, since $\forall z \leq y\, z \in I$ holds, we have that J is downwards closed under $\leq$.

□

As promised in Section 3.1, we now show that IDENTITY(x) is provably instantiated on an initial segment.

Corollary 9 (in iQ). *IDENTITY(x) is provably instantiated in $i\mathsf{Q}_\mathsf{d}$ on an initial segment.*

Proof. Let $I := \mathfrak{I}_2 \cap$ IDENTITY and $J := \{x \in I \mid \forall y \leq x (y \in I)\}$.

We first verify that IDENTITY is closed under $\overline{0}$ and S to ensure that $\mathfrak{I}_2 \cap$ IDENTIY is closed under $\overline{0}$ and S: We have that $\overline{0} \in$ IDENTITY by Proposition 1. Suppose IDENTITY(x), then $\forall y (x = y \vee x \neq y)$. Let y be arbitrary. By (q3*), $y = \overline{0} \vee \exists z (y = \mathsf{S}z)$. If $y = \overline{0}$, then $\mathsf{S}x \neq y$ by (q2) and hence, $\forall y (\mathsf{S}x = y \vee \mathsf{S}x \neq y))$. If $y = \mathsf{S}z$, then by assumption we have that $x = z \vee x \neq z$ and hence, $\mathsf{S}x = \mathsf{S}z \vee \mathsf{S}x \neq \mathsf{S}z$ by the functionality and injectivity of S. But $\mathsf{S}z$ is just y and thus, we have shown that $\mathsf{S}x = y \vee \mathsf{S}x \neq y$. This proves that IDENTITY is closed under S.

We have that I is an initial segment by Proposition 8. Moreover, since $J \subseteq I \subseteq$ IDENTITY, we have that $i\mathsf{Q} \vdash J(x) \to$ IDENTITY(x). Thus, IDENTITY(x) is provably instantiated on the initial segment J.

□

Proposition 10 (in iQ). *Suppose $I \subseteq \mathfrak{I}_2$ and I is closed under $\overline{0}$ and S. We define $J := \{x \in I \mid \forall y \in I\ (y + x \in I)\}$. (i) Then J is closed under $\overline{0}, \mathsf{S}$ and $+$. Suppose further that I is downwards closed under $\leq$ and $I \subseteq \mathfrak{I}_1 \cap \mathfrak{I}_2 := \mathfrak{I}_3$. (ii) Then J is downwards closed under $\leq$.*

Proof. Let I be as specified for (i).

Suppose $y \in I$, then $y = y + \overline{0}$ implies that $y + \overline{0} \in I$ so $\overline{0} \in J$. Hence, J is closed under $\overline{0}$.

Suppose $x \in J$ and $y \in I$, then $y + \mathsf{S}x = \mathsf{S}(y + x)$ implies that $\mathsf{S}(y + x) \in I$ since $x \in J$ implies $y + x \in I$. Thus, J is closed under S.

Suppose $x, z \in J$ and $y \in I$, then we have that $y + x \in I$. We want to show that $x + z \in J$. Let $(y + x) + z = u$, then $u \in I$ since $y + x \in I$ and $z \in J$. Ergo, u is an o-associator, and we have that $y + (x + z) = u$. Finally, since $y \in I$ and $u \in I$, we have that $x + z \in J$. Thus, J is closed under $+$.

Now suppose the further conditions on I for (ii).

Suppose $z \leq x \in J$ and $y \in I$. We want to show that $y + z \in J$. We have by the former supposition that $u + z = x$ for some u by (q8). Hence, $y + (u + z) = y + x \in I$ since $x \in J$. Since $y + x$ is an o-associator and o-commutator, we have that:

$$y + (u + z) = (u + z) + y = u + (z + y).$$

Thus, $z+y \leq y+x$ by $(\mathsf{q8})$. Moreover, since $z+y$ is a o-commutator, $y+z \in I$, whence J is downwards closed under $\leq$.

□

We define:

$$\begin{aligned}
\mathfrak{I}_4 &:= \{z \mid \forall x \forall y (x+(y+z) = (x+y)+z)\} \\
\mathfrak{I}_5 &:= \{z \in \mathfrak{I}_4 \mid \forall x \in \mathfrak{I}_4 \forall y \in \mathfrak{I}_4 (x \cdot (y+z) = x \cdot y + x \cdot z)\} \\
\mathfrak{I}_6 &:= \{z \in \mathfrak{I}_5 \mid \forall x \in \mathfrak{I}_5 \forall y \in \mathfrak{I}_5 (x \cdot (y \cdot z) = (x \cdot y) \cdot z)\}.
\end{aligned}$$

We call the elements of the classes $\mathfrak{I}_4, \mathfrak{I}_5$ and $\mathfrak{I}_6$ respectively *a-associators*, *strong L-distributors* and *strong m-associators*.

Lemma 11 (in $i\mathsf{Q}$**).** *The classes $\mathfrak{I}_4$, $\mathfrak{I}_5$ and $\mathfrak{I}_6$ are closed under $\overline{0}$ and S.*

Proof. It is clear that $\mathfrak{I}_4$ is closed under $\overline{0}$. Suppose $z \in \mathfrak{I}_4$. We have by $(\mathsf{q4})$ that:

$$\begin{aligned}
x+(y+\mathsf{S}z) &= x+\mathsf{S}(y+z) \\
&= \mathsf{S}(x+(y+z)) \\
&= \mathsf{S}((x+y)+z) \\
&= (x+y)+\mathsf{S}z.
\end{aligned}$$

It is clear that $\mathfrak{I}_5$ is closed under $\overline{0}$. Suppose $x, y \in \mathfrak{I}_4$ and $z \in \mathfrak{I}_5$. We have by $(\mathsf{q4})$ and $(\mathsf{q7})$ that:

$$\begin{aligned}
x \cdot (y+\mathsf{S}z) &= x \cdot \mathsf{S}(y+z) \\
&= x \cdot (y+z) + x \\
&= (x \cdot y + x \cdot z) + x \\
&= x \cdot y + (x \cdot z + x) \\
&= x \cdot y + x \cdot \mathsf{S}z.
\end{aligned}$$

It is clear that $\mathfrak{I}_6$ is closed under $\overline{0}$. Suppose $x, y \in \mathfrak{I}_5$ and $z \in \mathfrak{I}_6$. By $(\mathsf{q7})$, we have that:

$$\begin{aligned}
x \cdot (y \cdot \mathsf{S}z) &= x \cdot (y \cdot z + y) \\
&= x \cdot (y \cdot z) + x \cdot y \\
&= (x \cdot y) \cdot z + x \cdot y \\
&= (x \cdot y) \cdot \mathsf{S}z.
\end{aligned}$$

□

Proposition 12 (in $i\mathsf{Q}$**).** *Suppose $I \subseteq \mathfrak{I}_6$ and I is closed under $\overline{0}, \mathsf{S}$ and $+$. Let:*

$$J := \{x \in I \mid \forall y \in I \; y \cdot x \in I\}.$$

(i) Then J is closed under $\overline{0}, \mathsf{S}, +$ and $\cdot$. Suppose further that I is downwards closed under $\leq$.
(ii) Then J is downwards closed under $\leq$.

Proof. Let I be as specified for (i).

We have that $\overline{0} \in J$ since $\overline{0} \in I$ and $y \cdot \overline{0} = \overline{0}$.

Suppose $x \in J$ and $y \in I$, then $y \cdot \mathsf{S}x = y \cdot x + y$ by $(\mathrm{q}7)$. Hence, $I(y \cdot \mathsf{S}x)$ since I is closed under $+$. Thus, $\mathsf{S}x \in J$.

Suppose $x, z \in J$ and $y \in I$, then we have that $y \cdot x \in I$ and $y \cdot z \in I$. Moreover, $y \cdot x + y \cdot z \in I$ since I is closed under $+$. Since $z \in J \subseteq I \subseteq \mathfrak{I}_5$, we have that z is a strong L-distributor. Hence, $y \cdot x + y \cdot z = y \cdot (x + z) \in I$. It follows that $x + z \in J$ and so J is closed under $+$.

Suppose $x, z \in J$ and $y \in I$, then we have that $y \cdot x \in I$. This implies that $(y \cdot x) \cdot z \in I$ since $z \in J$. Moreover, since $z \in J \subseteq I \subseteq \mathfrak{I}_6$, we have that $(y \cdot x) \cdot z = y \cdot (x \cdot z) \in I$. Thus, $x \cdot z \in J$ which means precisely that J is closed under $\cdot$.

Further, let I be as specified for (ii).

Suppose $z \leq x$ and $x \in J$. We want to show that $z \in J$. Suppose further that $y \in I$, then $y \cdot x \in I$. Since $z \leq x$, we have that $u + z = x$ for some u. Hence, $y \cdot (u + z) \in I$. Since $z \in J \subseteq I \subseteq \mathfrak{I}_5$, we have that $y \cdot (u + z) = y \cdot u + y \cdot z \in I$. Moreover, $y \cdot u + y \cdot z = y \cdot x$ implies that $y \cdot z \leq y \cdot x$. It follows that $y \cdot z \in I$ since I is closed downwards w.r.t. $\leq$. Finally, since y was an arbitrary element of I, we conclude that $z \in J$.

□

Let $\phi_1(x), \ldots, \phi_n(x)$ be given Δ_0-formulas where x occurs free. For each $j = 1, \ldots, n$, we define:

$$\mathfrak{T}_j := \{x \in \mathfrak{I}_1 \mid (\phi_j(\overline{0}) \wedge \forall y \leq x(\phi_j(y) \rightarrow \phi_j(\mathsf{S}y))) \rightarrow \phi_j(x)\}$$

Moreover, we let $\mathfrak{T} := \bigcap_{j=1}^{n} \mathfrak{T}_j$.

Lemma 13 (in *i*Q**).** *$\mathfrak{T}$ is closed under $\overline{0}$ and* S.

Proof. We first demonstrate that each $\mathfrak{T}_j$ is closed under $\overline{0}$ and S.

Suppose $\phi_j(\overline{0}) \wedge \forall y \leq \overline{0}(\phi_j(y) \rightarrow \phi_j(\mathsf{S}y))$, then each $\mathfrak{T}_j$ is closed under $\overline{0}$ since $\overline{0} \in \mathfrak{I}_1$ and $\phi_j(\overline{0})$ is trivially the case for each j. Hence, $\overline{0} \in \bigcap_{j=1}^{n} \mathfrak{T}_j = \mathfrak{T}$.

To show that each $\mathfrak{T}_j$ is closed under S, we need to prove that if x is an o-commutator, then $y \leq x \rightarrow y \leq \mathsf{S}x$ is a theorem of *i*Q: Suppose x is an o-commutator and $y \leq x$ — that is, $u + y = z$ for some u. By $(\mathrm{q}5)$ and the functionality of S, we find that $u + \mathsf{S}y = \mathsf{S}(u + y) = \mathsf{S}x$. Moreover, since x is an o-commutator , we have that $\mathsf{S}(y + u) = y + \mathsf{S}u = \mathsf{S}x$. Ergo, $y \leq \mathsf{S}x$ since the o-commutators are closed under S.

Suppose $x \in \mathfrak{T}_j$ and $\phi_j(\overline{0}) \wedge \forall y \leq \mathsf{S}x(\phi_j(y) \rightarrow \phi_j(\mathsf{S}y))$. We want to show that $\phi_j(\mathsf{S}x)$. We have that:

$$\phi_j(\overline{0}) \wedge \forall y \leq x(\phi_j(y) \rightarrow \phi_j(\mathsf{S}y))$$

by the assumption that $\phi_j(\overline{0}) \wedge \forall y \leq \mathsf{S}x(\phi_j(y) \rightarrow \phi_j(\mathsf{S}y))$ and the theorem of *i*Q just shown. Thus, we find that $\phi_j(x)$ by implication elimination. Moreover, since $x \in \mathfrak{I}_1$, we have that $x \leq x$ which implies that $x \leq \mathsf{S}x$ again by the theorem of $i\mathsf{Q}$ shown above. This implies that $\phi_j(\mathsf{S}x)$ by implication elimination since $\forall y \leq \mathsf{S}x(\phi_j(y) \rightarrow \phi_j(\mathsf{S}y))$. Finally, we know by Lemma 5 that $\mathfrak{I}_1$ is closed under S. Thus, $\mathfrak{T}_j$ is closed under S and hence, $\mathfrak{T}$ is closed under S.

□

Proposition 14 (in $i\mathsf{Q}$). *Suppose $I \subseteq \mathfrak{T} \cap \mathfrak{I}_2 \cap \mathfrak{I}_6$ and I is closed under $\overline{0}$ and S. (i) Then there is a $J \subseteq I$ closed under $\overline{0}, \mathsf{S}, +$ and $\cdot$. Suppose further that $I \subseteq \mathfrak{I}_1$ and I is downwards closed under $\leq$. (ii) Then J is downwards closed under $\leq$.*

Proof. Let I be as specified for (i). Define:

$$J_0 := \{x \in I \mid \forall y \in I\, y + x \in I\}$$
$$J\ := \{x \in J_0 \mid \forall y \in J_0\, y \cdot x \in J_0\}.$$

By Proposition 10 (i), we have that J_0 is closed under $\overline{0}, \mathsf{S}$ and $+$ since $I \subseteq \mathfrak{I}_2$ and I is closed under $\overline{0}$ and S.

