An Interpretation of Robinson Arithmetic in its Grzegorczyk's Weaker Variant

Vítězslav Švejdar[*][†]

Jan 2, 2007

The original publication is available at Fundamenta Informaticae.

Abstract

Q^- is a weaker variant of Robinson arithmetic Q in which addition and multiplication are partial functions, i.e. ternary relations that are graphs of possibly non-total functions. We show that Q is interpretable in Q^-. This gives an alternative answer to a question of A. Grzegorczyk whether Q^- is essentially undecidable.

1 Introduction

Robinson arithmetic Q was introduced by Rafael Robinson at the 1950 International Congress on Mathematics as an axiomatic theory formulated in the language $\{0, \mathrm{S}, +, \cdot\}$ with a constant, a unary function symbol and two binary function symbols. Its axiomatization consists of three axioms stipulating that the successor symbol S represents a function that is one-one and with a range containing all numbers except the number 0 (zero), and there are four other axioms about addition $+$ and multiplication $\cdot$ saying that $x + 0 = x$, that $x \cdot 0 = 0$, and that the sum $x + \mathrm{S}(y)$ and the product $x \cdot \mathrm{S}(y)$ is naturally connected to and uniquely determined by the sum $x + y$ and the product $x \cdot y$ respectively, see below. It is usually the book [8] by Tarski, Mostowski, and Robinson that is now quoted as the canonical source containing the presentation of Robinson arithmetic. *Peano arithmetic* PA is an extension of Q formulated in the same language; it is obtained by adding the induction schema to the seven axioms of Q. Nowadays it is more convenient to enrich the language of Robinson (and

[*]This work is a part of the research plan MSM 0021620839 that is financed by the Ministry of Education of the Czech Republic.

[†]Charles University, Prague, vitezslavdotsvejdaratcunidotcz, http://www1.cuni.cz/~svejdar/. Palachovo nám. 2, 116 38 Praha 1, Czech Republic.

Peano) arithmetic by adding one or both of the symbols $\leq$ and $<$ for unstrict and strict ordering, and by adding some straightforward axioms about these symbols, see e.g. [4]. Since these extensions are merely definitional extensions of the original theory of Rafael Robinson, they are still called Robinson arithmetic and denoted Q. The presence of one or both of the symbols $\leq$ and $<$ makes it easy to formulate the definition of bounded (i.e., Δ_0) formula and to define fragments of PA like $\mathrm{I}\Delta_0$, where the induction schema is restricted to bounded formulas only, see [6], or [4] again.

Besides finite axiomatizability, an important property of Robinson arithmetic Q is its *essential undecidability*: each consistent extension of Q is undecidable. Recall that a theory S is an extension of a theory T if the language of T is a subset of the language of S and if all theorems of T are provable in S. The essential undecidability of Q is especially interesting in conjunction with the fact that Q is a weak theory: even the most basic properties of $+$ and $\cdot$ like commutativity and associativity are unprovable in Q. Another important feature of Robinson arithmetic is its capability to *interpret theories.* Hájek and Pudlák [4] show a proof that $\mathrm{I}\Delta_0$, and even some extensions of $\mathrm{I}\Delta_0$, are interpretable in Q, in the sense defined in [8] and mentioned below in some more details. The method used in [4] for constructing an interpretation in Q is called *shortening of cuts* and was invented by R. Solovay in the unpublished [7]. Note however that the most technical part of the proof that Q interprets $\mathrm{I}\Delta_0$ is omitted in [4], and the reader is referred to [5].

In connection with the project to base the explanation of incompleteness and undecidability phenomena on axiomatic systems different from PA or Q, Andrzej Grzegorczyk asked the following question. Let the function symbols $+$ and $\cdot$ in the language of Robinson arithmetic be replaced by ternary predicate symbols A and M, and let Q^- be a theory obtained from Q by replacing the axioms about $+$ and $\cdot$ by axioms saying that A and M represent graphs of binary functions that may be *non-total* but do satisfy a natural reformulation of the corresponding axioms of Q. So Q^-, if enhanced by axioms asserting totality of operations, would be almost the same as Q except that nesting of terms would be restricted. Now Grzegorczyk's question reads: is Q^- essentially undecidable?

