Sequence encoding without induction

Emil Jeřábek*

Institute of Mathematics of the Academy of Sciences

Žitná 25, 115 67 Praha 1, Czech Republic, email: jerabek@math.cas.cz

January 27, 2012

Abstract

We show that the universally axiomatized, induction-free theory PA^- is a sequential theory in the sense of Pudlák [5], in contrast to the closely related Robinson's arithmetic.

Ever since Gödel's [1] arithmetization of syntax in the proof of his incompleteness theorem, sequence encoding has been an indispensable tool in the study of arithmetical theories and related areas of mathematical logic. While a common approach is to develop a particular sequence encoding in a suitable base theory and work with that, a general concept of theories supporting encoding of sequences of their elements, called *sequential theories*, was isolated by Pudlák [4, 5] during his work on interpretability. A similar but weaker notion was defined earlier by Vaught [7]. More generally, theories with "containers" of various kind were studied by Visser [8], who includes a discussion of variants of the notion of sequentiality and some historical remarks.

It is known that fairly weak arithmetical theories can be sequential (e.g., fragments of bounded arithmetic such as Buss' S^1_2, cf. Krajíček [3]), nevertheless sequential theories described in the literature so far generally involve some form of the induction schema. Indeed, the common induction-free base arithmetical theory, Robinson's Q [6], is *not* sequential (Visser [8]). This also shows that sequentiality is not preserved by interpretations (even in the tame form of definable cuts): the sequential theory S^1_2 is interpretable on a cut in Q. The reason is that in a sequential theory, all elements in the universe of the theory have to be admissible as sequence entries, not just elements from a proper cut. (On the other hand, the *lengths* of sequences may be confined to a small cut.)

In this note, we prove sequentiality of the theory PA^- of discretely ordered commutative semirings with the least element (without the subtraction axiom), and therefore of all its simple extensions. Like Q, PA^- is an induction-free theory axiomatized by basic properties of $+, \cdot, \leq$, and it (or its slightly stronger variants) is often used as an arithmetical base theory (see e.g. Kaye [2]). Our version of PA^- is purely universally axiomatized. The main result can

*Supported by Institutional Research Plan AV0Z10190503, grant IAA100190902 of GA AV ČR, and project 1M0545 of MŠMT ČR.

also be adapted in a straightforward way to the theory of discretely ordered (commutative) rings.

We encode sequences in PA^- using the well-known Gödel's β-function, slightly modified for a technical reason. Where the usual analysis of Gödel's β employs induction, we switch to a shorter cut; the main problem is to ensure we can make do with restricting only the lengths of sequences to the cut, while allowing arbitrary elements to appear in sequences. We proceed with the formal details.

Definition 1 Let PA^- be the theory of discretely ordered commutative semirings with the least element. That is, PA^- is the first-order theory with equality in the language $\langle 0, 1, +, \cdot, \leq \rangle$, axiomatized by

(A1) $$x + 0 = x$$

(A2) $$x + y = y + x$$

(A3) $$(x + y) + z = x + (y + z)$$

(M1) $$x \cdot 1 = x$$

(M2) $$x \cdot y = y \cdot x$$

(M3) $$(x \cdot y) \cdot z = x \cdot (y \cdot z)$$

(AM) $$x \cdot (y + z) = x \cdot y + x \cdot z$$

(O1) $$x \leq y \vee y \leq x$$

(O2) $$(x \leq y \wedge y \leq z) \to x \leq z$$

(S1) $$x + 1 \not\leq x$$

(S2) $$x \leq y \to (x = y \vee x + 1 \leq y)$$

(OA) $$x \leq y \to x + z \leq y + z$$

(OM) $$x \leq y \to x \cdot z \leq y \cdot z$$

Let $x < y$ abbreviate $x \leq y \wedge x \neq y$.

Note that many authors (e.g., Kaye [2] or Krajíček [3]) use a stronger definition of PA^-, namely as the theory of nonnegative parts of discretely ordered rings, which includes the subtraction axiom $x \leq y \to \exists z\,(z + x = y)$. In contrast, our version of PA^- is a universal theory, hence it does not even prove the existence of predecessors (e.g., the semiring $\mathbb{N}[x]$ of polynomials with nonnegative integer coefficients, ordered lexicographically, is a model of PA^-).

