The Review of Modern Logic
Volume 9 Numbers 1 & 2 (November 2001–November 2003) [Issue 29], pp. 67–79.

SIMPLE AXIOMS THAT ARE OBVIOUSLY TRUE IN $\mathbb{N}$

TOMASZ POŁACIK AND WIM RUITENBURG

Abstract. We discuss simple subtheories of Peano arithmetic over languages which include the monus function. The system ZDL corresponds with PA^-. The choice of language permits our theories to have special universal axiomatizations; their classes of models have corresponding model theoretic properties.

1. Introduction

A common base system in the study of arithmetic is PA^-, see [4]. Its models form the class of nonnegative parts of discretely (linearly) ordered rings. The theory is axiomatized over a first-order language with 0, 1, $x+y$, xy, and $x<y$ (or $x \leq y$). We discuss modifications of the base system which permit us to use results from model theory and universal algebra to obtain nice properties for their classes of models.

One drawback of PA^- as defined in [4] is, that it is not Π^0_1-axiomatizable or, equivalently, its class of models is not closed under submodels. For example, let $\mathbb{Z}[X]^+$ be the substructure of the ring of polynomials $\mathbb{Z}[X]$ by excluding all polynomials with negative leading coefficient. Let $\mathbb{N}[X]$ be the substructure of polynomials over the natural numbers. There is a straightforward way to extend the linear order of $\mathbb{Z}$ to $\mathbb{Z}[X]$ by setting X to infinitely large with respect to $\mathbb{Z}$. The substructures inherit this linear order. Obviously, $\mathbb{N}[X] \subseteq \mathbb{Z}[X]^+$ as ordered structures. But $\mathbb{Z}[X]^+$ is a model of PA^- while $\mathbb{N}[X]$ is not, see [4, pages 18, 20].

As first modification we choose a different language by deleting $x<y$ and adding the monus function (symbol) $x \dot{-} y$. Over this language we define as minimal system an equational theory Z_0. The theory Z of nontrivial models of Z_0 is axiomatized by $\mathrm{Z}_0 \cup \{1 = 0 \rightarrow \bot\}$. We consider additional universal axioms D, L, and N. Theories $\mathrm{Z}_0\mathrm{L}$, ZD and so on, are defined by adding the appropriate axioms to the theories

---

1991 *Mathematics Subject Classification.* Primary: 03F30; Secondary: 03C05, 03C62, 06D99, 11U09.

Key words and phrases. Subsystems of Peano Arithmetic, universal algebra.

Z_0 or Z. Already over Z_0 we can define a partial order $x \leq y$ which over ZDLN is a linear order. The theory ZDLN equals ZDL, and corresponds in obvious ways with PA^-.

Recall that a sentence is universal Horn if it has form $\forall x_1, \ldots, x_m(P_1 \wedge \ldots \wedge P_n \to P_0)$, where the P_i are atomic formulas, possibly including truth $\top$ or falsum $\bot$.

The theory ZD is the universal Horn fragment of ZDL; the theory Z_0D is the equational fragment of ZDL. It is natural to think of Z_0D as the right candidate for minimal system. However, many properties of Z_0D immediately generalize to Z_0. Additionally, we present a nice model of Z_0 which satisfies interesting induction schemata, but which is not a model of Z_0D.

Most of our techniques are well-known. For model theory, see [1]. For universal algebra, see [2] or [3].

2. Axioms and Basic Properties of Z_0 and Extensions

The theories of this section are universal over the language with nonlogical symbols 0, 1, $x + y$, $x \dot{-} y$, and $x \cdot y$. We usually write xy as short for $x \cdot y$. We also employ the usual abbreviations 2 for $1 + 1$, 3 for $2 + 1$, and so on.

Define Z_0 to be the theory axiomatized by

A1 $x + 0 = x$
A2 $x + y = y + x$
A3 $(x + y) + z = x + (y + z)$
A4 $(x + y) \dot{-} y = x$
A5 $x \dot{-} (y + z) = (x \dot{-} y) \dot{-} z$
A6 $x + (y \dot{-} x) = y + (x \dot{-} y)$

With restriction to appropriate sublanguages, the theory axiomatized by A1 through A6 is the *linear fragment* of Z_0. Additionally, Z_0 has axioms

A7 $x1 = x$
A8 $xy = yx$
A9 $(xy)z = x(yz)$
A10 $x(y + z) = xy + xz$
A11 $x(y \dot{-} z) = xy \dot{-} xz$

This completes the axiomatization of Z_0.