By Proposition 12 (i), we have that J is closed under $\overline{0}, \mathsf{S}, +$ and $\cdot$ since $J_0 \subseteq \mathfrak{I}_6$ and J_0 is closed under $\overline{0}, \mathsf{S}$ and $+$.

Now, let I be as specified for (ii) and let J_0, J be as above.

By Proposition 10 (ii), we have that J_0 is downwards closed under $\leq$ since $I \subseteq \mathfrak{I}_2$, $I \subseteq \mathfrak{I}_1$ and I is downwards closed under $\leq$.

By Proposition 12 (ii), we have that J is downwards closed under $\leq$ since $J_0 \subseteq \mathfrak{I}_6$ and J_0 is downwards closed under $\leq$.

□

Theorem 15. *$i\mathsf{Q}$ locally interprets $iI\Delta_0$.*

Proof. Let $I := \mathfrak{T} \cap \mathfrak{I}_2 \cap \mathfrak{I}_6$ and let $J := \{x \in I \cap \mathfrak{I}_1 \mid \forall y \leq x(y \in I)\}$. By Proposition 8, J is an initial segment since $I \subseteq \mathfrak{I}_2$ and I is closed under $\overline{0}$ and S. Further, by Proposition 14, J is closed under $\overline{0}, \mathsf{S}, +, \cdot$ and downwards closed under $\leq$ since $J \subseteq \mathfrak{T} \cap \mathfrak{I}_2 \cap \mathfrak{I}_6$, J is an initial segment and $J \subseteq \mathfrak{I}_1$.

We claim that J determines an interpretation of induction for $\phi_1, ..., \phi_n$. It suffices to show that:

(i) For each j, $J \subseteq \mathfrak{T} \subseteq \mathfrak{T}_j$ by the absoluteness principle (Lemma 3) since J is closed under $\overline{0}, \mathsf{S}, +, \cdot$ and downwards closed under $\leq$.

(ii) J verifies the nonlogical axioms of $i\mathsf{Q}$.

Ad (i). $J \subseteq \mathfrak{T} \subseteq \mathfrak{T}_j$ for every j is trivially the case by the way we defined J (i.e., since $J \subseteq \mathfrak{T} \cap \mathfrak{I}_2 \cap \mathfrak{I}_6$ and $\mathfrak{T} = \bigcap_{j=1}^{n} \mathfrak{T}_j$).

Ad (ii). J verifies all the nonlogical axioms of $i\mathsf{Q}$ since $J \subseteq \mathfrak{I}_1$ implies that J verifies $(\mathrm{q}3^*)$ and $(\mathrm{q}8)$ by Proposition 6. $(\mathrm{q}1) - (\mathrm{q}2)$ and $(\mathrm{q}4) - (\mathrm{q}7)$ are open formulas of $i\mathsf{Q}$. Hence, the remaining axioms of $i\mathsf{Q}$ are verified by any domain formula, inclusive of J.

Now, since we can choose any $\phi_1, ..., \phi_n \in \Delta_0$ we have that iQ locally interprets $iI\Delta_0$.

□

2.3. iQ INTERPRETS $iI\Delta_0 + \Omega_1$

In this brief subsection, we first outline the coding of the function ω_1 (also known as the smash function # — cf. [2], [10] and [7]), and second, we claim that the original proof that Q interprets $I\Delta_0 + \Omega_1$, given in [10] and [7], goes through constructively.

Define the following function:

$$\omega_1(x) := 2^{|x|\cdot|x|}$$

where $|x|$ is the length of (the binary representation of) x.

Further, let $iI\Delta_0 + \Omega_1$ be the theory $iI\Delta_0$ with the following axiom:

Ω_1. $\exists y(x = \omega_1(y))$

where "$x = \omega_1(y)$" is replaced by the appropriate Δ_0-formula. Next, we outline the crucial features of how to define such a Δ_0-formula.

The main part of the coding of ω_1 is the computation of base two exponentiation. This is tricky since the naïve approach to the Δ_0-definition of the computation of "$2^z = y$" does not turn out to be polynomially bounded. The naïve approach is to compute y by doing a recursion on the exponent using the successor function so that the sequence encoding the graph of the computation would look something like the following:

$$\langle 0,1\rangle, \langle 1,2\rangle, \langle 2,2\cdot 2\rangle, ..., \langle z, \overbrace{2\cdots 2}^{z}\rangle$$

where the first argument of each pair counts up to z and the second argument multiplies the output of the previous pair by 2. The problem with this particular algorithm is that the size of the sequence encoding the computation is not bounded by a polynomial in y. More precisely, given that each pair encodes roughly a computation of the order of the multiplication occurring in the pair, the size of the sequence encoding the naïve computation is roughly of the order:

$$2\cdot 2^2\cdot 2^3\cdot ...\cdot 2^{|y|} = 2^{1+2+...+|y|} \approx 2^{|y|^2} = \omega_1(y)$$

which is clearly not polynomial in y.

In [10] and subsequently in [7], the authors use a trick to avoid the pitfalls of the naïve approach. The trick is to encode the exponent in binary so that the recursion can be carried out more efficiently. Once z is in base 2, we can use the digits of the binary representation of z to indicate how to alter the second argument. In simplest terms, an admissible computation looks as follows: The first input is $\langle 0,1\rangle$, and if we have a stage $\langle m,n\rangle$ the next stage is either $\langle 2\cdot m, n^2\rangle$ or $\langle 2\cdot m+1, 2\cdot n^2\rangle$. So that we have $2^m = n$ if there is a computation ending in $\langle m,n\rangle$.

In this way, the size of a smallest sequence encoding the new computation is bounded by a polynomial in y — its size is approximated by:

$$2 \cdot 2^2 \cdot 2^4 \cdot 2^8 \cdot \ldots \cdot 2^z = 2^{1+2+4+8+\ldots+z} \approx 2^{2 \cdot z} = y^2.$$

To see how it works lets consider the simple example of a computation of 2^9. One possible sequence computing 2^9 would, thus, be as follows:

$$\langle 0,1\rangle, \langle 1, 2\cdot(1)^2\rangle, \langle 2, 2^2\rangle, \langle 4, (2^2)^2\rangle, \langle 9, 2\cdot(2^4)^2\rangle.$$

For the sake of comparison, consider the difference in size between the above sequence and a shortest sequence yielded by the naïve computation:

$$\langle 0,1\rangle, \langle 1,2\rangle, \langle 2,2^2\rangle, \langle 3,2^3\rangle, \langle 4,2^4\rangle, \langle 5,2^5\rangle, \langle 6,2^6\rangle, \langle 7,2^7\rangle, \langle 8,2^8\rangle, \langle 9,2^9\rangle$$

Once the coding of base two exponentiation is in place, it is easy to see that we can define ω_1 as a special case of exponentiation given that the size function, $|\cdot|$, is clearly Δ_0-definable.

We can, thus, proceed with the interpretability of $iI\Delta_0 + \Omega_1$ in $iI\Delta_0$.

Theorem 16. *$i\mathsf{Q}$ interprets $iI\Delta_0 + \Omega_1$.*

Proof. We refer the reader to the proofs given by Hájek and Pudlák ([7], pp.295-304) and Nelson ([10], pp. 36-59), and claim that they go through constructively given our new axiomatization of Q.

□

We now end our investigation into Nelson's result and turn to the main result of this Master's thesis.

3. Alternate Theories: $\mathsf{TC_Q}$ interprets Q

In this section, we begin by proposing a weak theory of concatenation that is meant to be the direct analogue of Q in the language of concatenation, we call the theory $\mathsf{TC_Q}$. The main result of this section (and this Master's thesis) is that $\mathsf{TC_Q}$ interprets Q. In order to arrive at this result, there are several intermediate steps: First, we demonstrate that $\mathsf{TC_Q}$ with the axiom stating the associativity of concatenation is interpretable in $\mathsf{TC_Q}$. Next, we interpret the analogue of $I\Delta_0$, $\mathsf{TC}_{I\Delta_0}$, in $\mathsf{TC_Q}$ with the associativity of concatenation. The associativity axiom is needed in order to achieve closure under concatenation in the shortening cuts used to define the interpretation of $\mathsf{TC}_{I\Delta_0}$. We use the stronger theory $\mathsf{TC}_{I\Delta_0}$ to do the coding of multiplication in the language of concatenation. Finally, we show that $\mathsf{TC}_{I\Delta_0}$ interprets Q, which entails that $\mathsf{TC_Q}$ does.

3.1. Weak Theories of Concatenation

We work in a basic theory of concatenation, $\mathsf{TC_Q}$ which is meant to be the analogue of Q for concatenation theory. The language of TC has three constant symbols $\square$, a and b, two unary function symbols $\mathsf{S_a}$ and $\mathsf{S_b}$, and one binary function symbol $*$.

The theory $\mathsf{TC_Q}$ is given by the following axioms:

tc1. $\mathsf{S}_{\mathsf{a}}x \neq \square$
$\mathsf{S}_{\mathsf{b}}x \neq \square$

tc2. $\mathsf{S}_{\mathsf{a}}x \neq \mathsf{S}_{\mathsf{b}}x$

tc3. $\mathsf{S}_{\mathsf{a}}x = \mathsf{S}_{\mathsf{a}}y \to x = y$
$\mathsf{S}_{\mathsf{b}}x = \mathsf{S}_{\mathsf{b}}y \to x = y$

tc4. $x = \square \vee \exists y(x = \mathsf{S}_{\mathsf{a}}y \vee x = \mathsf{S}_{\mathsf{b}}y)$

tc5. $x * \square = x$

tc6. $x * \mathsf{S}_{\mathsf{a}}y = \mathsf{S}_{\mathsf{a}}(x * y)$
$x * \mathsf{S}_{\mathsf{b}}y = \mathsf{S}_{\mathsf{b}}(x * y)$

In TC_{Q}, we define the following useful abbreviations:

- $\mathsf{a} := \mathsf{S}_{\mathsf{a}}\square$, $\mathsf{b} := \mathsf{S}_{\mathsf{b}}\square$, $\mathsf{ab} := \mathsf{a} * \mathsf{b}$, etc.
- $x \subseteq_{\mathsf{ini}} y :\leftrightarrow \exists z(x * z = y)$
- $x \subseteq_{\mathsf{end}} y :\leftrightarrow \exists z(z * x = y)$
- $x \subseteq_{*} y :\leftrightarrow \exists u \exists v((u * x) * v = y)$
- $\mathsf{tally}(x) :\leftrightarrow \neg \mathsf{b} \subseteq_{*} x$

We can add the substring relation as a primitive rather than as a defined relation. In this case we need the extra axiom.

tc7. $x \subseteq_{*} y \leftrightarrow \exists u \exists v((u * x) * v = y)$

A formula of the language of concatenation is Δ_0^{p} iff all quantifiers are $\subseteq_{*}$-bounded.

The schema for bounded induction in concatenation theory is as follows:

$$(\phi(\square) \wedge \forall y \subseteq_{*} x(\phi(y) \to (\phi(\mathsf{S}_{\mathsf{a}}y) \wedge \phi(\mathsf{S}_{\mathsf{b}}y))) \to \phi(x)$$

where ϕ is a bounded formula of the language of concatenation.

Let $\mathsf{TC}_{I\Delta_0}$ be TC_{Q} together with the schema of bounded induction.

A set I of strings is called an *initial segment* iff I is closed under $\square, \mathsf{S}_{\mathsf{a}}$ and S_{b}, and I is downwards closed under $\subseteq_{*}$.

Here we present the proof of the absoluteness principle for the language of concatenation, needed for the proof of Theorem 26 in section 3.2.

Lemma 17. *Suppose* U *is a theory with the binary predicate symbol* $\subseteq_{*}$ *and* I *is* U*-provably closed. Let* $\phi(\vec{z})$ *be a bounded formula of* U*. Then* U *proves:*

$$\vec{z} : I \to (\phi(\vec{z}) \leftrightarrow \phi(\vec{z})^{I}).$$

Proof. Call a U-formula ϕ *absolute* if U proves:

$$\vec{z} : I \to (\phi(\vec{z}) \leftrightarrow \phi(\vec{z})^{I}).$$

Atomic formulas are absolute since if ϕ is atomic, then ϕ^I is just ϕ so that $I \to (\phi \leftrightarrow \phi^I)$ is a tautology.

Next, suppose ϕ is absolute, then since ϕ and $\neg\phi$ have the same free variables and relativizations, we have that $\neg\phi$ is absolute.

Suppose ϕ_1 and ϕ_2 are absolute. We have that the free variables of $\phi_1 \vee \phi_2$ are precisely those of ϕ_1 and ϕ_2. Moreover, $(\phi_1 \vee \phi_2)^I$ is just $\phi_1^I \vee \phi_2^I$. Thus, $\phi_1 \vee \phi_2$ is absolute.