Sequentiality can be defined in several ways. For definiteness, we will follow the (relatively restrictive) definition of Pudlák [5]: a theory T is *sequential* if it contains Robinson's arithmetic Q relativized to some formula $N(x)$, and there is a formula $\beta(x, i, w)$ (whose intended meaning is that x is the ith element of a sequence w) such that T proves

(SEQ)
$$\forall w, x, k\, \exists w'\, \forall i, y\, [(N(k) \wedge i \leq k) \to [\,\beta(y, i, w') \leftrightarrow ((i < k \wedge \beta(y, i, w)) \vee (i = k \wedge y = x))]].$$

A definable set is called *inductive* if it contains 0 and is closed under successor, and it is a *cut* if it is furthermore downward closed.

We first establish some basic properties of PA^- which the reader might have been missing among the axioms:

Lemma 2 *PA^- proves*

(i) $(x \le y \wedge y \le x) \to x = y$

(ii) $x + z \le y + z \to x \le y$

(iii) $x \cdot 0 = 0$

(iv) $0 \le x$

(v) $(z \ne 0 \wedge x \cdot z \le y \cdot z) \to x \le y$

(vi) $x \le y + 1 \leftrightarrow (x \le y \vee x = y + 1)$

Proof: (i): Otherwise $x + 1 \le y$ by S2, hence $x + 1 \le x$ by O2, contradicting S1.

(ii): Otherwise $y < x$ by O1, hence $y + 1 \le x$ by S2 and $(x + z) + 1 \le (y + z) + 1 = (y + 1) + z \le x + z$ by OA, A2, A3, contradicting (O2 and) S1.

(iii): $x \cdot 0 + x = x \cdot 0 + x \cdot 1 = x(0 + 1) = x \cdot 1 = x = 0 + x$, hence $x \cdot 0 = 0$ by (ii) and (i).

(iv): $0 \le 1$ by S1 and O1, hence $0 = x \cdot 0 \le x \cdot 1 = x$.

(v): Otherwise $y < x$, thus $y + 1 \le x$, giving $yz \le yz + z = (y + 1)z \le xz \le yz$, hence $yz = yz + z$ by (i), and $z = 0$ by (ii) and (i).

(vi): Left-to-right: if $x < y + 1$, then $x + 1 \le y + 1$ by S2, hence $x \le y$. $\square$

Definition 3 Let $\langle x, y\rangle := (x + y)^2 + x$, and let

$$\beta(x, i, w) :\leftrightarrow \exists u, v, q\, [w = \langle u, v\rangle \wedge u = q(1 + (i + 1)v) + x \wedge x \le (i + 1)v]$$

be Gödel's β-function.

Lemma 4 *PA^- proves:*

(i) $(dx + y = dx' + y' \wedge y, y' < d) \to x = x' \wedge y = y'$

(ii) $\langle x, y\rangle = \langle x', y'\rangle \to (x = x' \wedge y = y')$

(iii) $(\beta(x, i, w) \wedge \beta(x', i, w)) \to x = x'$

Proof: (i): If $x < x'$, then $dx + y < dx + d = d(x + 1) \le dx' \le dx' + y' = dx + y$, a contradiction. Thus $x \ge x'$, and symmetrically, $x' \ge x$, thus $x = x'$, which implies $y = y'$.

(ii): We have $(x + y)^2 \le \langle x, y\rangle \le (x + y)^2 + (x + y) < (x + y + 1)^2$, and u^2 is monotone. Thus, $\langle x, y\rangle = \langle x', y'\rangle$ implies $x + y = x' + y'$, which in turn implies $x = x'$, which implies $y = y'$.

(iii): u, v are unique by (ii), and then (q and) x is unique by (i). $\square$

Definition 5 Let $x \operatorname{rem} y = z$ denote $z < y \wedge \exists q\,(x = z + qy)$ (this is PA^--provably a partial function by Lemma 4). We write $y \mid x$ for $\exists q\,(x = qy)$.

Note that $\beta(x, i, \langle u, v\rangle)$ iff $x = u \operatorname{rem}(1 + (i+1)v)$.