Let Z be the theory axiomatizable by Z_0 plus

$$1 = 0 \to \bot$$

Define the axiom D of discrete order by

$$x(1 \dot{-} x) = 0$$

Define the axiom L of linear order by

$(x \dot{-} y = 0) \vee (y \dot{-} x = 0)$

Define the axiom N of no nilpotents by

$x^2 = 0 \rightarrow x = 0$

We show that Z is the theory of nontrivial models of Z_0. We introduce a first-order definable order $x \leq y$ over Z_0 which justifies the names of axioms D and L. Theories with names like Z_0L or ZDN are defined by adding the appropriate axioms to the systems Z_0 or Z.

If $a + b = a + c$ holds over Z_0, then also $(a + b) \dot{-} a = (a + c) \dot{-} a$. So Z_0 satisfies

E1 $x + y = x + z \rightarrow y = z$

Also, $(a + b) \dot{-} (a + c) = ((a + b) \dot{-} a) \dot{-} c = b \dot{-} c$, giving us

E2 $(x + y) \dot{-} (x + z) = y \dot{-} z$

From $a + (0 \dot{-} a) = 0 + (a \dot{-} 0)$ we get $a + (0 \dot{-} a) = 0 + ((a + 0) \dot{-} 0) = a$. So Z_0 satisfies

E3 $0 \dot{-} x = 0$

Define abbreviations

$x \leq y$ for $x \dot{-} y = 0$
$x \sqcup y$ for $x + (y \dot{-} x)$

Axiom A6 states that $a \sqcup b = b \sqcup a$. Obviously, Z_0 satisfies $0 \leq a$ and $a \leq a$. Suppose $a \leq b$ and $b \leq a$. Then $a = a + (b \dot{-} a) = b + (a \dot{-} b) = b$. So we have $a \leq b \wedge b \leq a \rightarrow a = b$.

Lemma 2.1. *Over Z_0, the following are equivalent, for all a and c.*

- $a + b = c$, *for some* b
- $a \leq c$
- $a \sqcup c = c$
- $a + (c \dot{-} a) = c$

We leave the proof of Lemma 2.1 as an exercise. Suppose $a \leq b$ and $b \leq c$. Then there are a' and b' such that $a + a' = b$ and $b + b' = c$. So $a + a' + b' = c$, thus $a \leq c$. So we have

Proposition 2.2. *Over Z_0, the formula $x \leq y$ is a partial order with least element* 0.

We easily verify that Z_0 satisfies

E4 $x \leq y \leftrightarrow (x + z) \leq (y + z)$
E5 $x \leq y \wedge z \leq t \rightarrow (x + z) \leq (y + t)$

$((a \dot{-} b) \dot{-} a) = (a \dot{-} (a + b)) = 0$, so Z_0 satisfies

E6 $x \dot{-} y \leq x$

E7 $x \leq y \to (z \dot{-} y) \leq (z \dot{-} x)$ (set $y = x + b$)

$(a \dot{-} c) \dot{-} (b \dot{-} c) = (a \dot{-} b) \dot{-} (c \dot{-} b)$, so Z_0 satisfies

E8 $x \leq y \to (x \dot{-} z) \leq (y \dot{-} z)$

Obviously, over Z_0 we have $a \leq a \sqcup b$ and $b \leq a \sqcup b$. Formula E8 gives that $a \leq b$ implies $a \sqcup c \leq b \sqcup c$. So if $a \leq c$ and $b \leq c$, then $a \sqcup b \leq a \sqcup c = c$. Thus:

Proposition 2.3. *Over Z_0, the term $x \sqcup y$ is the least upper bound of x and y.*

Introduce abbreviation

$x \sqcap y$ for $x \dot{-} (x \dot{-} y)$

With formula E6 we get $a = (a \dot{-} b) \sqcup a = (a \dot{-} b) + a \sqcap b$. Adding $b \dot{-} a$ to both sides gives $a \sqcup b = (b \dot{-} a) + (a \dot{-} b) + a \sqcap b$. Since $a \sqcup b = b \sqcup a$, we have $a \sqcap b = b \sqcap a$. Obviously, $a \sqcap b \leq a$. So also $a \sqcap b \leq b$.

Lemma 2.4. *Over Z_0, the following are equivalent, for all a and c.*

- $a = c \dot{-} b$, *for some* b
- $a \leq c$
- $a \sqcap c = a$
- $a = c \dot{-} (c \dot{-} a)$

We leave the proof of Lemma 2.4 as an exercise. Formula E7 gives that $a \leq b$ implies $c \sqcap a \leq c \sqcap b$. So if $c \leq a$ and $c \leq b$, then $c = c \sqcap b \leq a \sqcap b$. Thus:

Proposition 2.5. *Over Z_0, the term $x \sqcap y$ is the greatest lower bound of x and y.*

With equation $a \sqcap b + (a \dot{-} b) = a$ one easily sees that Z_0 satisfies

E9 $x \sqcap y + (x \sqcup y) = x + y$

We leave it as easy exercises to show that Z_0 satisfies

E10 $(x + z) \sqcup (y + z) = (x \sqcup y) + z$
E11 $(x + z) \sqcap (y + z) = x \sqcap y + z$