Petr Hájek presented Grzegorczyk's question at the Prague-Vienna Workshop on Proof Theory and Proof Complexity in January 2006. He answered the question positively by elaborating the Σ-completeness and self-reference theorems for the theory Q^-, and he then also generalized the result for the case that the underlying logic is not the classical one, but a weak fuzzy logic, see [3]. After listening to P. Hájek's talk about Grzegorczyk's question, several people (J. Krajíček, J. Joosten, and the present author) conjectured that Q was interpretable in Q^-. Note that this represents an alternative approach to the question about essential undecidability of Q^-, because interpretability of an essentially undecidable theory T in a theory S entails essential undecidability of S (see [8]).

Later it appeared that what Petr Hájek worked on was in fact his reasonable interpretation of Grzegorczyk's question: the "real" Grzegorczyk's theory Q^- is *weaker* than the theory from P. Hájek's talk at the Prague-Vienna Workshop.

In this paper we show that Robinson arithmetic Q is interpretable in the theory Q^-, and it is the case even if Q^- has the meaning defined by A. Grzegorczyk. We also mention some connections and outline the Solovay's method of shortening of cuts.

It should be remarked that there exists a yet another way how to answer a question about an essential incompleteness and undecidability of a theory, namely use of Gödel Second Incompleteness Theorem. D. Willard in [9] mentions another Solovay's unpublished theorem saying that the Second Incompleteness Theorem is true for all reasonable extensions of Q even if addition and multiplication are non-total; hence in our setting, is true for all reasonable extensions of Q^-. Note that Willard's papers, e.g. [9, 10], yield both positive and negative results about validity of the Second Incompleteness Theorem in the situations where the axiomatic theory is very weak, some or all of its functions are non-total and the proof system varies.

2 Preliminaries

Before constructing an interpretation of Q in Q^- we state the definition of the theory Q^- and we also make the notion of interpretability more precise.

The language of the *theory* Q^- is $\{0, \mathrm{S}, \mathrm{A}, \mathrm{M}, \leq\}$ where 0 is a constant, S is a unary function, A and M are ternary relations, and $\leq$ is a binary predicate. The axioms of Q^- are the following:

A: $\forall x \forall y \forall z_1 \forall z_2 (\mathrm{A}(x,y,z_1)\ \&\ \mathrm{A}(x,y,z_2) \rightarrow z_1 = z_2)$,

M: $\forall x \forall y \forall z_1 \forall z_2 (\mathrm{M}(x,y,z_1)\ \&\ \mathrm{M}(x,y,z_2) \rightarrow z_1 = z_2)$,

Q1: $\forall x \forall y (\mathrm{S}(x) = \mathrm{S}(y) \rightarrow x = y)$,

Q2: $\forall x (\mathrm{S}(x) \neq 0)$,

Q3: $\forall x (x \neq 0 \rightarrow \exists y (x = \mathrm{S}(y)))$,

Q4: $\forall x \mathrm{A}(x, 0, x)$,

G5: $\forall x \forall y \forall z (\exists u (\mathrm{A}(x,y,u)\ \&\ z = \mathrm{S}(u)) \rightarrow \mathrm{A}(x, \mathrm{S}(y), z))$,

Q6: $\forall x \mathrm{M}(x, 0, 0)$,

G7: $\forall x \forall y \forall z (\exists u (\mathrm{M}(x,y,u)\ \&\ \mathrm{A}(u,x,z)) \rightarrow \mathrm{M}(x, \mathrm{S}(y), z))$,

Q8: $\forall x \forall y (x \leq y \equiv \exists z \mathrm{A}(z, x, y))$.