One step in the usual proof that Gödel's β-function works is to show that the numbers $1+v,\ 1+2v,\ \ldots,\ 1+kv$ are pairwise coprime if v is divisible by $1,\ \ldots,\ k-1$. The next lemma can be vaguely thought of as a replacement for this statement in our situation.

Lemma 6 *Let*

$$\begin{aligned}
&I_0(k) :\leftrightarrow \forall j \le i \le k\, \exists d\,(d + j = i),\\
&I_1(k) :\leftrightarrow I_0(k) \wedge \forall v\, \exists u\, [\forall i \le k\,(1 + iv \mid u)\\
&\qquad\qquad \wedge \forall i > k\,[(I_0(i) \wedge \forall 0 < j \le k\,(i - j \mid v)) \to \exists p\,(up \operatorname{rem}(1 + iv) = 1)]].
\end{aligned}$$

Then PA^- proves that I_0 is a cut and I_1 is inductive. Here, $i - j$ denotes the (unique) d such that $d + j = i$, which exists because of $I_0(i)$.

Proof: That I_0 is a cut is easy to see. $I_1(0)$ follows by taking $u = 1$. Assume $I_1(k)$, and let v be given. Let u be the witness for $I_1(k)$, and put $u' = (1 + (k+1)v)u$. Clearly $1 + iv \mid u'$ for all $i \le k+1$. Let $i > k+1$ be such that $I_0(i)$ and $i - j \mid v$ for all $j \le k+1$, $j > 0$. By $I_1(k)$, there exist p, q such that $up = 1 + (1 + iv)q$. Moreover, we claim that

$$(*) \qquad \big(1 + (k+1)v\big)p' = 1 + (1 + iv)q'$$

for some p', q'. Then $u'pp' = 1 + (1 + iv)\big(q + q' + qq'(1 + iv)\big)$, which completes the proof of $I_1(k+1)$.

In order to show $(*)$, write $k' = k + 1$, and fix z such that $(i - k')z = v$, which exists by our assumption on i. We have $k'v + k'^2 z = ik'z$, hence

$$(1 + k'v) + (1 + iv)k'^2 z = 1 + (1 + k'v)ik'z.$$

We add a suitable multiple of $(1 + k'v)(1 + iv)$ to both sides in order to move $1 + iv$ to the right-hand side and $1 + k'v$ to the left-hand side, as required in $(*)$:

$$\begin{aligned}
(1 + k'v)\big(1 + k' + ik'(i - (k'+1))z\big) &+ (1 + k'v)ik'z + (1 + iv)k'^2 z\\
&= (1 + k'v)(1 + k' + ik'v) + (1 + iv)k'^2 z\\
&= (1 + k'v) + (1 + iv)k'^2 z + (1 + k'v)(1 + iv)k'\\
&= 1 + (1 + k'v)ik'z + (1 + iv)(1 + k'v)k'\\
&= 1 + (1 + iv)\big(k' + k'^2(i - (k'+1))z\big) + (1 + iv)k'^2 z + (1 + k'v)ik'z,
\end{aligned}$$

and we can cancel $(1 + k'v)ik'z + (1 + iv)k'^2 z$ from both sides using Lemma 2. Thus, we have $(*)$ with $p' = 1 + k' + ik'(i - (k'+1))z$ and $q' = k' + k'^2(i - (k'+1))z$. $\square$

The main point of the following definition of $I_2(k)$ is that β-encoded sequences of length k can be recoded using a different v, as well as expanded by a $(k+1)$th element. This is made more explicit in Lemma 8.

Lemma 7 *Define*

$$\begin{aligned} I_2(k) :\leftrightarrow\ & I_1(k) \wedge \forall u, v, v', x\, \exists u' \\ & [(\forall 0 < i \le k\, (i \mid v') \wedge v' \ge v \wedge (k+1)v' \ge x \wedge \forall i \le k\, \exists r\, (r = u \operatorname{rem} (1 + iv))) \\ & \quad \to (\forall i \le k\, \exists r\, (r = u \operatorname{rem} (1 + iv) \wedge r = u' \operatorname{rem} (1 + iv')) \\ & \qquad \wedge x = u' \operatorname{rem} (1 + (k+1)v'))]. \end{aligned}$$

Then PA^- proves that I_2 is inductive.