Now

$$\begin{aligned} & a \sqcap b \\ &= ((a \dot{-} b) + a \sqcap b) \sqcap ((b \dot{-} a) + a \sqcap b) \\ &= (a \dot{-} b) \sqcap (b \dot{-} a) + a \sqcap b \end{aligned}$$

So Z_0 satisfies

E12 $(x \dot{-} y) \sqcap (y \dot{-} x) = 0$

Over Z_0, the lattice determined by $x \leq y$ is also distributive. We postpone this and several other beautiful results until after we discuss the structure of the class of models of Z_0 and its extensions. With our model theoretic results we can significantly simplify the derivation of certain collections of formulas.

It is now obvious that L axiomatizes linearity over Z_0: For all elements a and b it implies $a \leq b \vee b \leq a$.

Discrete order versus axiom D is more complicated. Recall that a linearly ordered ring is discrete when for all elements a and c, if $a \leq c \leq a+1$, then $c = a$ or $c = a+1$. Products of linearly ordered discrete rings are partially ordered with a distributive lattice, and satisfy the weaker property: If $a \leq c \leq a+1$, then $c - a$ is idempotent. It is reasonable to call such partially ordered rings discrete. A similar argument applies to Z_0D. Let a and c be elements of a model of Z_0D such that $a \leq c \leq a+1$. So $c = a+b$ for an element b satisfying $b \leq 1$, so also $b^2 \leq b$. Axiom D implies $b \leq b^2$. Thus b is idempotent.

Define abbreviation

$\delta(x, y)$ for $(x \dot- y) + (y \dot- x)$

We show that $\delta(x, y)$ behaves like a distance function. First an auxiliary result:

$$\begin{aligned}
&((a \dot- c) \sqcup (b \dot- c)) + (a \dot- b) \sqcap (c \dot- b) \\
&= (b \dot- c) + ((a \dot- (c + (b \dot- c)) + ((a \dot- b) \dot- ((a \dot- b) \dot- ((c \dot- b)) \\
&= (b \dot- c) + ((a \dot- (b + (c \dot- b)) + ((a \dot- b) \dot- ((a \dot- b) \dot- ((c \dot- b)) \\
&= (b \dot- c) + ((a \dot- b) \dot- (c \dot- b)) + ((a \dot- b) \dot- ((a \dot- b) \dot- ((c \dot- b)) \\
&= (b \dot- c) + [((a \dot- b) \dot- (c \dot- b)) \sqcup (a \dot- b)] \\
&= (b \dot- c) + (a \dot- b)
\end{aligned}$$

So Z_0 satisfies

E13 $((x \dot- z) \sqcup (y \dot- z)) + (x \dot- y) \sqcap (z \dot- y) = (x \dot- y) + (y \dot- z)$

Formula E13 immediately implies

E14 $(x \dot- z) \leq (x \dot- y) + (y \dot- z)$

With formula E14 we get $\delta(a, c) \leq \delta(a, b) + \delta(b, c)$. So we obviously have:

Proposition 2.6. *Over Z_0, the function $\delta(x, y)$ acts like a metric, satisfying*

$$\begin{aligned}
&\delta(x, y) = 0 \leftrightarrow x = y \\
&\delta(x, y) = \delta(y, x) \\
&\delta(x, z) \leq \delta(x, y) + \delta(y, z)
\end{aligned}$$

Finally, we place the new theories relative to one another and to PA^-.

Proposition 2.7. *The theories* Z_0D *and* Z_0DN *are equal.*

Proof. Let a be an element over Z_0D such that $a^2 = 0$. Then $a \leq a^2$ implies $a = 0$. □

With Proposition 2.7 we see that the 16 theories we can construct over Z_0 or Z by adding combinations of D, L, and N, really are at most 12 different theories. With the model theoretic results of Section 3 we easily see that these 12 all differ.

For all a over Z_0 we have $a0 = a(0 + 0) = a0 + a0$. So $a0 = 0$. Since $a1 = a$, we get that Z_0 satisfies

E15 $x0 = 0$

E16 $1 = 0 \to x = y$

This implies that Z is the theory of nontrivial models of Z_0.

We have already seen how to define $x \leq y$, so also $x < y$, over ZDL. Conversely, define $x \dot{-} y = z$ over PA^- by

$$x = y + z \vee (x < y \wedge z = 0)$$

It is a straightforward exercise to show that in this way we can convert models of ZDL into models of PA^- and back.

3. Model Theory of Z_0 and Extensions

The natural numbers $\mathbb{N}$ form a model of ZDL. The nonnegative rationals $\mathbb{Q}^{+0}$, and the nonnegative reals $\mathbb{R}^{+0}$, are models of ZLN.

