Independence results for variants of sharply bounded induction

Leszek Aleksander Kołodziejczyk *

February 19, 2011

Abstract

The theory T^0_2, axiomatized by the induction scheme for sharply bounded formulas in Buss' original language of bounded arithmetic (with $\lfloor x/2 \rfloor$ but not $\lfloor x/2^y \rfloor$), has recently been unconditionally separated from full bounded arithmetic S_2. The method used to prove the separation is reminiscent of those known from the study of open induction.

We make the connection to open induction explicit, showing that models of T^0_2 can be built using a "nonstandard variant" of Wilkie's well-known technique for building models of $IOpen$. This makes it possible to transfer many results and methods from open to sharply bounded induction with relative ease.

We provide two applications: (i) the Shepherdson model of $IOpen$ can be embedded into a model of T^0_2, which immediately implies some independence results for T^0_2; (ii) T^0_2 extended by an axiom which roughly states that every number has a least 1 bit in its binary notation, while significantly stronger than plain T^0_2, does not prove the infinity of primes.

1 Introduction

Buss' bounded arithmetic theory S_2 has a rich structure of subtheories, all believed to be proper. However, only a few very weak subtheories have actu-

*Institute of Mathematics, University of Warsaw, Banacha 2, 02-097 Warszawa, Poland, lak@mimuw.edu.pl. Partially supported by grant N N201 382234 of the Polish Ministry of Science and Higher Education.

ally been separated from S_2 without using unproved assumptions. Clearly, this state of affairs is at least in part caused by the lack of appropriately strong methods.

It seems that at present there are essentially three methods which prove some unconditional separations between S_2 and its fragments. Two of these are complexity-theoretic in character.

Firstly, the well-known lower bounds for circuit classes AC^0 and $AC^0(p)$ immediately imply independence results for associated theories V^0 and $V^0(p)$ (see [CN10]), and the results for V^0 can be improved using subtler variants of lower bound techniques [BIK+92]. V^0 and $V^0(p)$ are slightly odd from an arithmetical point of view, as they do not prove the totality of multiplication. Lower bounds for circuit classes which contain multiplication are likely to require a significant conceptual breakthrough in complexity theory [RR97].

The second method works for theories which do have total multiplication, but otherwise rather little "$\forall\exists$ content". The idea is to come up with a "somewhat complex" function f and then show, either by proof theory or by building well-chosen substructures of models, that some theories cannot prove f total. In practice, f is not particularly complex at all, say $f(x) = \lfloor x/3 \rfloor$. The method works for the sharply bounded polynomial induction scheme, or S^0_2, in a variety of languages (the first proof of this kind is in [Tak90] and the simplest in [Joh98]), and for theories such as $\hat{\Sigma}^b_1$-$IND^{|x|_4}$ (induction for strict Σ^b_1 formulas restricted to the range of the fourth iteration of the logarithm; [Pol00]).

The third method is to build models of arithmetic out of elements of suitable ordered fields. This approach has been used with much success in the study of open (quantifier-free) induction, beginning with Wilkie's influential paper [Wil78]. However, it has only recently been applied to induction for formulas with quantifiers. Boughattas and Ressayre [BR10] showed that Σ^b_1 induction restricted to the range of $|x|_3$ does not prove that powers of 2 have no non-trivial odd divisors. Afterwards, [BK10] used their techniques to prove a similar independence result for the full sharply bounded induction scheme, T^0_2, formulated in Buss' original language of bounded arithmetic, with the $\lfloor x/2 \rfloor$ symbol but without $\lfloor x/2^y \rfloor$. This result stands in stark contrast to a theorem of [Jeř06] showing that sharply bounded induction with $\lfloor x/2^y \rfloor$ in the language is quite strong.

For extremely weak theories, open induction-style techniques can be used to build models with rather crude pathologies, such as rational presentations of $\sqrt{2}$ or the strange powers of 2 from [BR10] and [BK10]. However, the

methods also work for somewhat stronger theories, leading to unprovability results for statements such as infinity of primes (e.g. [Smi93]). In the area of fragments of S_2, the power of open induction-style techniques is not yet fully understood and seems to deserve further study.