Suppose $\phi(\vec{z})$ is absolute and ψ is $\exists x(x \subseteq_* t \wedge \phi)$ where x does not occur free in t. Then the free variables of ψ are those free in t (call these $\vec{y}$) and those free in ϕ. Since I is closed under all the function symbols of U, we have that U proves:

$$\vec{y} : I \wedge \vec{z} : I \to I[t].$$

Moreover, since I is downwards closed under $\subseteq_*$, we have that U proves:

$$\vec{y} : I \wedge \vec{z} : I \to (\exists x(x \subseteq_* t \wedge \phi(\vec{z})) \leftrightarrow \exists x(I(x) \wedge x \subseteq_* t \wedge \phi(\vec{z}))).$$

Since ϕ is absolute and $(\vec{y} : I \wedge \vec{z} : I \wedge I(x)) \to \vec{z} : I$ is a tautology, we have that U proves:

$$\vec{y} : I \wedge \vec{z} : I \to (\exists x(x \subseteq_* t \wedge \phi(\vec{z})) \leftrightarrow \exists x(I(x) \wedge x \subseteq_* t \wedge \phi(\vec{z})^I))$$

which is precisely the condition for ψ's absoluteness. Ergo, ψ is absolute.

This completes the induction and hence we have established the absoluteness principle for U.

□

3.2. TC_{Q} INTERPRETS $\mathsf{TC}_{I\Delta_0}$

We first show that TC_{Q} interprets TC_{Q} with the associativity of concatenation. A string x is a *c-associator* iff $\forall y \forall z((y * z) * x = y * (z * x))$. We call the class of c-associative strings $\mathfrak{S}_0$.

Lemma 18 (in TC_{Q}). *$\mathfrak{S}_0$ is closed under $\square, \mathsf{S}_{\mathsf{a}}, \mathsf{S}_{\mathsf{b}}, *$ and predecessors.*

Proof. $\mathfrak{S}_0$ is obviously closed under $\square$ by $(\mathsf{tc5})$.

Moreover, $\mathfrak{S}_0$ is closed under S_{a} (and analogously S_{b}) by $(\mathsf{tc6})$.

Suppose x and x' are both c-associators, then the following is the case:

$$\begin{aligned} y * (z * (x * x')) &= y * ((z * x) * x') \\ &= (y * (z * x)) * x' \\ &= ((y * z) * x) * x' \\ &= (y * z) * (x * x'). \end{aligned}$$

In other words, $x * x'$ is a c-associator.

Finally, $\mathfrak{S}_0$ is closed under predecessors: Suppose $\mathsf{S_a}x \in \mathfrak{S}_0$, then the following is the case:

$$\begin{aligned}\mathsf{S_a}((y*z)*x) &= (y*z)*\mathsf{S_a}x\\ &= y*(z*\mathsf{S_a}x)\\ &= y*\mathsf{S_a}(z*x)\\ &= \mathsf{S_a}(y*(z*x)).\end{aligned}$$

Hence, by (tc3), we have that x is a c-associator. Analogously for the case of $\mathsf{S_b}$.

□

We define $\mathsf{TC_Q}+\mathsf{Assoc}_*$ to be $\mathsf{TC_Q}$ plus the following axiom:

$$\mathsf{Assoc}_*.(y*z)*x = y*(z*x).$$

Lemma 19. $\mathsf{TC_Q}$ *interprets* $\mathsf{TC_Q}+\mathsf{Assoc}_*$.

Proof. The signature of $\mathsf{TC_Q}$ remains the same — that is, τ is the identity translation. Let $I := \mathfrak{S}_0$. By Lemma 18, I is closed under $\square, \mathsf{S_a}, \mathsf{S_b}$ and $*$. Hence, I is an appropriate domain of interpretation. Next, we verify that the translation of the nonlogical axioms of $\mathsf{TC_Q}+\mathsf{Assoc}_*$ are valid in $\mathsf{TC_Q}$. We verify only the case of (tc4) and Assoc_*:

(tc4) $\mathsf{TC_Q} \vdash I(x) \rightarrow (x = \square \vee \exists y(x = \mathsf{S_a}y \vee x = \mathsf{S_b}y))$ since it suffices to show that there exists a $y \in \mathfrak{S}_0$ such that $\mathsf{S_a}y = x$ or $\mathsf{S_b}y = x$, and we have such a y by the fact that $\mathfrak{S}_0$ is closed under predecessors.

(Assoc_*) $\mathsf{TC_Q} \vdash (I(x) \wedge I(y) \wedge I(z)) \rightarrow (y*z)*x = y*(z*x)$ since $I(x)$.

Thus, I and τ determine a relative interpretation of $\mathsf{TC_Q}+\mathsf{Assoc}_*$ in $\mathsf{TC_Q}$.

□

Henceforth, we will work in $\mathsf{TC_Q}+\mathsf{Assoc}_*$. Note, however, that this is not strictly necessary: An analogous construction to the one we used in the case of $i\mathsf{Q}$ (cf. §2.2), would work here as well.

Lemma 20 (in $\mathsf{TC_Q}+\mathsf{Assoc}_*$). *Suppose I is closed under $\square, \mathsf{S_a}$ and $\mathsf{S_b}$. Define*

$$\begin{aligned}J \quad := \quad & \{x \in I \mid \forall y,u,v\,(y*x = u*v \rightarrow\\ & \exists z\,((y*z = u \wedge x = z*v) \vee (y = u*z \wedge z*x = v)))\}.\end{aligned}$$

Then J is closed under $\square, \mathsf{S_a}, \mathsf{S_b}$ and $*$. Moreover, if I is also closed under predecessors, then so is J.

Proof. Assume $y*\square = y = u*v$. Then the second disjunct of the consequent of the condition for membership in J is always satisfied when we choose $z := v$ since $y = u*v$ and $v*\square = v$. Thus, since $\square \in I$ and there is such a z, we have that $\square \in J$.

Suppose $x \in J$. Assume $y*\mathsf{S_a}x = u*v$. We want to show that there is a w such that:

$$(y*w = u \wedge \mathsf{S_a}x = w*v) \vee (y = u*w \wedge w*\mathsf{S_a}x = v)$$

is satisfied. By $(\mathsf{tc4})$, we may assume that $v = \Box \vee \exists v_0 (v = \mathsf{S_a} v_0 \vee v = \mathsf{S_b} v_0)$. If $v = \Box$, then we choose $w := \mathsf{S_a} x$ since $y * \mathsf{S_a} x = u * \Box = u$ and $\mathsf{S_a} x = \mathsf{S_a} x * \Box$.
If $v = \mathsf{S_a} v_0$, then $y * \mathsf{S_a} x = u * \mathsf{S_a} v_0$ implies $y * x = u * v_0$ by $(\mathsf{tc6})$ and $(\mathsf{tc3})$. Since $x \in J$, we have that there exists a z such that $y * z = u \wedge x = z * v_0$ or $y = u * z \wedge z * x = v_0$. In the case of the former, we choose $w := z$, then $y * z = u$ and $\mathsf{S_a} x = \mathsf{S_a}(z * v_0) = z * \mathsf{S_a} v_0 = z * v$. Thus, $(y * w = u \wedge \mathsf{S_a} x = w * v) \vee (y = u * w \wedge w * \mathsf{S_a} x = v)$ is satisfied whenever $y * \mathsf{S_a} x = u * v$:

$$y * \mathsf{S_a} x = y * (z * v) = (y * z) * v = u * v$$

by (Assoc_*). In the case of the latter, if we choose $w := z$, then $y = u * z \wedge z * \mathsf{S_a} x = v$ is satisfied whenever $y * \mathsf{S_a} x = u * v$:

$$u * v = u * (z * \mathsf{S_a} x) = (u * z) * \mathsf{S_a} x = y * \mathsf{S_a} x$$

by (Assoc_*) (I is closed under $\mathsf{S_a}$).
If $v = \mathsf{S_b} v_0$, then we have that $\mathsf{S_a}(y * x) = y * \mathsf{S_a} x = u * \mathsf{S_b} v_0 = \mathsf{S_b}(u * v_0)$ by $(\mathsf{tc6})$. But this is a contradiction since $\mathsf{S_a}(y * x) \neq \mathsf{S_b}(u * v_0)$ by $(\mathsf{tc2})$.
Finally, with all cases covered, we may conclude that $\mathsf{S_a} x \in J$. By similar reasoning, we find that $\mathsf{S_b} x \in J$. Thus, J is closed under $\mathsf{S_a}$ and $\mathsf{S_b}$.

Suppose $x_0, x_1 \in J$. Assume that $y * (x_0 * x_1) = u * v$. We want to show that there exists a w such that:

$$y * w = u \wedge x_0 * x_1 = w * v \quad \text{or} \quad y = u * w \wedge w * (x_0 * x_1) = v.$$

By (Assoc_*), we have that $(y * x_0) * x_1 = u * v$. Moreover, since $x_1 \in J$, we have that there exists a z_0 such that $(y * x_0) * z_0 = u \wedge x_1 = z_0 * v$ or $y * x_0 = u * z_0 \wedge z_0 * x_1 = v$.
In the case of the former, we take the desired $w := x_0 * z_0$ so we have that:

$$y * w = y * (x_0 * z_0) = (y * x_0) * z_0 = u$$

by (Assoc_*), and $w * v = (x_0 * z_0) * v = x_0 * (z_0 * v) = x_0 * x_1$ by (Assoc_*).
In the case of the latter, we have a $z_1 \in \mathfrak{S}_0$ such that (i) $y * z_1 = u \wedge x_0 = z_1 * z_0$ or (ii) $y = u * z_1 \wedge z_1 * x_0 = z_0$ since $x_0 \in J$. If (i) is the case, then we choose $w := z_1$ so we have that: $y * w = y * z_1 = u$ and $w * v = z_1 * v = z_1 * (z_0 * x_1) = (z_1 * z_0) * x_1 = x_0 * x_1$ since x_1 is a c-associator by (Assoc_*). If (ii) is the case, then we choose $w := z_1$ so we have that: $u * w = u * z_1 = y$ and $w * (x_0 * x_1) = z_1 * (x_0 * x_1) = (z_1 * x_0) * x_1 = z_0 * x_1 = v$ by (Assoc_*).
Finally, with all cases covered, we may conclude that $x_0 * x_1 \in J$ (I is closed under $*$). Thus, J is closed under $*$.

□

Define:

$$\begin{aligned} \mathfrak{S}_1 \quad := \quad & \{x \mid \forall y, u, v\, (y * x = u * v \rightarrow \\ & \exists z\, ((y * z = u \wedge x = z * v) \vee (y = u * z \wedge z * x = v)))\} \end{aligned}$$

and define $\mathfrak{S}_2 := \{x \mid \Box * x = x\}$.

Lemma 21 (in $\mathsf{TC_Q} + \mathsf{Assoc}_*$). *$\mathfrak{S}_2$ is closed under $\Box, \mathsf{S_a}, \mathsf{S_b}$ and $*$.*

Proof. It is obvious that $\square \in \mathfrak{S}_2$ by (Assoc_*) and since $\square * \square = \square$ by $(\mathsf{tc5})$.

Suppose $x \in \mathfrak{S}_2$, then by $(\mathsf{tc6})$, we have that $\square * \mathsf{S_a}x = \mathsf{S_a}(\square * x) = \mathsf{S_a}x$. Hence, $\mathsf{S_a}x \in \mathfrak{S}_2$. The same holds *mutatis mutandis* for $\mathsf{S_b}$.

Suppose $x, y \in \mathfrak{S}_2$. Then, by (Assoc_*), we have that $\square * (x * y) = (\square * x) * y = x * y$ since $x \in \mathfrak{S}_2$. Thus, we may conclude that $x * y \in \mathfrak{S}_2$.
□

Lemma 22 (in $\mathsf{TC_Q} + \mathsf{Assoc}_*$). *Suppose $I \subseteq \mathfrak{S}_2$ and I is an initial segment. Then I verifies* $(\mathsf{tc4})$ *and* $(\mathsf{tc7})$.

Proof. Suppose $\mathsf{S_a}x \in I$. We have that $x * \mathsf{S_a}\square = \mathsf{S_a}x$ by $(\mathsf{tc5})$ and $(\mathsf{tc6})$. Moreover, $\square * x * \mathsf{S_a}\square = \mathsf{S_a}x$ since $x \in \mathfrak{S}_2$ and hence, we have that $x \subseteq_* \mathsf{S_a}x$. Thus, $x \in I$ since I is downwards closed under $\subseteq_*$. Similarly for the case of $\mathsf{S_b}$. This means that any non-empty string in I has a predecessor in I, whence $(\mathsf{tc4})$ holds.

Suppose $x \subseteq_* y$ and $y \in I$, then for some u, v, $(u * x) * v = y$. Hence, it suffices to show that $u, v \in I$. We have that $(u * x) * v * \square = y$ by $(\mathsf{tc5})$ and hence, $v \subseteq_* y$. Thus, $v \in I$ since I is downwards closed under $\subseteq_*$. Moreover:

$$\begin{aligned} y &= \square * y \\ &= \square * ((u * x) * v) \\ &= (\square * (u * x)) * v \\ &= ((\square * u) * x) * v \\ &= (\square * u) * (x * v) \end{aligned}$$

since $y \in I \subseteq \mathfrak{S}_2$ and $v, x \in I \subseteq \mathfrak{S}_0$ by (Assoc_*). Thus, $u \subseteq_* y$ and we have that $u \in I$ since I is downwards closed under $\subseteq_*$. Finally, we have that $\exists u, v \in I\ ((u * x) * v = y)$. □

Lemma 23 (in $\mathsf{TC_Q} + \mathsf{Assoc}_*$). *Suppose $I \subseteq \mathfrak{S}_1$ and I is closed under $\square, \mathsf{S_a}, \mathsf{S_b}$ and $*$. Let $J := \{x \in I \mid \forall y \subseteq_* x\ (y \in I)\}$. Then J is an initial segment and J is closed under $*$.*

Proof. By $(\mathsf{tc5})$ and (Assoc_*), we have that for all $y \subseteq_* \square$, $y = \square$. Hence, J is closed under $\square$ since $\square \in I$.