The class of models of a first-order theory is closed under isomorphisms, ultraproducts, and elementary submodels. From universal algebra and model theory we also know that the class of models of an equational theory is closed under submodels, products, and (homomorphic) images. So these closure rules apply to the model classes of Z_0 and Z_0D. Similarly, the classes of models of the universal Horn theories Z, ZD, ZN, and Z_0N, are closed under submodels and products. The classes of models of the universal theories Z_0L, ZL, Z_0DL, ZDL, Z_0LN, and ZLN, are closed under submodels.

A subset I of a model $\mathcal{M}$ of Z_0 is called an *ideal* if it satisfies:

I1 $0 \in I$

I2 $a \leq b \in I$ implies $a \in I$, for all a, b

I3 $a, b \in I$ implies $a + b \in I$, for all a, b

I4 $a \in I$ implies $ab \in I$, for all a, b

An ideal is *nontrivial* if 1 is not an element of the ideal.

Let $\varphi \colon \mathcal{M} \to \mathcal{N}$ be a morphism between models of Z_0. Define $\ker(\varphi) = \{ m \in \mathcal{M} \mid \varphi(m) = 0 \}$. Morphisms define a congruence $\sim$ on their domain defined by $a \sim b$ exactly when $\varphi(a) = \varphi(b)$.

Proposition 3.1. *Each ideal I of a model $\mathcal{M}$ of* Z_0 *defines a congruence on $\mathcal{M}$ defined by $a \sim b$ exactly when $\delta(a,b) \in I$. If φ is a morphism with domain $\mathcal{M}$, then its kernel* $\ker(\varphi)$ *is an ideal on $\mathcal{M}$ which defines the same congruence on $\mathcal{M}$ as φ.*

Proof. Let I be an ideal, and let $a \sim b$ be defined by $\delta(a,b) \in I$. Obviously, $x \sim y$ is an equivalence relation. Suppose $a \sim b$ and $c \sim d$. Then $\delta(a+c,b+d) \leq \delta(a+c,b+c)+\delta(b+c,b+d) = \delta(a,b)+\delta(c,d) \in I$. Also, $\delta(a \dot- c, b \dot- d) \leq \delta(a \dot- c, b \dot- c)+\delta(b \dot- c, b \dot- d) \leq \delta(a,b)+\delta(c,d) \in I$. Finally, $\delta(ac,bd) \leq \delta(ac,bc) + \delta(bc,bd) = c\delta(a,b) + b\delta(c,d) \in I$.

Let φ be a morphism with domain $\mathcal{M}$. Obviously, $\ker(\varphi)$ is an ideal. Now $a \sim b$ if and only if $\varphi(a) = \varphi(b)$ if and only if $\delta(\varphi(a),\varphi(b)) = \varphi(\delta(a,b)) = 0$ if and only if $\delta(a,b) \in \ker(\varphi)$. □

For all models $\mathcal{M}$ and ideals I of $\mathcal{M}$, we can now form quotient models $\mathcal{M}/I$ in the expected way. All images of $\mathcal{M}$ are, up to isomorphism, of the form $\mathcal{M}/I$.

Let a be an element of a model $\mathcal{M}$ of Z_0. Define $\langle a\rangle = \{\, b \mid b \leq ac \text{ for some } c \,\}$. It is an easy exercise to show that $\langle a\rangle$ is an ideal, and the least ideal containing a.

Example 3.2. Consider the model $\mathcal{M}$ constructed from the product model $(\mathbb{Q}^{+0})^\omega$ as follows: Take the product model modulo the cofinite filter $\mathcal{F}$ on ω. Then choose for $\mathcal{M}$ the submodel generated by the constant functions plus the function ε defined by $\varepsilon(n) = \frac{1}{n+1}$ (the elements of $(\mathbb{Q}^{+0})^\omega/\mathcal{F}$ are equivalence classes of functions $\omega \to \mathbb{Q}^{+0}$). The structure $\mathcal{M} \cong \mathbb{Q}^{+0}[\varepsilon]$ is a model of ZLN such that $a\varepsilon \leq 1$ for all $a \in \mathcal{M}$. The quotient $\mathbb{Q}^{+0}[\varepsilon]/\langle\varepsilon\rangle \cong \mathbb{Q}^{+0}$.

Let $\mathcal{M}$ be a model of Z_0. Define $\sqrt{0}$ to be the set $\{\, x \in \mathcal{M} \mid x^n = 0 \text{ for some } n \,\}$. It is an easy exercise to show that $\sqrt{0}$ is an ideal, and proper when 1 is not equal to 0. The quotient $\mathcal{M}/\sqrt{0}$ is a model of $\mathrm{Z}_0\mathrm{N}$.

For ideals I, we define ideals $\sqrt{I}$ in the obvious way.