Proof: For $k = 0$, we can take $u' := x$.

Assume $I_2(k)$, we will prove $I_2(k+1)$. Let u, v, v', x be given. By $I_2(k)$, we can find a u_0 such that there exists $u_0 \operatorname{rem} (1 + iv') = u \operatorname{rem} (1 + iv)$ for all $i \le k+1$, using the fact that $u \operatorname{rem} (1 + (k+1)v) \le (k+1)v \le (k+1)v'$. Since $I_1(k+1)$ and v' is divisible by $1, \dots, k+1$, there are u_1, p, q such that $1 + iv' \mid u_1$ for all $i \le k+1$, and $u_1 p = 1 + (1 + (k+2)v')q$. Define $u' := u_0 + (x + u_0(k+2)v')u_1 p$. Then $u' \operatorname{rem} (1 + iv') = u \operatorname{rem} (1 + iv)$ for all $i \le k+1$, and $x = u' \operatorname{rem} (1 + (k+2)v')$, as

$$\begin{aligned} u' &= u_0 + \big(x + u_0(k+2)v'\big)\big(1 + (1 + (k+2)v')q\big) \\ &= \big(x + u_0(k+2)v'\big)q\big(1 + (k+2)v'\big) + u_0 + u_0(k+2)v' + x \\ &= \big(u_0 + xq + u_0(k+2)v'q\big)\big(1 + (k+2)v'\big) + x, \end{aligned}$$

and $x < 1 + (k+2)v'$. □

Lemma 8 *PA^- proves: if $I_2(k)$ and $\forall i < k\, \exists x\, \beta(x, i, w)$, then there exists a w' such that*

$$\forall i \le k\, \forall y\, [\beta(y, i, w') \leftrightarrow ((i < k \wedge \beta(y, i, w)) \vee (i = k \wedge y = x))].$$

Proof: Let $w = \langle u_0, v_0 \rangle$, and write $(w)_i = x$ instead of $\beta(x, i, w)$ for clarity. Applying $I_1(k)$ with $v = 1$, we see that there exists a $v' > 0$ divisible by $1, \dots, k+1$. Pick v_1 such that $v_1 \ge v_0$, $v_1 \ge x$, and $v' \mid v_1$. By $I_2(k)$, there exists u_1 such that for all $i < k$, $u_1 \operatorname{rem} (1 + (i+1)v_1) = u_0 \operatorname{rem} (1 + (i+1)v_0)$, and $u_1 \operatorname{rem} (1 + (k+1)v_1) = x$. Thus, if we put $w' := \langle u_1, v_1 \rangle$, then $(w')_i = (w)_i$ for all $i < k$, and $(w')_k = x$. □

Clearly, Lemmas 7 and 8 almost show that PA^- is sequential. However, as PA^- does not prove that division with remainder is total, it may happen for Gödel's β-function that $(w)_i$ is undefined for some values of $i < k$, and then the definition of sequentiality requires $(w')_i$ to be also undefined for the same values of i. This does not seem possible to arrange, as we have no way of forcing $(w')_i$ to be undefined when building w'. We fix this problem by modifying the definition of β a little bit.

Definition 9

$$\beta'(x, i, w) :\leftrightarrow [\,\beta(x, i, w) \wedge \forall j < i\, \exists y\, \beta(y, j, w)] \vee [x = 0 \wedge \exists j \le i\, \neg \exists y\, \beta(y, j, w)].$$

Note that β' is PA^--provably a total function.

Lemma 10 *PA^- proves that*

$$I_3(k) :\leftrightarrow I_2(k) \wedge \forall w' \, \exists w \, \forall i < k \, \forall x \, (\beta(x, i, w) \leftrightarrow \beta'(x, i, w'))$$

is inductive.

Proof: $I_3(0)$ is clear. Assuming $I_3(k)$, we have $I_2(k+1)$ by Lemma 7. Let w be given, and write $x = (w)_i$ instead of $\beta'(x, i, w)$ for clarity. Since $I_3(k)$, there exists w' such that $\beta((w)_i, i, w')$ for all $i < k$. By Lemma 8, there exists w'' such that $\beta((w)_i, i, w'')$ for $i < k$, and $\beta((w)_k, k, w'')$. This shows $I_3(k+1)$. $\square$

By the usual shortening of cuts, let $N(x)$ be such that PA^- proves that N is a cut closed under $+$ and $\cdot$, and $N(x) \to I_3(x)$.