Hájek's variant of Q^- has axioms H5 and H7 instead of G5 and G7, where

H5: $\forall x \forall y \forall z (\exists u (\mathrm{A}(x,y,u)\ \&\ z = \mathrm{S}(u)) \equiv \mathrm{A}(x, \mathrm{S}(y), z))$,

H7: $\forall x \forall y \forall z (\exists u (\mathrm{M}(x,y,u)\ \&\ \mathrm{A}(u,x,z)) \equiv \mathrm{M}(x, \mathrm{S}(y), z))$.

As to omitting parentheses, the connective $\rightarrow$ has lower precedence than $\&$ and $\vee$, but higher than equivalence $\equiv$. The axiom G5 can also be written as $\forall x\forall y\forall u(\mathrm{A}(x,y,u)\rightarrow\mathrm{A}(x,\mathrm{S}(x),\mathrm{S}(u))$. The axiom A ensures that for each x and y there exists at most one z which is their sum, i.e. which satisfies $\mathrm{A}(x,y,z)$. We will informally write $x+y$ to denote such a z. We allow to write $x+y$ regardless whether x and y actually have a sum; so $x+y$ can be undefined. We write $!(x+y)$ to indicate that x and y do have a sum, i.e. that $x+y$ exists (is defined). It should however be stressed that this convention does not mean a change in the underlying logic, which is still the classical first-order predicate logic where function symbols denote total functions. The same convention applies to multiplication: $!(x\cdot y)$ says that x and y have a product $x\cdot y$. We allow nesting, i.e. we allow writing *terms* in the language $\{0,\mathrm{S},+,\cdot\}$. If a term t is defined then all its subterms must be defined. For example, if $!(z\cdot y+x)$ then $!(z\cdot y)$. We will also have to be careful when using the *equality symbol* $=$. The meaning of $t=s$, where t and s are terms, is "both t and s exist and are equal". So for example, from $(z+y)+x=u\cdot v$ one can conclude that $(z+y)+x$ is defined (and thus $!(z+y)$) and also $u\cdot v$ is defined. Using these conventions, the axioms Q4, G5, Q6, and G7 can be rewritten as

Q4: $\forall x(x+0=x)$,

G5: $\forall x\forall y(!(x+y)\ \rightarrow\ x+\mathrm{S}(y)=\mathrm{S}(x+y))$,

Q6: $\forall x(x\cdot 0=0)$,

G7: $\forall x\forall y(!(x\cdot y+x)\ \rightarrow\ x\cdot\mathrm{S}(y)=x\cdot y+x)$,

while Hájek's axioms H5 and H7 would be

H5: $\forall x\forall y(!(x+y)\ \vee\ !(x+\mathrm{S}(y))\ \rightarrow\ x+\mathrm{S}(y)=\mathrm{S}(x+y))$,

H7: $\forall x\forall y(!(x\cdot y+x)\ \vee\ !(x\cdot\mathrm{S}(y))\ \rightarrow\ x\cdot\mathrm{S}(y)=x\cdot y+x)$.

To make the exposition complete, the original axioms Q5 and Q7 of Robinson arithmetic are $\forall x\forall y(x+\mathrm{S}(y)=\mathrm{S}(x+y))$ and $\forall x\forall y(x\cdot\mathrm{S}(y)=x\cdot y+x)$ respectively. Observe that axiom G5 implies that if $!(x+y)$ then $!(x+\mathrm{S}(y))$, while H5 implies that $!(x+y)$ iff $!(x+\mathrm{S}(y))$. As to multiplication, none of G7 and H7 guarantees that $!(x\cdot\mathrm{S}(y))$ provided $!(x\cdot y)$. This is because if $!(x\cdot y)$ then the sum $x\cdot y+x$ still may not exist.