Example 3.3. Let $\mathcal{M}$ be the model of Example 3.2. Up to isomorphism, the quotient $\mathcal{M}/\langle\varepsilon^2\rangle = \mathbb{Q}^{+0}[d]$, with $d = \varepsilon/\langle\varepsilon^2\rangle$ satisfying $d^2 = 0$ while d is nonzero. So $\mathbb{Q}^{+0}[d]$ is a model of ZL which is not a model of ZLN. We easily verify that $\langle d\rangle = \sqrt{0}$.

The collection of ideals of a model of Z_0 is closed under unions of chains and under intersections. A union of a chain of proper ideals is proper. So each proper ideal is contained in a maximal proper ideal. The collection of ideals forms a complete lattice with respect to set inclusion.

Let a be an element of a model $\mathcal{M}$ of Z_0. Define $\langle 0\rangle : \langle a\rangle = \{\, b \mid ab = 0\,\}$. It is an easy exercise to show that $\langle 0\rangle : \langle a\rangle$ is an ideal, and nontrivial exactly when a is nonzero. Let I_a be the ideal $\cup_n(\langle 0\rangle : \langle a^n\rangle)$. In the quotient $\mathcal{M}/I_a$, if $ab = ac$, then $b = c$.

A nontrivial ideal I is called *linear* if $a \sqcap b \in I$ implies $a \in I$ or $b \in I$, for all a and b. So, with formula E12, I is linear exactly when $\mathcal{M}/I$ is a model of Z_0L.

Proposition 3.4. *Let $\mathcal{M}$ be a model of* Z*, and $a \in \mathcal{M}$ be such that $a \neq 0$. Then there is an ideal J of $\mathcal{M}$ which is maximal with the property that a is not an element of J. Additionally, J is such that*

$\mathcal{M}/J$ is a model of ZL
For all $b \in \mathcal{M}/J$, if $bc \leq a$ for all c, then $b = 0$

Proof. The zero ideal does not contain a. By Zorn's Lemma, there is a maximal ideal J such that $a \notin J$.

Let J be an ideal, maximal in not containing a. Let $b, c \in \mathcal{M}/J$ be such that $b \sqcap c = 0$. To show: $b = 0$ or $c = 0$. If $a \in \langle b\rangle \cap \langle c\rangle$, then there is d such that $a \leq (bd) \sqcap (cd) = (b \sqcap c)d = 0$, contradiction. So we may assume that $a \notin \langle b\rangle$. So, by the maximality of J, $\langle b\rangle = 0$. Thus $b = 0$.

If $bc \leq a$ for all c, then $a \notin \langle b\rangle$. So, by the maximality of J, $b = 0$. □

So models of Z are, up to isomorphism, exactly the submodels of products of models of ZL, even subdirect products of models of ZL which satisfy the additional property

$$\exists x[x \neq 0 \wedge \forall y(\forall z(yz \leq x) \rightarrow y = 0)]$$

With universal algebra and with model theory we have:

Proposition 3.5. *The theory* Z *is the universal Horn fragment of* ZL*. The theory* Z_0 *is the equational fragment of* ZL*. The theory* ZD *is the universal Horn fragment of* ZDL*. The theory* Z_0D *is the equational fragment of* ZDL*.*

Let $\mathbb{Z}\Big[X, X\sqrt{2}\Big]^+$ be the substructure of the ring $\mathbb{Z}\Big[X, X\sqrt{2}\Big]$, obtained by removing all polynomials with negative leading coefficient. Set $n \dot{-} X = 0$, for all natural numbers n. This uniquely makes $\mathbb{Z}\Big[X, X\sqrt{2}\Big]^+$ a model of ZDL, satisfying

$$\exists xy(\delta((x+1)^2, 2(y+1)^2) = 0)$$

Now $\mathbb{N}$ satisfies

$$1 \dot{-} \delta((x+1)^2, 2(y+1)^2) = 0$$

So Z_0D is not the equational fragment of the theory of $\mathbb{N}$. Since $\mathbb{N}$ is submodel of all models of Z, the universal fragment of its theory is the unique largest consistent universal extension of Z.

Applications of Proposition 3.5: Let a and b be elements of a model of ZL. If $a \leq b$, then $a \sqcap b = a$ and $a \sqcup b = b$, so $ab = (a \sqcap b)(a \sqcup b)$. Otherwise, $b \leq a$ and, by an argument similar to the one above, $ab = (a \sqcap b)(a \sqcup b)$. So, with Proposition 3.5, Z_0 satisfies

E17 $xy = (x \sqcap y)(x \sqcup y)$

The following is now obvious: Let a, b, and c be elements of a model of ZL. Then $b \leq c \vee c \leq b$ implies that $a \sqcap (b \sqcup c) = a \sqcap b \sqcup a \sqcap c$. So, with Proposition 3.5:

Proposition 3.6. *Over* Z_0*, the lattice determined by* $x \leq y$ *is distributive.*

We easily verify that Z_0N is axiomatizable by Z_0 plus

E18 $xy = 0 \to x \sqcap y = 0$

With formula E12 we see that Z_0L is axiomatizable by Z_0 plus

E19 $x \sqcap y = 0 \to (x = 0 \vee y = 0)$

So, with formula E17, Z_0LN is axiomatizable by Z_0 plus

E20 $xy = 0 \to (x = 0 \vee y = 0)$

A nontrivial ideal I is called *prime* if $ab \in I$ implies $a \in I$ or $b \in I$, for all a and b. Obviously, prime ideals are linear. I is prime exactly when $\mathcal{M}/I$ is a model of Z_0LN.