Suppose $x \in J$. Assume $y \subseteq_* \mathsf{S_a}x$. Then there exists u, v such that $(u * y) * v = \mathsf{S_a}x = x * \mathsf{S_a}\square = x * \mathsf{a}$. Since $\mathsf{a} \in I$, we have that there exists a z_0 such that:

$$(u * y) * z_0 = x \wedge v = z_0 * \mathsf{a} \quad \text{or} \quad u * y = x * z_0 \wedge z_0 * v = \mathsf{a}.$$

In the former case, $y \subseteq_* x$ so that $y \in I$. In latter case, we note that $v = \square \vee \exists v_0 (v = \mathsf{S_a}v_0 \vee v = \mathsf{S_b}v_0)$ by $(\mathsf{tc4})$.
If $v = \square$, then we find that $z_0 = \mathsf{S_a}\square = \mathsf{a}$ and hence, $u * y = x * \mathsf{a}$. Since $\mathsf{a} \in I$, we have that there exists a z_1 such that (i) $u * z_1 = x \wedge y = z_1 * \mathsf{a}$ or (ii) $u = x * z_1 \wedge z_1 * y = \mathsf{a}$. If (i) is the case, then $z_1 \subseteq_* x$, $y = \mathsf{S_a}z_1$ and the fact that I is closed under $\mathsf{S_a}$ implies that $y \in I$. If (ii) is the case, then $y \subseteq_* \mathsf{a}$ implies $y \in I$.
If $v = \mathsf{S_a}v_0$, then $z_0 * v_0 = \square$ by $(\mathsf{tc6})$ and $(\mathsf{tc3})$. So we have that $z_0 = \square$ by the theorem of $\mathsf{TC_Q}$

shown above. By our case supposition this gives $u * y = x * \square = x$ which implies that $y \subseteq_* x$. Thus, $y \in I$.
If $v = \mathsf{S}_\mathsf{b} v_0$, then we have a contradiction since $z_0 * v = \mathsf{S}_\mathsf{b}(z_0 * v_0) \neq \mathsf{S}_\mathsf{a}\square$ by $(\mathrm{tc2})$ but we have that $z_0 * v = \mathsf{S}_\mathsf{a}\square$ from our case supposition.

Suppose $y \subseteq_* x$ and $x \in J$. We want to show that $y \in J$. Assume $y_0 \subseteq_* y$. Then there exists u_0, v_0 such that $(u_0 * y_0) * v_0 = y$. Moreover, since $y \subseteq_* x$, there exists u, v such that $(u * y) * v = x$. Hence, $(u * u_0) * y_0 * (v_0 * v) = x$ by (Assoc_*). Thus, $y_0 \subseteq_* x$ so that $y \in I$.

Suppose $x_0, x_1 \in J$ and $x_0 * x_1 \subseteq_* y$. Then, for some u, v, we have that $(u * y) * v = u * (y * v) = x_0 * x_1$ by (Assoc_*). Since $x_1 \in I \subseteq \mathfrak{S}_1$, there exists a z_0 such that:

$$x_0 * z_0 = u \wedge x_1 = z_0 * (y * v) \quad \text{or} \quad x_0 = u * z_0 \wedge z_0 * x_1 = y * v.$$

In the case of the former, we have that $y \subseteq_* x_1$ by the second conjunct, whence $y \in I$.
In the case of the latter, since $x_1 \in I \subseteq \mathfrak{S}_1$, we have that there exists a z_1 such that:

$$\text{(i) } z_0 * z_1 = y \wedge x_1 = z_1 * v \quad \text{or} \quad \text{(ii) } z_0 = y * z_1 \wedge z_1 * x_1 = v.$$

If (i) is the case, we note that $z_0 \subseteq_* x_0$ by the first conjunct of the above and $z_1 \subseteq_* x_1$ by the second conjunct of (i). Hence, $z_0, z_1 \in I$. Thus, $y = z_0 * z_1 \in I$ since I is closed under $*$. If (ii) is the case, then we find that $y \subseteq_* z_0 \subseteq_* x_0$ by the first conjunct of (ii) and the first conjunct of the above. So, $y \subseteq_* x_0$: there exists w_0, w_1 such that $w_0 * y * w_1 = z_0$ and w'_0, w'_1 such that $w'_0 * z_0 * w'_1 = x_0$ and hence, $(w_0 * w'_0) * z_0 * (w_1 * w'_1) = x_0$ by (Assoc_*). Thus, we have that $y \in I$.

□

Let $\phi_1(x), ..., \phi_n(x)$ be given Δ^{p}_0-formulas where x occurs free. For each $j = 1, ..., n$, we define:

$$\mathfrak{T}_j := \{x \in \mathfrak{S}_2 \mid (\phi_j(\square) \ \wedge \ \forall y \subseteq_* x(\phi_j(y) \rightarrow \phi_j(\mathsf{S}_\mathsf{a} y) \wedge \phi_j(\mathsf{S}_\mathsf{b} y))) \rightarrow \phi_j(x)\}.$$

Moreover, we let $\mathfrak{T} := \bigcap_{j=1}^{n} \mathfrak{T}_j$.

Lemma 24 (in TC_Q). *$\mathfrak{T}$ is closed under $\square, \mathsf{S}_\mathsf{a}$ and S_b.*

Proof. Suppose $\phi_j(\square) \wedge \forall y \subseteq_* \square(\phi_j(y) \rightarrow \phi_j(\mathsf{S}_\mathsf{a} y) \wedge \phi_j(\mathsf{S}_\mathsf{b} y))$, then each $\mathfrak{T}_j$ is closed under $\square$ since $\square \in \mathfrak{S}_2$ and $\phi_j(\square)$ is trivially the case. Hence, $\square \in \bigcap_{j=1}^{n} \mathfrak{T}_j = \mathfrak{T}$.

To show that each $\mathfrak{T}_j$ is closed under S_a and S_b, we need to prove that:

$$y \subseteq_* x \rightarrow y \subseteq_* \mathsf{S}_\mathsf{a} x \wedge y \subseteq_* \mathsf{S}_\mathsf{b} x$$

is a theorem of TC_Q: Suppose $y \subseteq_* x$. By $(\mathrm{tc6})$ and the functionality of S_a and S_b, we find that $(u * y) * \mathsf{S}_\mathsf{a} v = \mathsf{S}_\mathsf{a}((u * y) * v) = \mathsf{S}_\mathsf{a} x$ and similarly for S_b Thus, $y \subseteq_* \mathsf{S}_\mathsf{a} x$ and $y \subseteq_* \mathsf{S}_\mathsf{b} x$.

Suppose $x \in \mathfrak{T}_j$ and $\phi_j(\square) \wedge \forall y \subseteq_* \mathsf{S}_\mathsf{a} x(\phi_j(y) \rightarrow \phi_j(\mathsf{S}_\mathsf{a} y) \wedge \phi_{j(}(\mathsf{S}_\mathsf{b} y))$. We want to show that $\phi_j(\mathsf{S}_\mathsf{a} x)$. We have that:

$$\phi_j(\square) \wedge \forall y \subseteq_* x(\phi_j(y) \rightarrow \phi_j(\mathsf{S}_\mathsf{a} y) \wedge \phi_j(\mathsf{S}_\mathsf{b} y))$$

by the assumption that $\phi_j(\square) \wedge \forall y \subseteq_* \mathsf{S}_\mathsf{a} x(\phi_j(y) \rightarrow \phi_j(\mathsf{S}_\mathsf{a} y) \wedge \phi_j(\mathsf{S}_\mathsf{b} y))$ and the theorem of TC_Q just shown. Thus, we find that $\phi_j(x)$ by implication elimination. Moreover, since $x \in \mathfrak{S}_2$, we have that $x \subseteq_* x$ which implies that $x \subseteq_* \mathsf{S_a}x$ again by the theorem of $\mathsf{TC_Q}$ shown above. This implies that $\phi_j(\mathsf{S_a}x)$ since we have that $\forall y \subseteq_* \mathsf{S_a}x(\phi_j(y) \to \phi_j(\mathsf{S_a}y) \wedge \phi_j(\mathsf{S_b}y))$. Finally, we know by Lemma 21 that $\mathfrak{S}_2$ is closed under $\mathsf{S_a}$. Thus, $\mathfrak{T}_j$ is closed under $\mathsf{S_a}$ and hence, $\mathfrak{T}$ is closed under $\mathsf{S_a}$. The same proof works for the case of $\mathsf{S_b}$. Therefore, we also have that $\mathfrak{T}$ is closed under $\mathsf{S_b}$.

□

Proposition 25 (in $\mathsf{TC_Q} + \mathsf{Assoc}_*$). *Suppose $I \subseteq \mathfrak{T}$ and I is closed under $\square, \mathsf{S_a}$ and $\mathsf{S_b}$.*
(i) Then there is a $J \subseteq I$ closed under $\square, \mathsf{S_a}, \mathsf{S_b}$ and $*$. Suppose further that $J \subseteq \mathfrak{S}_1$.
(ii) Then there is a $J' \subseteq J$ closed under $\square, \mathsf{S_a}, \mathsf{S_b}$ and $*$ that is downwards closed under $\subseteq_*$.

Proof. Since $I \subseteq \mathfrak{T}$ and I is closed under $\square, \mathsf{S_a}$ and $\mathsf{S_b}$, by Lemma 20, we have that there is a $J \subseteq I$ closed under $\square, \mathsf{S_a}, \mathsf{S_b}$ and $*$.

Since $J \subseteq I \subseteq \mathfrak{T} \cap \mathfrak{S}_1$ and J is closed under $\square, \mathsf{S_a}$ and $\mathsf{S_b}$, by Lemma 23, we have that there is a $J' \subseteq J$ closed under $\square, \mathsf{S_a}, \mathsf{S_b}$ and $*$ that is downwards closed under $\subseteq_*$.

□

Theorem 26. $\mathsf{TC_Q}$ *locally interprets* $\mathsf{TC}_{I\Delta_0}$.

Proof. By Lemma 19, it suffices to show that $\mathsf{TC_Q} + \mathsf{Assoc}_*$ interprets $\mathsf{TC}_{I\Delta_0}$. We let $I := \mathfrak{T} \cap \mathfrak{S}_0$,

$$\begin{aligned} J \quad &:= \quad \{x \in I \mid \forall y, u, v(y * x = u * v \to \\ &\qquad \exists z((y * z = u \wedge x = z * v) \vee (y = u * z \wedge z * x = v)))\} \end{aligned}$$

and let $J_0 := \{x \in J \mid \forall y \subseteq_* x(y \in J)\}$. By Lemma 20, J is closed under $\square, \mathsf{S_a}, \mathsf{S_b}$ and $*$ since $J \subseteq \mathfrak{S}_0$ and I is closed under $\square, \mathsf{S_a}$ and $\mathsf{S_b}$. Further, by Lemma 23, J_0 is an initial segment and closed under $*$ since $J_0 \subseteq \mathfrak{T} \cap \mathfrak{S}_1 \subseteq \mathfrak{S}_1$ and J is closed under $\square, \mathsf{S_a}, \mathsf{S_b}$ and $*$.

We claim that J_0 determines an interpretation of induction for $\phi_1, ..., \phi_n$. It suffices to show that:

(i) For each j, $J_0 \subseteq \mathfrak{T} \subseteq \mathfrak{T}_j$ by the absoluteness principle (Lemma 17) since J_0 is closed under $\square, \mathsf{S_a}, \mathsf{S_b}, *$ and downwards closed under $\subseteq_*$.

(ii) J_0 verifies the nonlogical axioms of $\mathsf{TC_Q}$.

Ad (i). $J_0 \subseteq \mathfrak{T} \subseteq \mathfrak{T}_j$ for every j is trivially the case by the way we defined J_0 (i.e., since $J_0 \subseteq \mathfrak{T} \cap \mathfrak{S}_1$ and $\mathfrak{T} = \bigcap_{j=1}^{n} \mathfrak{T}_j$).

Ad (ii). J_0 verifies all the nonlogical axioms of $\mathsf{TC_Q}$ since $J_0 \subseteq \mathfrak{S}_2$ implies that J_0 verifies (tc4) and (tc7) by Lemma 22. (tc1) – (tc3) and (tc5) – (tc6) are open formulas of $\mathsf{TC_Q}$. Hence, the remaining axioms of $\mathsf{TC_Q} + \mathsf{Assoc}_*$ are verified by any domain formula, inclusive of J_0.

Now, since we can choose any $\phi_1, ..., \phi_n \in \Delta_0^{\mathsf{P}}$ we have that $\mathsf{TC_Q} + \mathsf{Assoc}_*$ locally interprets $\mathsf{TC}_{I\Delta_0}$, which implies that $\mathsf{TC_Q}$ does.

□

It is also possible to show that $\mathsf{TC_Q}$ globally interprets $\mathsf{TC}_{I\Delta_0}$ by adapting a trick due to Alex Wilkie. However, we will not pursue this line of investigation here.