A *translation* $*$ *of formulas* of a theory T to formulas of a theory S is determined by a definitional extension S' of the theory S, a translation of symbols, and a domain. A *translation of symbols* is a function $\sharp$ which maps each symbol H in the language of T to a symbol $H^\sharp$ of the same arity and kind (function or predicate) in the language of the definitional extension S'. A *domain* is a formula $\delta(x)$ of S' with one free variable used to relativize quantifiers in the given translation $*$ of formulas: $(\forall x\varphi)^*$ is $\forall x(\delta(x)\rightarrow\varphi^*)$ and $(\exists x\varphi)^*$ is $\exists x(\delta(x)\,\&\,\varphi^*)$.

Logical connectives are preserved by a translation of formulas. A translation $*$ of formulas is an *interpretation of* T *in* S if its domain $\delta(x)$ satisfies

$$S'\vdash\exists x\delta(x)\quad\text{and}\quad S'\vdash\forall x_1\,..\,\forall x_n(\delta(x_1)\,\&\,..\,\&\,\delta(x_n)\rightarrow\delta(F^\sharp(x_1,..,x_n)))$$

for each function symbol F in the language of T (i.e. the domain is provably non-empty and closed under the interpreted functions), and if, moreover, $S'\vdash\varphi^*$ for each axiom φ of T. A theory T is *interpretable in* S if there exists an interpretation of T in S.

So we consider the same interpretations as in [8]; to an expert, they can be described as global one-dimensional non-parametrical interpretations. It is not difficult to check that if $*$ is an interpretation of T in S then, for each theorem φ of T, the sentence φ^* is provable in the definitional extension S' given by the interpretation $*$; also if T is interpretable in S and S is consistent then T is consistent, too.

3 An interpretation of Q in Q^-

We write "1" as a shorthand for $\mathrm{S}(0)$. Instead of interpreting Q as it is, it appears more convenient to interpret somewhat stronger theory than Q. So we prove the following.

Theorem 1 *Robinson arithmetic* Q *enhanced by axioms asserting associativity of both operations, left distributivity, and axioms* $\forall x(0+x=x)$, $\forall x(1\cdot x=x)$, $\forall x\forall y\forall z(y+x=z+x\ \rightarrow\ y=z)$, *is interpretable in the theory* Q^-.

Proof We choose Q^- itself as its definitional extension (see our definition of interpretability above), and we choose an identical mapping as the translation of symbols. So the only non-trivial part of the interpretation we construct is its domain, which we denote $J(x)$. It will be useful to think of J as a "set" of natural numbers, i.e. identify J with the collection $\{\,x\,;\,J(x)\,\}$. Before constructing J, we subsequently define five auxiliary formulas (sets) A, B, C, K, and I. The purpose of A, B, and C is to restrict the universe to numbers having nice properties, while K and I will be closed under certain operations. Finally we will have to verify that addition and multiplication are total on $J\times J$, the set J is closed under both of them, and all axioms of Q as well as the additional axioms listed in our Theorem "are valid in Q^- in the sense of J", i.e. their translations are provable if J is used to relativize quantifiers. Since the symbol $\leq$ is introduced by a definition, we simply ignore it. Put

$$\begin{aligned}A=\{\,x\,;\,&\forall y(\mathrm{S}(y)+x=\mathrm{S}(y+x))\ \&\ \forall y\forall z(y+x=z+x\ \rightarrow\ y=z)\ \&\\ &\&\ \forall y\forall z(!(z+y)\ \rightarrow\ (z+y)+x=z+(y+x))\,\}.\end{aligned}$$