Theorem 11 *PA^- is a sequential theory with respect to N and β'.*

Proof: PA^- proves itself relativized to N, as it is a universal theory. Moreover, if $x \leq y$ and $N(y)$, there exists z such that $z + x = y$ as $I_0(y)$, and we have $N(z)$ as N is downward closed. Thus, the subtraction axiom holds in N, hence N is an interpretation of Q in PA^-.

In order to show (SEQ) for β', let w, x, k such that $N(k)$ be given, and write $(w)_i = y$ for $\beta'(y, i, w)$. By the definition of I_3, we can find a w' such that $\beta((w)_i, i, w')$ for each $i < k$. Then Lemma 8 gives a w'' such that $\beta((w)_i, i, w'')$ for each $i < k$, and $\beta(x, k, w'')$. By the definition of β', this implies $(w'')_i = (w)_i$ for $i < k$, and $(w'')_k = x$. $\square$

In contrast, Robinson's Q is not sequential, despite that it is fairly close to PA^- in strength. In fact, Visser [8] proved that it does not even support pairing; we include a somewhat different proof of his result below for completeness:

Theorem 12 *Q is not sequential, and it has no pairing operation: i.e., there is no formula $\pi(x, y, p)$ such that Q proves*

(i) $\forall x, y \, \exists p \, \pi(x, y, p)$,

(ii) $\forall x, y, x', y', p \, [(\pi(x, y, p) \wedge \pi(x', y', p)) \to (x = x' \wedge y = y')]$.

Proof: Let $M = \mathbb{N} \,\dot\cup\, \{a_0, a_1\}$, and define arithmetical operations on M extending the usual operations on $\mathbb{N}$ by $a_i + x = a_i$, $n + a_i = a_i$, $n \cdot a_i = a_i$, $a_i \cdot 0 = 0$, $a_i \cdot x = a_i$ if $x \neq 0$, where $x \in M$, and $n \in \mathbb{N}$. Then $M \vDash Q$, and the function f identical on $\mathbb{N}$ such that $f(a_i) = a_{1-i}$ is an automorphism of M. Let π be a pairing operation, and find an x such that $\pi(a_i, a_j, x)$. Since f is an automorphism, $\pi(a_{1-i}, a_{1-j}, f(x))$. By unique decoding of pairs, it follows that $f(x) \neq x$, i.e., $x \in \{a_0, a_1\}$. However, there are only two elements in $\{a_0, a_1\}$, while there are four pairs of the form $\langle a_i, a_j \rangle$, contradicting uniqueness. $\square$

Acknowledgement

I am grateful to Albert Visser for many useful suggestions.

References

[1] Kurt Gödel, *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme, I*, Monatshefte für Mathematik und Physik 38 (1931), pp. 173–198.

[2] Richard Kaye, *Models of Peano arithmetic*, Oxford Logic Guides vol. 15, Oxford University Press, 1991.

[3] Jan Krajíček, *Bounded arithmetic, propositional logic, and complexity theory*, Encyclopedia of Mathematics and Its Applications vol. 60, Cambridge University Press, 1995.

[4] Pavel Pudlák, *Some prime elements in the lattice of interpretability types*, Transactions of the American Mathematical Society 280 (1983), no. 1, pp. 255–275.

[5] ———, *Cuts, consistency statements and interpretations*, Journal of Symbolic Logic 50 (1985), no. 2, pp. 423–441.

[6] Alfred Tarski, Andrzej Mostowski, and Rafael M. Robinson, *Undecidable theories*, North-Holland, Amsterdam, 1953.

[7] Robert L. Vaught, *Axiomatizability by a schema*, Journal of Symbolic Logic 32 (1967), no. 4, pp. 473–479.

[8] Albert Visser, *Pairs, sets and sequences in first-order theories*, Archive for Mathematical Logic 47 (2008), no. 4, pp. 299–326.