3.3. Developing Arithmetic in Concatenation Theory

In order to show that multiplication is definable in $\mathsf{TC_Q}$, we first code finite relations between tally numbers as strings over the alphabet $\{\mathtt{a},\mathtt{b}\}$. We construct our coding as follows: A finite relation is coded as a sequence of tuples satisfying that relation with specific strings between each element of the tuple and between each element of the relation itself. This can be done in numerous ways. The elements of relations in our case are strings of a's so that coding becomes rather simple. Let $c_1 := \mathtt{bb}$ and $c_2 := \mathtt{ba}$ be the *seperators* between elements of the relation and elements of the tuples respectively. Under this coding, a finite binary relation between tallies (strings of a's), $s_1,t_1,s_2,t_2,...,s_k,t_k$ (where s_i,t_i are paired) is, thus, represented by any string r containing the following pairs as substrings:

$$\mathtt{bb}*s_1*\mathtt{ba}*t_1*\mathtt{bb}, \mathtt{bb}*s_2*\mathtt{ba}*t_2*\mathtt{bb}, ..., \mathtt{bb}*s_k*\mathtt{ba}*t_k*\mathtt{bb}$$

unless one of the pair happens to be an endstring of the string in question r; in which case, $\mathtt{bb}*s_i*\mathtt{ba}*t_i*\mathtt{bb}$ needn't be a substring of r, but merely $\mathtt{bb}*s_i*\mathtt{ba}*t_1$ or $\mathtt{bb}*s_i*\mathtt{ba}*t_i*\mathtt{b}$ need be endstrings of r. Note that this coding does not uniquely pick out a relation for any given set of pairs: In particular, the pairs might appear in any order yielding different strings representing the relation. Moreover, they might appear many times throughout giving still different representations of the relation. What is more, there might be "garbage" substrings between any of the pairs yielding still different representations of the relation.

More precisely, we code the pairs and relations in a definitional extension of $\mathsf{TC_Q}$ as follows:

$$\mathsf{pair}(x) \quad :\leftrightarrow \quad \exists t_1,t_2\ (\mathsf{tally}(t_1)\wedge\mathsf{tally}(t_2)\wedge x=\mathtt{bb}*t_1*\mathtt{ba}*t_2)$$

$$\begin{aligned} u[x]v \quad :\leftrightarrow \quad & \mathsf{tally}(u)\wedge\mathsf{tally}(v)\wedge(\mathtt{bb}*u*\mathtt{ba}*v\subseteq_{\mathsf{end}} x \vee \mathtt{bb}*u*\mathtt{ba}*v*\mathtt{b}\subseteq_{\mathsf{end}} x \vee \\ & \mathtt{bb}*u*\mathtt{ba}*v*\mathtt{bb}\subseteq_{*} x) \end{aligned}$$

The relations that define a computation of multiplication, "$x\cdot y=z$", are given by those strings r such that the empty pair is part of r and for all tallies u and v that form a pair that is part of r, we have that $u=v=\square$ or there are tallies u',v' such that $u=u'*\mathtt{a}$ and $v=v'*x$. For example, r might be one of the following (amongst others) if $x=2$ and $y=3$:

- $\mathtt{bb\square ba\square}*\mathtt{bbabaaa}*\mathtt{bbaabaaaaa}*\mathtt{bbaaabaaaaaaa}$
- $\mathtt{bbabaaa}*\mathtt{bbaaabaaaaaaa}*\mathtt{bb\square ba\square}*\mathtt{bbaabaaaaa}$
- $\mathtt{bb\square ba\square}*\mathtt{bbabaaa}*\mathtt{bbaabaaaaa}*\mathtt{bbaaabaaaaaaa}*\mathtt{bbabaaa}*\mathtt{baabaaaaa}*\mathtt{baabaaaaa}$
- $\mathtt{bb\square ba\square}*\mathtt{bbabaaa}*\mathtt{bababababababababababababbbbbbbbbbb}*\mathtt{bbaabaaaaa}*\mathtt{bbaaabaaaaaaa}$
- $\mathtt{babababababbbbb}*\mathtt{bbabaaa}*\mathtt{bbaaabaaaaaaa}*\mathtt{bb\square ba\square}*\mathtt{bbaabaaaaab}*\mathtt{bb\square ba\square}$

More precisely, the computation of multiplication is encoded by the following:

$$\begin{aligned} \mathsf{multrel}(u,x) \quad :\leftrightarrow \quad & \mathsf{tally}(x)\wedge\square[u]\square\wedge\forall s,t\ (s[u]t\rightarrow \\ & ((s=\square\wedge t=\square)\vee\exists s',t'\ (s'[u]t'\wedge s=s'*\mathtt{a}\wedge t=t'*x))) \end{aligned}$$

$$x\odot y=z \quad :\leftrightarrow \quad \exists u\ (\mathsf{multrel}(u,x)\wedge y[u]z)$$

For the remainder of this subsection, we aim to prove that our coding preserves the structural properties of multiplication (Proposition 30).

Lemma 27 **(in $\mathsf{TC}_{I\Delta_0}$).** *The following is provable:*

$$\forall u,y,z\,(x = y*z \wedge u \subseteq_* x \to (u \subseteq_* y \vee u \subseteq_* z \vee \exists v,w\,(v \subseteq_{\mathsf{end}} y \wedge w \subseteq_{\mathsf{ini}} z \wedge u = v*w))).$$

Proof. We show the desired fact by Δ_0^{p}-induction over ϕ with:

$$\begin{aligned}\phi(x) \quad :\leftrightarrow \quad & \forall u,y,z\,((x = y*z \wedge u \subseteq_* x) \to \\ & (u \subseteq_* y \vee u \subseteq_* z \vee \exists v,w\,(v \subseteq_{\mathsf{end}} y \wedge w \subseteq_{\mathsf{ini}} z \wedge u = v*w))).\end{aligned}$$

Note that $\phi(x)$ can easily be rewritten as a Δ_0^{p}-formula.

We have that $\phi(\square)$: If $y*z = \square$ and $u \subseteq_* \square$, then we have that $u \subseteq_* y$ since $u = \square$. Hence, the consequent of $\phi(\square)$ is trivially satisfied.

Assume $\phi(x)$. We want to show that $\phi(\mathsf{S_a}x)$ and $\phi(\mathsf{S_b}x)$.

Ad $\phi(\mathsf{S_a}x)$. Let y be fixed. We show that:

$$\forall u,z\,((\mathsf{S_a}x = y*z \wedge u \subseteq_* \mathsf{S_a}x) \to (u \subseteq_* y \vee u \subseteq_* z \vee \exists v,w\,(v \subseteq_{\mathsf{end}} y \wedge w \subseteq_{\mathsf{ini}} z \wedge u = v*w)))$$

by induction on z. Define:

$$\begin{aligned}\psi(z) \quad :\leftrightarrow \quad & \forall u((\mathsf{S_a}x = y*z \wedge u \subseteq_* \mathsf{S_a}x) \to \\ & (u \subseteq_* y \vee u \subseteq_* z \vee \exists v,w\,(v \subseteq_{\mathsf{end}} y \wedge w \subseteq_{\mathsf{ini}} z \wedge u = v*w))).\end{aligned}$$

We have that $\psi(\square)$: Suppose $\mathsf{S_a}x = y*\square$ and $u \subseteq_* \mathsf{S}_a x$. Then we have that $u \subseteq_* y$ by (tc5). Hence, the consequent of $\psi(\square)$ holds.

Assume $\psi(z)$. We want to show that $\psi(\mathsf{S_a}z)$ and $\psi(\mathsf{S_b}z)$.

For $\psi(\mathsf{S}_a z)$: Suppose $\mathsf{S_a}x = y*\mathsf{S_a}z$ and $u \subseteq_* \mathsf{S_a}x$. Then there exist s,s' such that:

$$s*u*s' = \mathsf{S_a}x = y*\mathsf{S_a}z.$$

By (tc4), we have that $s' = \square \vee \exists s_0'(s' = \mathsf{S_a}s_0' \vee s' = \mathsf{S_b}s_0')$.

In case $s' = \mathsf{S_a}s_0'$, we have that $\mathsf{S_a}(s*u*s_0') = \mathsf{S_a}x = \mathsf{S_a}(y*z)$ by (tc6). By (tc3), we have that $s*u*s_0' = x = y*z$. So, $u \subseteq_* x$ and $x = y*z$. Thus, by the induction hypothesis $\phi(x)$, we have that:

$$u \subseteq_* y, \quad u \subseteq_* z \quad \text{or} \quad \exists v,w\,(v \subseteq_{\mathsf{end}} y \wedge w \subseteq_{\mathsf{ini}} z \wedge u = v*w)).$$

If $u \subseteq_* y$, then the consequent of $\psi(\mathsf{S_a}z)$ holds and hence, $\psi(\mathsf{S_a}z)$ does. If $u \subseteq_* z$, then since $z \subseteq_* \mathsf{S_a}z$, we have that $u \subseteq_* \mathsf{S_a}z$, so that $\psi(\mathsf{S_a}z)$ holds. If $\exists v,w\,(v \subseteq_{\mathsf{end}} y \wedge w \subseteq_{\mathsf{ini}} z \wedge u = v*w))$, then we have that $w \subseteq_{\mathsf{ini}} \mathsf{S_a}z$ and so we have that $\exists v,w\,(v \subseteq_{\mathsf{end}} y \wedge w \subseteq_{\mathsf{ini}} \mathsf{S_a}z \wedge u = v*w))$ and so, $\psi(\mathsf{S_a}z)$ holds.

In case $s' = \mathsf{S}_{\mathsf{b}}s'_0$, we have a contradiction since $\mathsf{S}_{\mathsf{b}}(s*u*s'_0) = \mathsf{S}_{\mathsf{a}}x$ by (tc6), but $\mathsf{S}_{\mathsf{b}}(s*u*s'_0) \neq \mathsf{S}_{\mathsf{a}}x$ by (tc2).

In case $s' = \Box$, we have that $s*u = \mathsf{S}_{\mathsf{a}}x$ and again by (tc4) that $u = \Box \vee \exists u_0(u = \mathsf{S}_{\mathsf{a}}u_0 \vee u = \mathsf{S}_{\mathsf{b}}u_0)$. If $u = \Box$, then $u = \Box \subseteq_* y$ so that the consequent of $\psi(\mathsf{S}_{\mathsf{a}}z)$ is trivially satisfied. If $u = \mathsf{S}_{\mathsf{b}}u_0$, then we have a contradiction since $\mathsf{S}_{\mathsf{a}}x = s*\mathsf{S}_{\mathsf{b}}u_0 = \mathsf{S}_{\mathsf{b}}(s*u_0)$, but by (tc2), $\mathsf{S}_{\mathsf{a}}x \neq \mathsf{S}_{\mathsf{b}}(s*u_0)$. If $u = \mathsf{S}_{\mathsf{a}}u_0$, then $\mathsf{S}_{\mathsf{a}}(s*u_0) = \mathsf{S}_{\mathsf{a}}x = \mathsf{S}_{\mathsf{a}}(y*z)$. Hence, by (tc3), $s*u_0 = x = y*z$ so that $u_0 \subseteq_* x$ and $x = y*z$. Thus, by the induction hypothesis $\phi(x)$, we have that:

$$u_0 \subseteq_* y \vee u_0 \subseteq_* z \vee \exists v_0, w_0(v_0 \subseteq_{\mathsf{end}} y \wedge w_0 \subseteq_{\mathsf{ini}} z \wedge u_0 = v_0 * w_0).$$

We consider each disjunct in turn. When $u_0 \subseteq_* y$, then there exist r, r' such that $r*u_0*r' = y$, and by (tc4) we have that $r' = \Box \vee \exists r'_0(r' = \mathsf{S}_{\mathsf{a}}r'_0 \vee r' = \mathsf{S}_{\mathsf{b}}r'_0)$. If $r' = \Box$, then there exists v, w such that $v \subseteq_{\mathsf{end}} y \wedge w \subseteq_{\mathsf{ini}} z \wedge u = v*w)$ — namely, $v := u_0$ and $w := \mathsf{a}$. If $r' = \mathsf{S}_{\mathsf{a}}r'_0$ or $r' = \mathsf{S}_{\mathsf{b}}r'_0$, then $u \subseteq_* y$ since $u_0 \subseteq_* y$, $r' \neq \Box$, $y \subseteq_* x$ and $u \subseteq_* x$.When $u_0 \subseteq_* z$, we have that $u \subseteq_* \mathsf{S}_{\mathsf{a}}z$ since $u_0 \subseteq_* z$, $u_0 \subseteq_{\mathsf{ini}} u$, $z \subseteq_* \mathsf{S}_{\mathsf{a}}x$ and $u \subseteq_* \mathsf{S}_{\mathsf{a}}x$. When $\exists v_0, w_0(v_0 \subseteq_{\mathsf{end}} y \wedge w_0 \subseteq_{\mathsf{ini}} z \wedge u_0 = v_0 * w_0)$, then there exist v, w such that $v \subseteq_{\mathsf{end}} y \wedge w \subseteq_{\mathsf{ini}} z \wedge u = v*w)$ — namely, $v := v_0$ and $w := \mathsf{S}_{\mathsf{a}}w_0$.

For $\psi(\mathsf{S}_{\mathsf{b}}z)$: No matter what the value of u, the antecedent is always false and hence, the implication is trivially satisfied.

Therefore, we may conclude that $\phi(\mathsf{S}_{\mathsf{a}}x)$. *Ad* $\phi(\mathsf{S}_{\mathsf{b}}x)$ we use an analogous argument *mutadis mutandis*.