Note that from $\mathrm{S}(y)+x=\mathrm{S}(y+x)$ it follows that $!(y+x)$. So an important property of all elements of A is that they can be added to any number from the right. We claim that A is an *inductive set*, i.e. that $\mathsf{Q}^- \vdash 0 \in A$ and $\mathsf{Q}^- \vdash \forall x(x \in A \to \mathrm{S}(x) \in A)$. Verification of $0 \in A$ is easy. Assume $x \in A$. Let y be given. From $\mathrm{S}(y) + x = \mathrm{S}(y + x)$ we have $!(\mathrm{S}(y) + x)$ and $!(y + x)$. Then axiom G5 yields $\mathrm{S}(y) + \mathrm{S}(x) = \mathrm{S}(\mathrm{S}(y) + x)$ and $\mathrm{S}(y + \mathrm{S}(x)) = \mathrm{S}(\mathrm{S}(y + x))$. So using $\mathrm{S}(y) + x = \mathrm{S}(y + x)$ once again, we obtain $\mathrm{S}(y) + \mathrm{S}(x) = \mathrm{S}(y + \mathrm{S}(x))$. So $\mathrm{S}(x)$ satisfies the first condition in the definition of A. Now let y and z such that $y + \mathrm{S}(x) = z + \mathrm{S}(x)$ be given. From $x \in A$ we know $!(y + x)$ and $!(z + x)$. So axiom G5 is applicable and yields $\mathrm{S}(y+x) = \mathrm{S}(z+x)$. By Q1, $y+x = z+x$. Then from $x \in A$ we have $y = z$. So $\mathrm{S}(x)$ satisfies the second condition in the definition of A. Verification that $\mathrm{S}(x)$ also satisfies the third condition is similar; now from $!(z+y)$ we have $(z+y)+x = z+(y+x)$, and so $!((z+y)+x)$, $!(y+x)$ and $!(z+(y+x))$, and using axiom G5 three times yields $(z+y)+\mathrm{S}(x) = z+(y+\mathrm{S}(x))$. Thus indeed, A is an inductive set. Observe that each pair of elements of A has a sum which, however, may lie outside A. Also observe that each pair x, y of elements of A satisfies $y + \mathrm{S}(x) = \mathrm{S}(y + x)$, i.e. satisfies the equality from axiom Q5, and this is true despite the fact that only the weaker axiom G5 was used to show the properties of A. However, A is not a domain of any interesting interpretation because the axiom Q3 may be not true in the sense of A. Indeed, it is not evident how to show $x \in A$ provided $\mathrm{S}(x) \in A$. Now let

$$B = \{\, x \in A\,;\ \forall z{\in}A \forall u\, !(u + z \cdot x)\ \ \&\ \ \forall z{\in}A \forall y(!(z \cdot y) \to \\ \to z \cdot (y + x) = z \cdot y + z \cdot x) \,\}.$$

It is easy to verify that $0 \in B$. Assume $x \in B$. If $z \in A$ then from the associative property of z and from $!(u + z \cdot x)$ we have $(u + z \cdot x) + z = u + (z \cdot x + z)$. Then axiom G7 yields $!(u + z \cdot \mathrm{S}(x))$. Thus $\mathrm{S}(x)$ satisfies the first condition in the definition of B. For the second condition, assume that $z \in A$ and that $z \cdot (y + x) = z \cdot y + z \cdot x$, consider the equations

$$\begin{aligned} z \cdot (y + \mathrm{S}(x)) &= z \cdot \mathrm{S}(y + x) = z \cdot (y + x) + z, \\ z \cdot y + z \cdot \mathrm{S}(x) &= z \cdot y + (z \cdot x + z) = (z \cdot y + z \cdot x) + z, \end{aligned} \tag{1}$$

and note that they follow from axioms of Q^- and also that the assumption $z \in A$ is used twice: to conclude that $!(z \cdot (y + x) + z)$, and to shift the parentheses in the second line. It follows from (1) that $\mathrm{S}(x)$ satisfies the second condition in the definition of B. So $\mathrm{S}(x) \in B$ and thus B is an inductive set. We now know that associativity of $+$ holds for all elements of B for which it makes sense (since $B \subseteq A$). Also left distributivity holds for all elements of B for which it makes sense. Any two elements of B have both a sum and a product, which however may lie outside B. Now we are able to define the third auxiliary set:

$$C = \{\, x \in B\,;\ \forall y{\in}B \forall z{\in}B((z \cdot y) \cdot x = z \cdot (y \cdot x)) \,\}.$$