An element a is called *nilpotent* when $a^n = 0$, for some n.

Proposition 3.7. *Let* $\mathcal{M}$ *be a model of* Z*, and* $a \in \mathcal{M}$ *be such that* a *is not nilpotent. Then there is an ideal* J *of* $\mathcal{M}$ *which is maximal with the property that no power of* a *is an element of* J*. Additionally,* J *is prime.*

Proof. By Zorn's Lemma there exists an ideal J that is maximal in not containing a power of a. Suppose we have elements b and c that are not in J. Set $J[b] = \{ y \mid y \leq j + db \text{ for some } j \in J \text{ and } d \in \mathcal{M} \}$ and $J[c] = \{ y \mid y \leq j + dc \text{ for some } j \in J \text{ and } d \in \mathcal{M} \}$. Obviously, $J[b]$ and $J[c]$ are ideals. By the maximality of J, there are integers m and n such that $a^m \leq j_1 + d_1 b$ and $a^n \leq j_2 + d_2 c$. So $a^{m+n} \leq (j_1 + d_1 b)(j_2 + d_2 c) \in J[bc]$. So $bc \notin J$. Thus J is prime. $\square$

In particular, models of ZN are, up to isomorphism, exactly the submodels of products of models of ZLN. With universal algebra and with model theory we have:

Proposition 3.8. *The theory* ZN *is the universal Horn fragment of* ZLN.

Model $\mathbb{R}^{+0}$ satisfies

$$\exists xy(\delta((x+1)^2, 2(y+1)^2) = 0)$$

while $\mathbb{Q}^{+0}$ satisfies

$$\forall xyzw(\delta((x+1)^2, 2(y+1)^2)z = \delta((x+1)^2, 2(y+1)^2)w \rightarrow z = w)$$

So ZN is not the universal Horn fragment of the theory of $\mathbb{Q}^{+0}$.

We construct structures $R(\mathcal{M})$ from models $\mathcal{M}$ of Z_0, similar to the construction of $\mathbb{Z}$ from $\mathbb{N}$. Take all pairs $(m, n) \in M \times M$, where M is the underlying set of $\mathcal{M}$. Define $(m, n) \simeq (p, q)$ exactly when $m + q = p + n$. Informally, (m, n) stands for $m - n$. It is a standard exercise to verify that $\simeq$ defines an equivalence relation which is respected by addition $(m, n) + (p, q) = (m + p, n + q)$ and multiplication $(m, n) \cdot (p, q) = (mp + nq, mq + np)$. Additionally, $(m, n) \dot{-} (p, q) = ((m + q) \dot{-} (n + p), 0)$ respects the equivalence. The result is a commutative ring with a function $x \dot{-} y$ such that the substructure on the elements of the form $(m, 0)$, is isomorphic to $\mathcal{M}$. The commutative ring is nontrivial, exactly when $\mathcal{M}$ is a model of Z. The commutative ring is an integral domain, exactly when $\mathcal{M}$ is a model of ZLN. The map $m \mapsto (m, 0)$ is an embedding. As for $\mathbb{N}$ and $\mathbb{Z}$, it is usual to identify $\mathcal{M}$ with this image. Since $(m, n) = (m \dot{-} n, 0) + (0, n \dot{-} m)$, each element a of $R(\mathcal{M})$ can be uniquely written as $a = p - q$, for $p, q \in M$ satisfying $p \sqcap q = 0$. The structure $R(\mathcal{M})$ admits a distributive lattice structure defined by $a \leq b$ exactly when $a \dot{-} b = 0$. The order $a \leq b$ is linear, exactly when $\mathcal{M}$ is a model of $\mathrm{Z}_0\mathrm{L}$.

Let $\mathcal{M}$ be a model of ZLN. Then $R(\mathcal{M})$ 'is' a linearly ordered integral domain. Its quotient field $Q(\mathcal{M})$ is embeddable in an ordered real closed field $\mathcal{R}$, with $a \dot{-} b$ defined by the maximum of $a - b$ and 0. Let $\mathcal{R}^{+0}$ be the substructure of nonnegative elements. Then $\mathcal{R}^{+0}$ is a model of ZLN. The theory of ordered real closed fields is complete, so $\mathcal{R}^{+0}$ is elementarily equivalent to $\mathbb{R}^{+0}$.