□

Lemma 28 (in $\mathsf{TC}_{I\Delta_0}$). *The following is provable:*

$$\forall r, u, v\, \exists s\, \forall x, y\, ((x[s]y \wedge \mathsf{tally}(u) \wedge \mathsf{tally}(v)) \leftrightarrow$$
$$(\mathsf{tally}(u) \wedge \mathsf{tally}(v) \wedge (x[r]y \vee (x = u \wedge y = v)))).$$

Proof. Let r, u and v be arbitrary strings. Choose $s := r*(\mathtt{bb}*u*\mathtt{ba}*v)$ and let x and y be arbitrary strings. We show that $(x[s]y \wedge \mathsf{tally}(u) \wedge \mathsf{tally}(v)) \leftrightarrow (\mathsf{tally}(u) \wedge \mathsf{tally}(v) \wedge (x[r]y \vee (x = u \wedge y = v)))$.

Suppose $x[s]y \wedge \mathsf{tally}(u) \wedge \mathsf{tally}(v)$ – that is, u, v, x and y are tallies, and:

$$(\mathtt{bb}*x*\mathtt{ba}*y \subseteq_{\mathsf{end}} s \vee \mathtt{bb}*x*\mathtt{ba}*y*\mathtt{b} \subseteq_{\mathsf{end}} s \vee \mathtt{bb}*x*\mathtt{ba}*y*\mathtt{bb} \subseteq_* s).$$

This yields three cases to consider.

Case 1: If $\mathtt{bb}*x*\mathtt{ba}*y \subseteq_{\mathsf{end}} s$, then by Lemma 27 we have that $\mathtt{bb}*x*\mathtt{ba}*y \subseteq_{\mathsf{end}} \mathtt{bb}*u*\mathtt{ba}*v$ or there exist w_1 and w_2 such that:

$$w_1 \subseteq_{\mathsf{end}} r \wedge w_2 = \mathtt{bb}*u*\mathtt{ba}*v \wedge \mathtt{bb}*x*\mathtt{ba}*y = w_1 * w_2.$$

In case $\mathtt{bb}*x*\mathtt{ba}*y \subseteq_{\mathsf{end}} \mathtt{bb}*u*\mathtt{ba}*v$, then there exists a z such that $z*\mathtt{bb}*x*\mathtt{ba}*y = \mathtt{bb}*u*\mathtt{ba}*v$. By (tc4), we have that $z = \Box \vee \exists z_0(z = \mathsf{S}_{\mathsf{a}}z_0 \vee z = \mathsf{S}_{\mathsf{b}}z_0)$. If $z = \Box$, then we have that $\mathtt{bb}*x*\mathtt{ba}*y = \mathtt{bb}*u*\mathtt{ba}*v$, and hence, $x = u \wedge y = v$. If $z = \mathsf{S}_{\mathsf{b}}z_0$, then we have that $z_0*\mathtt{b}*\mathtt{bb}*x*\mathtt{ba}*y = \mathtt{bb}*u*\mathtt{ba}*v$, but since $\mathtt{bbb} \not\subseteq_* \mathtt{bb}*u*\mathtt{ba}*v$, we have a contradiction. If $z = \mathsf{S}_{\mathsf{a}}z_0$, then $z_0*\mathtt{a}*\mathtt{bb}*x*\mathtt{ba}*y = \mathtt{bb}*u*\mathtt{ba}*v$, but $\mathtt{abb} \not\subseteq_* \mathtt{bb}*u*\mathtt{ba}*v$ means we have a

contradiction.
In case there are w_1 and w_2 such that:

$$w_1 \subseteq_{\mathsf{end}} r \wedge w_2 = \mathtt{bb} * u * \mathtt{ba} * v \wedge \mathtt{bb} * x * \mathtt{ba} * y = w_1 * w_2,$$

then by (tc4) we have that $w_2 = \Box \vee \exists w_1'(w_1 = \mathsf{S}_\mathsf{a} w_1' \vee w_1 = \mathsf{S}_\mathsf{b} w_1')$. If $w_1 = \Box$, then $\mathtt{bb} * x * \mathtt{ba} * y = \Box * \mathtt{bb} * u * \mathtt{ba} * v$, and hence $x = u \wedge y = v$. If $w_1 = \mathsf{S}_\mathsf{b} w_1'$, then we have that $w_1' * \mathtt{b} * \mathtt{bb} * u * \mathtt{ba} * v = \mathtt{bb} * x * \mathtt{ba} * y$, but since $\mathtt{bbb} \not\subseteq_* \mathtt{bb} * x * \mathtt{ba} * y$, we have a contradiction . If $w_1 = \mathsf{S}_\mathsf{a} w_1'$, then we have a contradiction since $w_0' * \mathtt{a} * \mathtt{bb} * u * \mathtt{ba} * v = \mathtt{bb} * x * \mathtt{ba} * y$ and $\mathtt{abb} \not\subseteq_* \mathtt{bb} * x * \mathtt{ba} * y$.
Hence, if $\mathtt{bb} * x * \mathtt{ba} * y \subseteq_{\mathsf{end}} s$, then $x = u \wedge y = v$.

Case 2: If $\mathtt{bb} * x * \mathtt{ba} * y * \mathtt{b} \subseteq_{\mathsf{end}} s$, then we have a contradiction since: $\mathtt{bb} * x * \mathtt{ba} * y * \mathtt{b} \subseteq_{\mathsf{end}} s$ implies that $\exists z(z * \mathtt{bb} * x * \mathtt{ba} * y * \mathtt{b} = s)$. So that, by (tc6):

$$\mathsf{S}_\mathsf{b}(z * \mathtt{bb} * x * \mathtt{ba} * y) = r * \mathtt{bb} * u * \mathtt{ba} * v$$

where $\mathsf{tally}(v)$. If $v = \Box$, then we have that $\mathsf{S}_\mathsf{b}(z * \mathtt{bb} * x * \mathtt{ba} * y) = \mathsf{S}_\mathsf{a}(r * \mathtt{bb} * u * \mathtt{b})$ by (tc5) and (tc6), but then we have a contradiction by (tc2) since $\mathsf{S}_\mathsf{b}(z * \mathtt{bb} * x * \mathtt{ba} * y) \neq \mathsf{S}_\mathsf{a}(r * \mathtt{bb} * u * \mathtt{b})$. If $v = \mathsf{S}_\mathsf{a} v_0$, then we have that $\mathsf{S}_\mathsf{b}(z * \mathtt{bb} * x * \mathtt{ba} * y) = \mathsf{S}_\mathsf{a}(r * \mathtt{bb} * u * \mathtt{ba} * v_0)$, but this is a contradiction since $\mathsf{S}_\mathsf{b}(z * \mathtt{bb} * x * \mathtt{ba} * y) \neq \mathsf{S}_\mathsf{a}(r * \mathtt{bb} * u * \mathtt{ba} * v_0)$ by (tc2).

Case 3: Finally, if $\mathtt{bb} * x * \mathtt{ba} * y * \mathtt{bb} \subseteq_* s$, then by Lemma 27 we have the following $\mathtt{bb} * x * \mathtt{ba} * y * \mathtt{bb} \subseteq_* r$, $\mathtt{bb} * x * \mathtt{ba} * y * \mathtt{bb} \subseteq_* \mathtt{bb} * u * \mathtt{ba} * v$ or there exist w and w' such that $w \subseteq_{\mathsf{end}} r \wedge w' \subseteq_{\mathsf{ini}} \mathtt{bb} * u * \mathtt{ba} * v \wedge \mathtt{bb} * x * \mathtt{ba} * y * \mathtt{bb} = w * w'$.
In case $\mathtt{bb} * x * \mathtt{ba} * y * \mathtt{bb} \subseteq_* r$, then we have that $x[r]y$ since $\mathsf{tally}(x)$, $\mathsf{tally}(y)$ and $\mathtt{bb} * x * \mathtt{ba} * y * \mathtt{bb} \subseteq_* r$.
In case $\mathtt{bb} * x * \mathtt{ba} * y * \mathtt{bb} \subseteq_* \mathtt{bb} * u * \mathtt{ba} * v$, then we have a contradiction since $\mathtt{bb} \subseteq_{\mathsf{end}} v$ implies that $\mathtt{b} \subseteq_* v$, but $\mathsf{tally}(v)$ implies that $\neg \mathtt{b} \subseteq_* v$.
In case there exists w and w' such that $w \subseteq_{\mathsf{end}} r \wedge w' \subseteq_{\mathsf{ini}} \mathtt{bb} * u * \mathtt{ba} * v \wedge \mathtt{bb} * x * \mathtt{ba} * y * \mathtt{bb} = w * w'$, then by (tc4), Lemma 27 and (tc2) we have that $w' = \Box \vee w' = \mathtt{b} \vee w' = \mathtt{bb}$ since $\mathsf{tally}(v)$, $\mathsf{tally}(y)$ and $\mathtt{bb} \subseteq_{\mathsf{end}} \mathtt{bb} * x * \mathtt{ba} * y * \mathtt{bb}$. If $w' = \Box$, then $x[r]y$ since $\mathtt{bb} * x * \mathtt{ba} * y * \mathtt{bb} \subseteq_* r$. If $w' = \mathtt{b}$, then $\mathtt{bb} * x * \mathtt{ba} * y * \mathtt{b} \subseteq_{\mathsf{end}} r$ and hence, $x[r]y$. Finally, if $w' = \mathtt{bb}$, then $\mathtt{bb} * x * \mathtt{ba} * y \subseteq_{\mathsf{end}} r$ so that $x[r]y$.

Hence, we have that $\mathsf{tally}(u) \wedge \mathsf{tally}(v) \wedge (x[r]y \vee (x = u \wedge y = v))$.

For the other direction of the biconditional, suppose $\mathsf{tally}(u) \wedge \mathsf{tally}(v) \wedge (x[r]y \vee (x = u \wedge y = v))$. We want to show that $x[s]y \wedge \mathsf{tally}(u) \wedge \mathsf{tally}(v)$.

If $x[r]y$ – that is, x and y are tallies and:

$$\mathtt{bb} * x * \mathtt{ba} * y \subseteq_{\mathsf{end}} r \vee \mathtt{bb} * x * \mathtt{ba} * y * \mathtt{b} \subseteq_{\mathsf{end}} r \vee \mathtt{bb} * x * \mathtt{ba} * y * \mathtt{bb} \subseteq_* r,$$

then we obviously have that:

$$\mathtt{bb} * x * \mathtt{ba} * y \subseteq_{\mathsf{end}} s \vee \mathtt{bb} * x * \mathtt{ba} * y * \mathtt{b} \subseteq_{\mathsf{end}} s \vee \mathtt{bb} * x * \mathtt{ba} * y * \mathtt{bb} \subseteq_* s$$

since $s := r * (\mathtt{bb} * u * \mathtt{ba} * v)$. Thus, we have that $x[s]y$.

If $x = u \wedge y = v$, then $x[s]y$ since $\mathsf{bb} * x * \mathsf{ba} * y \subseteq_{\mathsf{end}} s$ by the way we defined s.

Hence, we conclude that $x[s]y \wedge \mathsf{tally}(u) \wedge \mathsf{tally}(v)$.

□

Lemma 29 (in $\mathsf{TC}_{I\Delta_0}$). *$\odot$ is functional — i.e., the following is provable:*

$$x \odot y = z \wedge x \odot y = w \to z = w.$$

Proof. Suppose $x \odot y = z$ and $x \odot y = w$. Then by the definition of $\odot$, we have that there exists r and s respectively such that $\mathsf{multrel}(r,x) \wedge y[r]z$ and $\mathsf{multrel}(s,x) \wedge y[s]w$.

We show by bounded induction on $u \subseteq_* y$ that $\forall v, v'((u[r]v \wedge u[s]v') \to v = v')$ since then, in particular, we have that $z = w$.

Suppose that $u = \square$ and let v and v' be arbitrary. Suppose further that $\square[r]v$ and $\square[s]v'$. Then since $\mathsf{multrel}(r,x)$ and $\mathsf{multrel}(s,x)$, we have respectively that:

$$v = \square \vee \exists u_0, v_0(u_0[r]v_0 \wedge \square = u_0 * \mathsf{a} \wedge v = v_0 * x) \text{ and,}$$

$$v' = \square \vee \exists u_0', v_0'(u_0'[s]v_0' \wedge \square = u_0' * \mathsf{a} \wedge v' = v_0' * x).$$

If $\exists u_0, v_0(u_0[r]v_0 \wedge \square = u_0 * \mathsf{a} \wedge v = v_0 * x)$ or $\exists u_0', v_0'(u_0'[s]v_0' \wedge \square = u_0' * \mathsf{a} \wedge v' = v_0' * x)$ is the case, then we have a contradiction by $(\mathsf{tc1})$. Hence, we have that $v = \square = v'$ as desired.

Assume as inductive hypothesis that $\forall v, v'((u[r]v \wedge u[s]v') \to v = v')$. We prove that $\forall v, v'((\mathsf{S_a}u[r]v \wedge \mathsf{S_a}u[s]v') \to v = v')$

Let v and v' be arbitrary and suppose that $\mathsf{S_a}u[r]v$ and $\mathsf{S_a}u[s]v'$. Then since $\mathsf{S_a}u \neq \square$ by $(\mathsf{tc1})$ and since $\mathsf{multrel}(r,x)$ and $\mathsf{multrel}(s,x)$, we have respectively that:

$$\exists u_0, v_0(u_0[r]v_0 \wedge \mathsf{S_a}u = u_0 * \mathsf{a} \wedge v = v_0 * x) \text{ and,}$$

$$\exists u_0', v_0'(u_0'[s]v_0' \wedge \mathsf{S_a}u = u_0' * \mathsf{a} \wedge v' = v_0' * x).$$

Thus, since $u_0 = u_0' = u$, we have that $u[r]v_0 * x$ and $u[s]v_0' * x$. Finally, by our inductive hypothesis, this implies that $v = v_0 * x = v_0' * x = v'$ as desired.