From $y \in B$ we have $!(z \cdot y)$ and so $(z \cdot y) \cdot 0 = 0$. Thus $0 \in C$. To show $\forall x(x \in C \to \mathrm{S}(x) \in C)$, assume that $y \in B$ and $z \in B$, assume that $!((z \cdot y) \cdot x)$ and $!(z \cdot (y \cdot x))$, and consider the equations

$$\begin{aligned} (z \cdot y) \cdot \mathrm{S}(x) &= (z \cdot y) \cdot x + z \cdot y, \\ z \cdot (y \cdot \mathrm{S}(x)) &= z \cdot (y \cdot x + y) = z \cdot (y \cdot x) + z \cdot y. \end{aligned} \tag{2}$$

Note that $!((z \cdot y) \cdot x + z \cdot y)$ and $!(z \cdot (y \cdot x) + z \cdot y)$ follow from y satisfying the first condition in the definition of B. Also note that the distributivity rule, used in the second line of (2), is legally used since the right addend in the parenthesis (i.e. y) is in B and the factor to the left of the parenthesis (i.e. z) is in A; the latter is true since $B \subseteq A$. The left addend in the parenthesis, i.e. $y \cdot x$, can be arbitrary. It easily follows from (2) that if $x \in C$ then $\mathrm{S}(x) \in C$. So C is an inductive set which is a subset of B.

The rest is Solovay's method of shortening of cuts with modifications designed to make the method work for the weak theory Q^-. Put

$$\begin{aligned} K &= \{\, x\,;\ \forall u \forall v{\in}C(u + v = x \to u \in C) \,\}, \\ I &= \{\, x\,;\ 0 + x = x\ \ \&\ \ \forall y(y \in K \equiv y + x \in K) \,\}, \\ J &= \{\, x\,;\ 1 \cdot x = x\ \ \&\ \ \forall y{\in}I(y \cdot x \in I) \,\}. \end{aligned}$$

The meaning of $y + x \in K$ is "the sum $y + x$ exists and is an element of K", and similarly for $y \cdot x \in I$. We enumerate and prove a series of properties of K, I, and J.

(i) $K \subseteq C$. This is evident since from $x \in K$ and $x + 0 = x$ we have $x \in C$.

(ii) K is an inductive set. Assume $u + v = 0$ and $v \in C$. If $u = 0$ then $u \in C$. Otherwise $u = \mathrm{S}(z)$ for some z. From $\mathrm{S}(z) + v = 0$ and $v \in C \subseteq A$, and from the first condition in the definition of A we obtain $\mathrm{S}(z + v) = 0$, a contradiction with axiom Q2. Observe that the usual construction, as described e.g. in [4], dictates to take $K = \{\, x\,;\ \forall y{\le}x(y \in C) \,\}$ in this place. If we followed it, we would end up in a serious problem of verifying that $\forall u \forall v(u + v = 0 \to u = 0)$; note that this sentence is easily proved in Hájek's variant of Q^-. Now assume $x \in K$ and let u and v be such that $v \in C$ and $u + v = \mathrm{S}(x)$. Once again, if $u = 0$ then $u \in C$ and we are done. If $u = \mathrm{S}(z)$ then from $v \in C \subseteq A$ we have $\mathrm{S}(z + v) = \mathrm{S}(x)$, so $z + v = x$. From $x \in K$ we have $z \in C$. Since C is inductive, we indeed have $u = \mathrm{S}(z) \in C$.

(iii) $\forall x(\mathrm{S}(x) \in K \to x \in K)$. Assume that $\mathrm{S}(x) \in K$ and let u and v be such that $v \in C$ and $u + v = x$. Then $u + \mathrm{S}(v) = \mathrm{S}(x)$ and $\mathrm{S}(v) \in C$, so $\mathrm{S}(x) \in K$ yields $u \in C$.