Proposition 3.9. *The theory* ZLN *is the universal fragment of the theory of* $\mathbb{R}^{+0}$.

Proof. $\mathbb{R}^{+0}$ is a model of ZLN. Each model of ZLN is embeddable in a model of the theory of $\mathbb{R}^{+0}$. □

In contrast to the case for $\mathrm{Z}_0\mathrm{D}$ versus $\mathbb{N}$, we have

Proposition 3.10. *The equational fragment of the theory of* $\mathbb{Q}^{+0}$ *equals the equational fragment of* ZLN.

Proof. $\mathbb{Q}^{+0}$ is a model of ZLN. Let $\mathcal{M}$ be the submodel of $(\mathbb{Q}^{+0})^\omega$ of all Cauchy sequences $\{a_n\}_n$. On $\mathcal{M}$, the subset $\{\,\{a_n\}_n \mid \lim_{n\to\infty} a_n = 0\,\}$ forms an ideal J. The quotient $\mathcal{M}/J$ is isomorphic to $\mathbb{R}^{+0}$. □

Is Z_0 the equational fragment of ZLN? We conjecture that it is.

4. Induction Schemata

The straightforward translation between PA^- and ZDL allows for immediate translations of induction schemata over PA^- into induction schemata over ZDL. We may extend ideas of induction schemata to proper subtheories. Here is a motivating example.

Proposition 4.1. *The model* $\mathbb{R}^{+0}$ *satisfies*

$$\forall x(\varphi(x) \to \varphi(x+1)) \wedge \exists x\varphi(x) \to \exists y\forall x(y \le x \to \varphi(x))$$

for all formulas $\varphi(x)$ *in which* y *does not occur free.*

Proof. The model $\mathbb{R}^{+0}$ satisfies

$$x \dot{-} y = z \leftrightarrow (x \le y \wedge z = 0) \vee (x = y + z))$$

This allows us to translate formulas over the language of $\mathbb{R}^{+0}$ to the language of ordered rings with the theory of the ordered field $\mathbb{R}$, while preserving derivability. We now easily check that the theory of $\mathbb{R}^{+0}$ satisfies quantifier elimination. For every allocation of the variables minus x, the set r for which $\varphi(r)$ holds, is a finite collection of open and closed intervals, permitting ∞ as open endpoint. In the case of $\varphi(x)$ satisfying the assumptions of the induction schema, the collection of intervals must include a nonempty one of the form (s, ∞) or $[s, \infty)$. □

5. Intuitionistic Z

So far we tried to avoid technical results that are less familiar to researchers in logic. Such attempts are naturally subjective. Part of our attempt meant that we limited ourselves to classical logic and model theory. In this final section we take a few steps into the area of intuitionistic logic and Kripke model theory. For an accessible exposition of intuitionistic first-order logic and Kripke models, see [5].

Before discussing an intuitionistic version of Z, we have to revisit our definitions of Section 2. We now introduce Z_0 as the set of axioms A1 through A11 rather than as a theory. Names like Z_0L or ZDN refer to the appropriate finite sets of axioms. The classical theories of the earlier section are now renamed Z_0L^c or ZDN^c. Corresponding first-order intuitionistic theories are named Z_0L^i or ZDN^i. And so on.

We call a first-order formula φ *geometric* when there are formulas σ and τ, built from atoms and $\top$ and $\bot$ using conjunction, disjunction and existential quantification only, and variables $\mathbf{x} = x_1, \dots, x_n$, such that φ equals

$$\forall \mathbf{x}(\sigma \to \tau)$$

We may call formulas geometric when they are geometric up to some obvious intuitionistically provable equivalence.

Let $\Gamma \cup \{\varphi\}$ be a set of geometric formulas. Then φ follows from Γ using classical logic, if and only if φ follows from Γ using intuitionistic logic. This implies that all formulas which we derived in Section 2, also follow in the intuitionistic case. We leave it as an exercise to give a direct intuitionistic proof that, over Z_0^i, terms $x \sqcap y$ and $x \sqcup y$ satisfy the equations for a distributive lattice. A geometrically axiomatizable theory is called *geometric*.