This completes our induction, so we have that $z = w$ since $y \subseteq_* y$, $y[r]z$ and $y[s]w$.

□

Proposition 30 (in $\mathsf{TC}_{I\Delta_0}$). *(m.1) $(x \odot \square = z \vee \square \odot y = z) \leftrightarrow z = \square$;*
(m.2) $x \odot \mathsf{S_a}y = z \leftrightarrow \exists v(x \odot y = v \wedge z = v * x)$.

Proof. Ad (m.1). Suppose $x \odot \square = z$. By the definition of $\odot$, we have that there exists a u such that:

$$\mathsf{multrel}(u,x) \wedge \square[u]z.$$

Moreover, by the definition of $\mathsf{multrel}(u,x)$, we have that $\square[u]\square$. Hence, we have that $\square[u]z$ and $\square[u]\square$. As a particular instance of the induction carried out in Lemma 29, we have that

$(\Box[u]z \wedge \Box[u]\Box) \to z = \Box$. Thus, we conclude that $z = \Box$.

Suppose $\Box \odot y = z$. By the definition of $\odot$, we have that there exists a u such that:

$$\mathsf{multrel}(u, \Box) \wedge y[u]z.$$

Moreover, by the definition of $\mathsf{multrel}(u, \Box)$, we have that:

$$\begin{aligned}&\mathsf{tally}(\Box) \wedge \Box[u]\Box \wedge \\ &\forall s,t\ (s[u]t \to ((s = \Box \wedge t = \Box) \vee \exists s',t'\ (s'[u]t' \wedge s = s' * \mathsf{a} \wedge t = t' * \Box))).\end{aligned}$$

We show by induction on s that $\forall t\ (s[u]t \to t = \Box)$. Suppose $s = \Box$ and $s[u]t$, then since $\mathsf{multrel}(u, \Box)$ we have that $s = \Box \wedge t = \Box$ or $\exists s',t'\ (s'[u]t' \wedge s = s' * \mathsf{a} \wedge t = t' * \Box)$. In case $s = \Box \wedge t = \Box$, then $t = \Box$. In case $\exists s',t'\ (s'[u]t' \wedge s = s' * \mathsf{a} \wedge t = t' * \Box)$, we have that there exists a s' such that $\Box = s' * \mathsf{a}$. But this is a contradiction by (tc1). Hence, $t = \Box$.
Assume as inductive hypothesis that $\forall t\ (s[u]t \to t = \Box)$.
Ad $\mathsf{S_a}s$. Suppose that $\mathsf{S_a}s[u]t$ where t is arbitrary. Then we have that $\mathsf{S_a}s = \Box \wedge t = \Box$ or $\exists s',t'\ (s'[u]t' \wedge \mathsf{S_a}s = s' * \mathsf{a} \wedge t = t' * \Box)$. In case $\mathsf{S_a}s = \Box \wedge t = \Box$, we have a contradiction by (tc1). In case $\exists s',t'\ (s'[u]t' \wedge \mathsf{S_a}s = s' * \mathsf{a} \wedge t = t' * \Box)$, we have that $s[u]t$ since $s'[u]t'$, $s' = s$ and $t = t'$. Hence, by the inductive hypothesis we have that $t = \Box$.
Ad $\mathsf{S_b}s$. Suppose that $\mathsf{S_b}s[u]t$ where t is arbitrary. Then we have a contradiction. Hence, $\forall t\ (\mathsf{S_b}s[u]t \to t = \Box)$ holds trivially since the antecedent is always false.
Therefore, we conclude that for any $s[u]t$ in $\mathsf{multrel}(u, \Box)$, we have that $t = \Box$. Finally, since in particular $x[u]z$, we have that $z = \Box$.

The other direction of the biconditional is trivial and hence, we have that *(m.1)*.

Ad (m.2). Suppose $x \odot \mathsf{S_a}y = z$ — that is:

$$\mathsf{multrel}(u,x) \wedge \mathsf{S_a}y[u]z.$$

We want to show that there exist v and u' such that:

$$\mathsf{multrel}(u',x) \wedge y[u']v$$

where $z = v * x$. Choose $u' := u$. We show that each of the two conjuncts $\mathsf{multrel}(u',x)$ and $y[u']v$ holds in turn.

For $\mathsf{multrel}(u',x)$: We automatically have that $\mathsf{multrel}(u',x)$ since $\mathsf{multrel}(u,x)$.

For $y[u']v$: Since $\mathsf{multrel}(u,x)$ and $\mathsf{S_a}y[u]z$, we have that there exists s,t such that $s[u]t \wedge \mathsf{S_a}y = s * \mathsf{a} \wedge z = t * x$. Hence, since $y = s$ and $v = t$, we have that $y[u]v$. Thus, we conclude that $y[u']v$.

Now, suppose $\exists v(x \odot y = v \wedge z = v * x)$ — that is, $z = v * x$ and moreover, there exists a u' such that:

$$\mathsf{multrel}(u',x) \wedge y[u']v.$$

We want to show that $x \odot \mathsf{S_a}y = z$ — that is, there exists a u such that:

$$\mathsf{multrel}(u,x) \wedge \mathsf{S_a}y[u]z.$$

Choose $u := u' * (\texttt{bb} * \mathsf{S}_{\mathsf{a}}y * \texttt{ba} * z)$. We show that each of the two conjuncts $\mathsf{multrel}(u,x)$ and $\mathsf{S}_{\mathsf{a}}y[u]z$ holds in turn.

For $\mathsf{multrel}(u,x)$: We must show that (i) $\mathsf{tally}(x)$, (ii) $\square[u]\square$ and:

$$\text{(iii) } \forall s,t\ (s[u]t \to ((s = \square \wedge t = \square) \vee \exists s',t'\ (s'[u]t' \wedge s = s' * \mathsf{a} \wedge t = t' * x))).$$

We demonstrate each in turn.

(i) $\mathsf{tally}(x)$ since $\mathsf{multrel}(u',x)$.

(ii) $\square[u]\square$ since $\square[u']\square$.

(iii) Suppose $s[u]t$, then we have that $s[u']t$ or $\texttt{bb} * s * \texttt{ba} * t = \texttt{bb} * \mathsf{S}_{\mathsf{a}}y * \texttt{ba} * z$ by Lemma 28. In case $s[u']t$, we have that $(s = \square \wedge t = \square) \vee \exists s',t'\ (s'[u']t' \wedge s = s' * \mathsf{a} \wedge t = t' * x)$ since $\mathsf{multrel}(u',x)$. Hence, we conclude that:

$$(s = \square \wedge t = \square) \vee \exists s',t'\ (s'[u]t' \wedge s = s' * \mathsf{a} \wedge t = t' * x).$$

In case $\texttt{bb} * s * \texttt{ba} * t = \texttt{bb} * \mathsf{S}_{\mathsf{a}}y * \texttt{ba} * z$, we have that $\exists s',t'\ (s'[u]t' \wedge \mathsf{S}_{\mathsf{a}}y = s' * \mathsf{a} \wedge z = t' * x)$ — namely, $s' = y$ and $t' = v$ since $y[u']v$ implies that $y[u]v$.

For $\mathsf{S}_{\mathsf{a}}y[u]z$: We have that $\mathsf{S}_{\mathsf{a}}y[u]z$ since $\texttt{bb} * \mathsf{S}_{\mathsf{a}}y * \texttt{ba} * z \subseteq_{\mathsf{end}} u$ by the way we defined u.

□

3.4. TOTALITY OF $\odot$

Notice that our coding of $x \odot y = z$ is not bounded. As a consequence, we cannot use Δ_0^{p}-induction to prove that $\odot$ is total; rather, we will again use the method of shortening cuts. In [13], Svejdar interprets Q in a weak relational variant of Q. The main insight of his proof is how to get the totality of multiplication out of the relational variant via shortening cuts. We use analogous methods here to achieve the totality of $\odot$.

We follow Svejdar [13] in using the following notation $!(x \odot y)$ to indicate that x and y do have a tally product — i.e., $x \odot y$ is defined. Note that if a term is defined, then all of its subterms are.

Let $T := \{x \mid \mathsf{tally}(x)\}$. It is easy to verify that T is closed under $\square, \mathsf{S}_{\mathsf{a}}$ and $*$.

Lemma 31 (in $\mathsf{TC}_{I\Delta_0}$). *Define:*

$$\begin{array}{rcl} B & := & \{x \in T \mid \forall z,u \in T\ !(z \odot x) \wedge \\ & & \forall z,y \in T\ (!(z \odot y) \to z \odot (y * x) = (z \odot y) * (z \odot x))\}. \end{array}$$

Then B is closed under $\square$ and S_{a}.

Proof. Let z be an arbitrary tally, then $z \odot \square = \square$ by Proposition 30 *(m.1)*, so that $!(z \odot \square)$. Moreover, now let z and y be arbitrary tallies and assume $!(z \odot y)$. Then we have that $z \odot (y * \square) = z \odot y = (z \odot y) * \square = (z \odot y) * (z \odot \square)$ by Proposition 30 *(m.1)*, (tc5) and since $!(z \odot y)$. Hence,

$\Box \in B$.

Assume $x \in B$ – that is, $\forall z, u \in T \ !(z \odot x)$ and:

$$\forall z, y \in T \ (!(z \odot y) \to z \odot (y * x) = (z \odot y) * (z \odot x)).$$

We first show that $!(z \odot \mathsf{S_a}x)$ for an arbitrary tally z. We have that $!((z \odot x) * z)$ since $!(z \odot x)$. Now, by Proposition 30 *(m.2)*, we have that $(z \odot x) * z = z \odot \mathsf{S_a}x$, so that $!(z \odot \mathsf{S_a}x)$. Second, we show that $!(z \odot y) \to z \odot (y * \mathsf{S_a}x) = (z \odot y) * (z \odot \mathsf{S_a}x)$ for arbitrary tallies y and z. Assume $!(z \odot y)$. By $(\mathsf{tc6})$, Proposition 30 *(m.2)*, our initial assumption and (Assoc_*), it follows that:

$$\begin{aligned} z \odot (y * \mathsf{S_a}x) &= z \odot \mathsf{S_a}(y * x) \\ &= (z \odot (y * x)) * z \\ &= ((z \odot y) * (z \odot x)) * z \\ &= (z \odot y) * ((z \odot x) * z) \\ &= (z \odot y) * (z \odot \mathsf{S_a}x) \end{aligned}$$

So we have that $\mathsf{S_a}x$ satisfies both conditions in the definition of B and thus, we conclude that $\mathsf{S_a}x \in B$.

□

Lemma 32 (in $\mathsf{TC}_{I\Delta_0}$). *Define*

$$C \ := \ \{x \in B \mid \forall y, z \in B((z \odot y) \odot x = z \odot (y \odot x))\}.$$

Then C is closed under $\Box$ and $\mathsf{S_a}$.

Proof. Since $y \in B$, we have that $!(z \odot y)$ and hence, $(z \odot y) \odot \Box = \Box = z \odot \Box = z \odot (y \odot \Box)$ by Proposition 30 *(m.1)*. Thus, $\Box \in C$.

Assume that $y, z \in B$ and that $x \in C$. Then by Proposition 30 *(m.2)*, the fact that $x \in C$ and $y \in B$, and (Assoc_*), we have the following:

$$\begin{aligned} (z \odot y) \odot \mathsf{S_a}x &= ((z \odot y) \odot x) * (z \odot y) \\ &= (z \odot (y \odot x)) * (z \odot y) \\ &= z \odot ((y \odot x) * y) \\ &= z \odot (y \odot \mathsf{S_a}x) \end{aligned}$$

Moreover, note that since y satisfies the first condition in the definition of B, we have $!(((z \odot y) \odot x) * (z \odot y))$ and $!((z \odot (y \odot x) * (z \odot y))$. Thus, $\mathsf{S_a}x \in C$. □

Lemma 33 (in $\mathsf{TC}_{I\Delta_0}$). *Define*

$$K \ := \ \{x \in T \mid \forall u \in T \forall v \in C(u * v = x \to u \in C)\}.$$

Then K is closed under $\Box$ and $\mathsf{S_a}$, and K is progressive.

Proof. Note that $K \subseteq C$: Assume $x \in K$, then by $(\mathsf{tc5})$ we have that $x * \square = x$ so that $x \in C$.

Assume $u * v = \square$ and $v \in C$. By $(\mathsf{tc4})$, we have that $u = \square \vee \exists y(u = \mathsf{S_a}y \vee u = \mathsf{S_b}y)$. If $u = \square$, then $u \in C$ by $(\mathsf{tc5})$. If $u = \mathsf{S_a}y$ for some y, then we have that $\mathsf{S_a}y * v = \mathsf{S_a}(y * v) = \square$ since $\forall y(\mathsf{S_a}y * v = \mathsf{S_a}(y * v))$ is provable using Δ_0^{p}-induction. But this is a contradiction since $\mathsf{S_a}(y * v) \neq \square$ by $(\mathsf{tc1})$. If $u = \mathsf{S_b}y$ for some y, then we also have a contradiction since $u \in T$. Thus, $\square \in K$.