(iv) $I \subseteq K$. If $x \in I$ then the choice $y := 0$ yields $0 + x \in K$; from this and from $0 + x = x$ it follows that $x \in K$.

(v) I is inductive. Evidently $0 \in I$. Assume $x \in I$. Then $0 + \mathrm{S}(x) = \mathrm{S}(x)$ is evident. Also the implication $\to$ in $\forall y(y \in K \equiv y + \mathrm{S}(x) \in K)$ easily follows from $x \in I$ and K being inductive. To verify $\leftarrow$, assume $y + \mathrm{S}(x) \in K$.

From $x \in I \subseteq A$ we know $!(y+x)$. Thus $\mathrm{S}(y+x) = y + \mathrm{S}(x) \in K$. Now property (iii) yields $y + x \in K$. So indeed, $y \in K$.

(vi) $\forall x{\in}I\forall y(y \in I \equiv y + x \in I)$. We have to show, for an $x \in I$, that

$$\forall y(y \in I \rightarrow 0 + (y+x) = y + x \ \&\ \forall z(z \in K \equiv z + (y+x) \in K)), \quad (3)$$
$$\forall y(y + x \in I \rightarrow 0 + y = y \ \&\ \forall z(z \in K \equiv z + y \in K)). \quad (4)$$

Assume $y \in I$. Then from $0+y = y$ and $x \in A$ we have $0+(y+x) = y+x$. Let z be given. From $y \in I \subseteq A$ we know $!(z+y)$ and thus $(z+y)+x = z+(y+x)$. If $z \in K$ then $y \in I$ yields $z+y \in K$, and then $x \in I$ yields $z+(y+x) \in K$. On the other hand, $(z+y)+x \in K$ and $x \in I$ yields $z+y \in K$, and this together with $y \in I$ yields $z \in K$. So (3) is true. To verify (4), assume $y+x \in I$. Look at the definition of K: from $y+x \in I \subseteq K$ and $x \in I \subseteq C$ we have $y \in C$. Thus $y \in A$, and $!(z+y)$ for any z. From $!(0+y)$ and $0+(y+x) = (y+x)$, and from x satisfying the third and second condition in the definition of A, we have $0+y = y$. Let z be given. If $z \in K$ then from $z+(y+x) \in K$, the associative property of x and $x \in I$ we have $z+y \in K$. On the other hand, if $z+y \in K$ then from $x \in I$ we have $(z+y)+x \in K$ and $z+(y+x) \in K$, and $y+x \in I$ yields $z \in K$. So (4) is also true. Observe that this property (vi) implies that I is closed under addition.

(vii) $J \subseteq I$. This is obtained similarly as $K \subseteq C$ above, now choosing $y := 1$.

(viii) J is an inductive set. Evidently $0 \in J$. Assume $x \in J$. Then $1\cdot\mathrm{S}(x) = \mathrm{S}(x)$ follows from $1 \cdot x = x$ using axiom G7. Let $y \in I$ be given. From $y \cdot x \in I$ and $y \in I \subseteq A$ we have $!(y \cdot x + y)$, and so $y \cdot \mathrm{S}(x) = y \cdot x + y$. Since I is closed under addition, we have $y \cdot \mathrm{S}(x) \in I$.

(ix) J is closed under addition. Assume $x_1, x_2 \in J$. To show $x_1 + x_2 \in J$, use the distributivity rule to observe that $1 \cdot (x_1 + x_2) = x_1 + x_2$, and use the distributivity rule and the fact that I is closed under addition to observe that $\forall y{\in}I(y \cdot (x_1 + x_2) \in I)$.

(x) J is closed under multiplication. Assume $x_1, x_2 \in J$. Then $1\cdot(x_1\cdot x_2) = x_1\cdot x_2$ is evident. Let $y \in I$ be given. From $x_1 \in J$ and $y \in I$ we have $y \cdot x_1 \in I$, from this and $x_2 \in J$ we have $(y \cdot x_1) \cdot x_2 \in I$, and the associative property of x_2 yields $y \cdot (x_1 \cdot x_2) \in I$.