Let Γ be a set of geometric formulas. Then a Kripke model satisfies Γ^i, exactly when the node structures of the Kripke model are models of Γ^c. For example, the node structures of Kripke models of $\mathrm{Z_0L}^i$ are models of $Z_0\mathrm{L}^c$ (or: The Kripke models are locally $\mathrm{Z_0L}^c$); and so on. Geometric theory ZDL^i has enough strength to prove interesting results that are not expressible geometrically:

Proposition 5.1. *The theory* ZDL^i *satisfies the principle of decidable equality*

$$x = y \vee \neg\, x = y$$

Proof. Obviously, Z^i satisfies the geometric formula

$$(x + 1) \leq x \to \bot$$

and ZDL^i satisfies the geometric formula

$$x \leq y \vee y + 1 \leq x$$

Assume ZDL^i, and let a and b be elements. Then we have $(a \leq b \vee (b+1) \leq a) \wedge (b \leq a \vee (a+1) \leq b)$. So also $(a \leq b \wedge b \leq a) \vee \neg\, a = b$, and thus $a = b \vee \neg\, a = b$. ☐

Since ZDL is geometric, the decidable equality principle for ZDL^i is equivalent to the statement that all (classical) morphisms between models of ZDL^c are one-to-one. Proposition 5.1 also implies that the quantifier-free formula fragment of ZDL^i satisfies the rules of classical propositional logic.

We call a formula Π_2^0 when it is of the form $\forall \mathbf{x} \exists \mathbf{y} \varphi$, for some quantifier-free formula φ.

Proposition 5.2. *The theory* ZDL^c *is* Π_2^0*-conservative over* ZDL^i*.*

Proof. Let $\mathrm{ZDL}^c \vdash \forall \mathbf{x} \exists \mathbf{y} \varphi(\mathbf{xy})$ for some quantifier-free formula φ. Let α be a node of a Kripke model $\mathcal{K}$ of ZDL^i, and $\mathbf{a}$ be a string of elements of domain $D\alpha$ of node structure $\mathcal{D}_\alpha$. It suffices to show that $\alpha \Vdash \exists \mathbf{y}\varphi(\mathbf{ay})$. We have $\mathcal{D}_\alpha \models \mathrm{ZDL}^c$. So there are elements $\mathbf{b}$ in $D\alpha$ such that $\mathcal{D}_\alpha \models \varphi(\mathbf{ab})$. Since the propositional fragment of ZDL^i satisfies classical logic, also $\alpha \Vdash \varphi(\mathbf{ab})$. Thus $\alpha \Vdash \exists \mathbf{y}\varphi(\mathbf{ay})$. $\square$

A generalization to Π_2-conservativity, with bounded quantifications allowed where in Π_2^0 we only have quantifier-free formulas, is not valid in full generality. For example, let φ be the sentence

$$\forall x(\forall y(y \leq x \to \neg\, y^2 = x) \vee \exists y(y \leq x \wedge y^2 = x))$$

Then φ is a tautology over classical logic, so certainly derivable over ZDL^c. Let $\mathbb{Z}\Big[X, X\sqrt{2}\Big]$ be the linearly ordered ring with $n \leq X$ for all integers n. The substructure $\mathbb{Z}\Big[X, X\sqrt{2}\Big]^+$ of nonnegative polynomials uniquely determines a model of ZDL^c. Similarly construct submodel $\mathbb{Z}[X]^+$ of $\mathbb{Z}\Big[X, X\sqrt{2}\Big]^+$. In the Kripke model

$$\begin{array}{l} \beta \bullet \ \mathcal{D}_\beta = \mathbb{Z}\Big[X, X\sqrt{2}\Big]^+ \\ \ \ \ \uparrow \\ \alpha \bullet \ \mathcal{D}_\alpha = \mathbb{Z}[X]^+ \end{array}$$

of ZDL^i, let a be the element $2X^2 \in D\alpha$. Then $\alpha \nVdash \forall y(y \leq a \to \neg\, y^2 = a) \vee \exists y(y \leq a \wedge y^2 = a)$. So φ is not derivable over ZDL^i.

References

[1] Chang, C.C.; H.J. Keisler. *Model Theory,* third edition. Studies in Logic and the Foundations of Mathematics, Vol. 73, North-Holland, Elsevier Science, 1990.

[2] Cohn, Paul M. *Universal Algebra,* revised edition. Mathematics and its Applications, Vol. 6, Reidel, Dordrecht, 1981.

[3] Grätzer, George. *Universal Algebra.* D. Van Nostrand, Princeton, 1968.

[4] Kaye, Richard. **Models of Peano Arithmetic.** Oxford Logic Guides, Vol. 15, the Clarendon Press, Oxford University Press, New York, 1991.

[5] Troelstra, Anne S.; Dirk van Dalen. **Constructivism in Mathematics. An Introduction,** Vol. 1. Studies in Logic and the Foundations of Mathematics, Vol. 121, North-Holland, Amsterdam 1988.

Institute of Mathematics, University of Silesia, Bankowa 14, 40-007 Katowice, Poland

E-mail address: `polacik@us.edu.pl`

Department of Mathematics, Statistics and Computer Science, Marquette University, P.O. Box 1881, Milwaukee WI 53201, U.S.A.

E-mail address: `wimr@mscs.mu.edu`