Now, assume $x \in K$ and let $u \in T$ and $v \in C$ be such that $u * v = \mathsf{S_a}x$. Again, by $(\mathsf{tc4})$, we have that $u = \square \vee \exists y(u = \mathsf{S_a}y \vee u = \mathsf{S_b}y)$. If $u = \square$, then $u \in C$ by $(\mathsf{tc5})$. If $u = \mathsf{S_a}y$ for some y, then we have that $\mathsf{S_a}y * v = \mathsf{S_a}(y * v) = \mathsf{S_a}x$ since $\forall y(\mathsf{S_a}y * v = \mathsf{S_a}(y * v))$ is provable using Δ_0^{p}-induction. So, by $(\mathsf{tc3})$, $y * v = x$ and we have that $y \in C$ since $x \in K$. Since C is closed under $\mathsf{S_a}$, we conclude that $\mathsf{S_a}y \in C$ and hence, $\mathsf{S_a}x \in K$.

Assume $\mathsf{S_a}x \in K$ and let u, v be such that $v \in C$ and $u * v = x$. Then $u * \mathsf{S_a}v = \mathsf{S_a}x$ and $\mathsf{S_a}v \in C$, so that $\mathsf{S_a}x \in K$ which yields $u \in C$. Thus, $x \in K$.

□

Lemma 34 (in $\mathsf{TC}_{I\Delta_0}$). *Define*

$$I \quad := \quad \{x \in T \mid \forall y(y \in K \leftrightarrow y + x \in K)\}.$$

Then I is closed under $\square, \mathsf{S_a}$ and $*$.

Proof. Note that $I \subseteq K$: Let $x \in I$ and choose $y := \square$ so that $\square * x \in K$. From this and $\square * x = x$, it follows that $x \in K$.

$\square \in I$ by $(\mathsf{tc5})$ and $(\mathsf{tc6})$.

Assume $x \in I$. We want to show that $\forall y(y \in K \leftrightarrow y * \mathsf{S_a}x \in K)$.
For the $\rightarrow$ direction of the biconditional: Suppose $y \in K$, then $y * x \in K$ since $x \in I$. Moreover, since K is closed under $\mathsf{S_a}$ and by $(\mathsf{tc6})$, we have that $\mathsf{S_a}(y * x) = y * \mathsf{S_a}x \in K$.
For the $\leftarrow$ direction of the biconditional: Suppose $y * \mathsf{S_a}x \in K$, then by $(\mathsf{tc6})$ we have that $y * \mathsf{S_a}x = \mathsf{S_a}(y * x)$. Since K is progressive (cf. the last lemma), we have that $y * x \in K$ and thus, $y \in K$ since $x \in I$.

Assume $x_1, x_2 \in I$. We want to show that $x_1 * x_2 \in I$ – that is:

$$\forall z(z \in K \leftrightarrow z * (x_1 * x_2) \in K).$$

For the $\rightarrow$ direction of the biconditional: Assume $z \in K$, then $x_1 \in I$ yields $z * x_1 \in I$, and this together with $x_2 \in I$ yields $(z * x_1) * x_2 \in K$. Now since $(z * x_1) * x_2 = z * (x_1 * x_2)$, we have that $z * (x_1 * x_2) \in K$.
For the $\leftarrow$ direction of the biconditional: Assume $z * (x_1 * x_2) \in K$, then this together with $x_2 \in I$ yields $z * x_1 \in K$, and this together with $x_1 \in I$ yields $z \in K$. Thus, $x_1 * x_2 \in I$.

□

Lemma 35 (in $\mathsf{TC}_{I\Delta_0}$). *Define*

$$J \quad := \quad \{x \in T \mid \mathsf{a} \odot x = x \wedge \forall y \in I(y \odot x \in I)\}.$$

Then J is closed under $\square, \mathsf{S_a}, *$ and $\odot$, and J is progressive.

Proof. Note that $J \subseteq I$: Assume $x \in J$, then $\forall y \in I(y \odot x \in I)$. Choose $y := \mathtt{a}$ so that $\mathtt{a} \odot x = x \in I$ since $\mathtt{a} \odot x = x$.

$\square \in J$ since $\mathtt{a} \odot \square = \square$ and $y \odot \square = \square \in I$ by Proposition 30 *(m.1)*.

Suppose $x \in J$. Then $\mathtt{a} \odot \mathsf{S}_{\mathtt{a}} x = \mathsf{S}_{\mathtt{a}} x$ follows from $\mathtt{a} \odot x = x$ and Proposition 30 *(m.2)*. Moreover, if $y \in I$, then we have that $y \odot x \in I$ so that $!((y \odot x) * x)$. Since $y \odot \mathsf{S}_{\mathtt{a}} x = (y \odot x) * x$ by Proposition 30 *(m.2)* and I is closed under addition, we have that $y \odot \mathsf{S}_{\mathtt{a}} x \in I$. Thus, $\mathsf{S}_{\mathtt{a}} x \in J$.

Suppose $x_1, x_2 \in J$. Since $!(\mathtt{a} \odot x_1)$ and $x_2 \in B$, we have that:

$$\mathtt{a} \odot (x_1 * x_2) = (\mathtt{a} \odot x_1) * (\mathtt{a} \odot x_2) = x_1 * x_2.$$

Moreover, if $y \in I$, then since $!(y \odot x_1)$, $x_2 \in B$ and I is closed under addition, we have that $(y \odot x_1) * (y \odot x_2) = y \odot (x_1 * x_2) \in I$. Thus, $x_1 * x_2 \in J$.

Suppose $x_1, x_2 \in J$. Then $\mathtt{a} \odot (x_1 \odot x_2) = x_1 \odot x_2$ since $x_2 \in C$. Let $y \in I$. From $x_1 \in J$ and $y \in I$, we have that $y \odot x_1 \in I$, and moreover from this and $x_2 \in J$, we have $(y \odot x_1) \odot x_2 \in I$. Finally, since $x_2 \in C$, this yields $y \odot (x_1 \odot x_2) \in I$. Thus, $x_1 \odot x_2 \in J$.

Assume $\mathsf{S}_{\mathtt{a}} x \in J$. From $J \subseteq K$ and the fact that K is progressive, we have that $x \in K \subseteq B$, so $!(\mathtt{a} \odot x)$ and hence, $\mathtt{a} \odot \mathsf{S}_{\mathtt{a}} x = (\mathtt{a} \odot x) * \mathtt{a}$. Then from $\mathtt{a} \odot \mathsf{S}_{\mathtt{a}} x = \mathsf{S}_{\mathtt{a}} x$ we have $\mathtt{a} \odot x = x$. Assume $y \in I$. Similarly, from $x \in K \subseteq B$, we have that $!(y \odot x)$, and from (Assoc_*) and Proposition 30 *(m.2)*, we have that $(y \odot x) * y = y * \mathsf{S}_{\mathtt{a}} x \in I$. Finally, from the fact that $\forall x_1, x_2 (x_1 * x_2 \in I \rightarrow (x_1 \in I \wedge x_2 \in I))$ (cf. the last lemma), we obtain in particular that $y \odot x \in I$. Thus, $x \in J$.

□

3.5. TC_{Q} INTERPRETS Q

Finally, we conclude this section by demonstrating our main result.

Theorem 36. TC_{Q} *interprets* Q.

Proof. It suffices to show that $\mathsf{TC}_{I\Delta_0}$ interprets Q since we have that TC_{Q} interprets $\mathsf{TC}_{I\Delta_0}$ by Theorem 26.

We translate the signature of Q into the signature of $\mathsf{TC}_{I\Delta_0}$ via the relative translation $\tau : \{\overline{0}, \mathsf{S}, +, \cdot\} \rightarrow \{\square, \mathsf{S}_{\mathtt{a}}, \mathsf{S}_{\mathtt{b}}, *\}$.

$$\begin{aligned}
(\overline{0})^{\tau} &:= \square \\
(\mathsf{S}x)^{\tau} &:= \mathsf{S}_{\mathtt{a}} x \\
(x + y)^{\tau} &:= x * y \\
(x \cdot y)^{\tau} &:= x \odot y.
\end{aligned}$$

Let J be as defined in Lemma 35. Then J is closed under $\square, \mathsf{S}_{\mathtt{a}}, *$ and $\odot$, and so J is an appropriate domain of interpretation.

Next, we check that the translation of the nonlogical axioms of Q are valid in $\mathsf{TC}_{I\Delta_0}$:

(q1): $\mathsf{TC}_{I\Delta_0} \vdash (J(x) \wedge J(y)) \to (\mathsf{q1})^\tau$ by (tc3).

(q2): $\mathsf{TC}_{I\Delta_0} \vdash J(x) \to (\mathsf{q2})^\tau$ by (tc1).

(q3): $\mathsf{TC}_{I\Delta_0} \vdash J(x) \to (\mathsf{q3})^\tau$ by (tc4).

(q4): $\mathsf{TC}_{I\Delta_0} \vdash (J(x) \wedge J(y)) \to (\mathsf{q4})^\tau$ by (tc5).

(q5): $\mathsf{TC}_{I\Delta_0} \vdash (J(x) \wedge J(y)) \to (\mathsf{q5})^\tau$ by (tc6).

(q6): $\mathsf{TC}_{I\Delta_0} \vdash (J(x) \wedge J(y)) \to (\mathsf{q6})^\tau$ by Proposition 30 *(m.1)* and Lemma 35.

(q7): $\mathsf{TC}_{I\Delta_0} \vdash (J(x) \wedge J(y)) \to (\mathsf{q7})^\tau$ by Proposition 30 *(m.2)* and Lemma 35.

(q8): $\mathsf{TC}_{I\Delta_0} \vdash (J(x) \wedge J(y)) \to (\mathsf{q8})^\tau$ since J is downwards closed under $\subseteq_*$.

Thus, J and τ determine an interpretation of Q in $\mathsf{TC}_{I\Delta_0}$ and hence, in TC_{Q}.

□

4. Conclusion

This thesis has two main results: The first is a revised axiomatization of Q in light of considerations about the decidability of identity and equality with zero in the intuitionistic case and a constructive proof of Nelson's classic result that Q interprets $I\Delta_0 + \Omega_1$. The second result of this thesis is a proof that a basic theory of concatenation based on Q, TC_{Q}, interprets Q. This result provides a weak axiomatic theory different from Q, but which yields the same metamathematical benefits since it has what we called *local coding*. In this sense, the result contributes to both Grzegorczyk's programme and Visser's programme. In [17], Visser uses the latter result to show that Grzegorczyk's theory TC with the empty string $\square$ added, is mutually interpretable with Q, which strengthens Grzegorczyk and Zdanowski's result in [6] that TC is essentially undecidable.

BIBLIOGRAPHY

1. J. Burgess. *Fixing Frege*. Princeton University Press, 2005.
2. S. Buss. *Bounded Arithmetic*. Bibliopolis, Napoli, 1986.
3. S. Buss. Nelson's work on logic and foundations and other reflection on foundations of mathematics. *Diffusion, Quantum Theory, and Radically Elementary Mathematics*, pages 183–208, 2006.
4. G.F. Collins and Halpern J.D. On the interpretability of arithmetic in set theory. *The Notre Dame Journal of Formal Logic*, 11:477–483, 1970.
5. A. Grzegorczyk. Undecidability without arithmetization. *Studia Logica*, 79:163–230, 2005.
6. A. Grzegorczyk and K. Zdanowski. Undecidability and concatenation. *forthcoming*, 2008.
7. P. Hájek and P. Pudlák. *Metamathematics of First-Order Arithmetic*. Perspectives in Mathematical Logic. Springer, Berlin, 1991.
8. F. Montagna and A. Mancini. A minimal predicative set theory. *Notre Dame Journal of Formal Logic*, 35:186–203, 1994.
9. P. Pudlák Mycielski, P. and A.S. Stern. A lattice of chapters of mathematics (interpretations between theorems. *Memoirs of the American Mathematical Society*, 426, 1990.
10. E. Nelson. *Predicative arithmetic*. Princeton University Press, Princeton, 1986.
11. P. Pudlák. Some prime elements in the lattice of interpretability types. *Transactions of the American Mathematical Association*, 280:255–75, 1983.
12. W.V. Quine. Concatenation as a basis for arithmetic. *Journal of Symbolic Logic*, 11:105–114, 1946.
13. V. Svejdar. An interpretation of robinson arithmetic in its grzegorczyk's weaker variant. *forthcoming*, 2007.
14. W. Szmielew and A. Tarski. Mutual interpretability of some essentially undecidable theories. *Proceedings of the International Congress of Mathematicians*, 1:734, 1950.
15. A. Mostowski Tarski, A. and R. Robinson. *Undecidable Theories*. North Holland, 1953.
16. A. Visser. Faith and falsity: A study of faithful interpretations and false σ^0_1-sentences. *forthcoming*, 2007.
17. A. Visser. Growing commas: A study of sequentiality and concatenation. *forthcoming*, 2007.
18. A. Visser. Pairs, sets and sequences in first order theories. *forthcoming*, 2007.
19. A. Visser. Cardinal arithmetic in weak theories. *forthcoming*, 2008.