(xi) $\forall x(\mathrm{S}(x) \in J \rightarrow x \in J)$. Assume $\mathrm{S}(x) \in J$. From $J \subseteq K$ and (iii) we have $x \in K \subseteq B$, so $!(1 \cdot x)$ and hence $1 \cdot \mathrm{S}(x) = 1 \cdot x + 1$. Then from $1 \cdot \mathrm{S}(x) = \mathrm{S}(x)$ we have $1 \cdot x = x$. Assume $y \in I$. Similarly as above, from $x \in K \subseteq B$ we have $!(y \cdot x)$, and from $y \in I \subseteq A$ we have $!(y \cdot x + y)$. So $y \cdot x + y = y \cdot \mathrm{S}(x) \in I$, and from the implication $\leftarrow$ in (vi) we obtain $y \cdot x \in I$.

To summarize, J is closed under all functions of Q, i.e. 0, S, +, and $\cdot$, and so J is a domain of an interpretation. Axiom Q3 is valid in the sense of J because of the property (xi). Axioms Q1, Q2, Q4–Q7 are valid in the sense of J because they are universal sentences. ∎

Remark Let the theory from our Theorem, i.e. Q enhanced by both associativity rules, the left distributivity rule, left neutrality of 0 and 1 w.r.t. + and $\cdot$ respectively, and $\forall x\forall y\forall z(y + x = z + x \rightarrow y = z)$, be temporarily called Q^+. Once we have an interpretation of Q^+ (in Q or in Q^-), it is easy to use the same but simplified method, see [4], to construct an interpretation of some extension T of Q^+ in Q^+ (and thus in Q and in Q^-).

Acknowledgment I would like to thank Petr Hájek for inspiring this paper, and also for useful comments. I also thank Prof. Grzegorczyk for a stimulating interest and for clarifying his original question, and I thank the unknown referee for useful remarks and for a suggestion to extend a previous version of the paper to the weaker theory with axioms G5 and G7.

References

[1] S. R. Buss. Nelson's work on logic and foundations and other reflections on foundations of mathematics. In W. G. Faris, editor, *Diffusion, Quantum Theory, and Radically Elementary Mathematics*, Mathematical Notes 47, pages 183–208. Princeton Univ. Press, 2006.

[2] A. Grzegorczyk. Computable relations and the essential undecidability of a very weak arithmetic of natural numbers. Manuscript, 2006.

[3] P. Hájek. Mathematical fuzzy logic and natural numbers. *Fundamenta Informaticae*, 81(1–3):155–163, 2007.

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

[5] E. Nelson. *Predicative arithmetic.* Princeton Univ. Press, Princeton, 1986.

[6] J. B. Paris and L. A. S. Kirby. Σ_n-collection schemas in arithmetic. In A. Macintyre, L. Pacholski, and J. Paris, editors, *Logic Colloquium '77*, number 96 in Studies in Logic and the Foundations of Mathematics, pages 199–209. North-Holland, Amsterdam, 1978.

[7] R. M. Solovay. Interpretability in set theories. Unpublished letter to P. Hájek, Aug. 17, 1976, http://www.cs.cas.cz/~hajek/RSolovayZFGB.pdf.

[8] A. Tarski, A. Mostowski, and R. M. Robinson. *Undecidable Theories.* North-Holland, Amsterdam, 1953.

[9] D. E. Willard. A version of the Second Incompleteness Theorem for axiom systems that recognize addition but not multiplication as a total function. In V. F. Hendricks et al., editors, *First-Order Logic Revisited: Proc. of the 75 Years of First-Order Logic Conference*, pages 337–368, Berlin, Germany, Sept. 2003. Logos Verlag, Berlin, 2004.

[10] D. E. Willard. An exploration of the partial respects in which an axiom system recognizing solely addition as a total function can verify its own consistency. *J. Symb. Logic*, 70(4):1171–1209, 2005.