We continue this study in the present paper, emphasizing the case of sharply bounded induction and its extensions. Our initial aim is build models of Buss' T_2^0 by a procedure almost identical to the one devised for open induction by Wilkie. The only difference is that where [Wil78] uses the standard integers, we need to use a nonstandard initial segment of a model of PA (which leads to some technical problems). Having a construction modelled very closely upon Wilkie's has an important benefit: it becomes reasonably easy to transfer results and methods known from work on open induction to the sharply bounded setting. We provide two applications.

Firstly, we show that Shepherdson's model, a well-known extremely pathological model of open induction, can be extended to a model of T_2^0. This immediately yields a number of independence results for T_2^0 (some already known), and provides further insight into a major source of weakness of T_2^0: the theory is almost completely unable to reason about numbers viewed as sequences of bits.

It is then quite natural to ask whether Wilkie-style methods can work for theories which know a bit more about bits. We provide a positive answer in the case of one such theory: T_2^0 extended by an axiom saying roughly that every number has a least 1 bit in its binary notation. This extension is strong enough to rule out a rational $\sqrt{2}$ or odd divisors of powers of 2. Nevertheless, we are able to show that it does not prove the infinity of primes.

The structure of the paper is as follows. Section 2 is preliminary. Section 3 recalls the definition of open induction and outlines Wilkie's method of building models. Section 4 explains how a "nonstandard variant" of this method can yield models of T_2^0. Section 5 contains the result on Shepherdson's model, and Section 6 is about T_2^0 extended by the axiom on least 1 bits. We conclude with some remarks and a discussion of open problems in Section 7.

2 Preliminaries

Although we expect that the reader has some familiarity with the main theories and concepts of bounded arithmetic (as described in e.g. [HP93], [Kra95] or [Bus98]), we actually use rather little background knowledge

from the area. The relevant knowledge includes: the language $L_{BA} = \{0, 1, \leq, +, \cdot, |x|, \#, \lfloor x/2 \rfloor\}$, where $|x|$ is $\lfloor \log(x+1) \rfloor$ (length in binary) and $x\#y = 2^{|x|\cdot|y|}$; the theory BASIC; the notions of a sharply bounded quantifier (i.e. one bounded by $|t|$ for some term t) and Σ_0^b formula (one in which all quantifiers are sharply bounded); the induction schemes IND and PIND, where IND is as usual and the induction step in PIND is $\varphi(\lfloor x/2 \rfloor) \Rightarrow \varphi(x)$ instead of $\varphi(x) \Rightarrow \varphi(x+1)$; the theories T_2^0 (= BASIC + Σ_0^b-IND) and S_2^0 (= BASIC + Σ_0^b-PIND). Σ_n^b, T_2^n and S_2^n for $n > 0$ will only be mentioned in passing.

We also use some basic facts on nonstandard models of Peano Arithmetic (to be found in the first few chapters of [Kay91]) and real closed fields (see e.g. Section 3.3 of [Mar02]).

Notational and terminological conventions: L_{PA} is the usual language of Peano Arithmetic PA. For a model $\mathcal{N}$, $L_{\mathcal{N}}$ denotes the extension of the language, be it L_{PA} or L_{BA}, by constants for all elements of $\mathcal{N}$. If b is an element of $\mathcal{N}$, then $b^{\mathbb{N}}$ stands for the cut in $\mathcal{N}$ determined by the standard powers of b. If J is a cut in $\mathcal{N}$, $\log J$ is the initial segment $\{i : 2^i \in J\}$ (which is a cut if J is closed under $+$). On the other hand, the notation bJ is used only for J closed under $\cdot$ and $b \in J$: it denotes the ideal in J generated by b, which is not a cut unless $b = 1$. The set defined by the formula φ in $\mathcal{N}$ is $\varphi^{\mathcal{N}}$. In contrast, we write $\mathrm{card}_{\mathcal{N}}(X)$ or $\lfloor x \rfloor_{\mathcal{N}}$ ($\mathcal{N}$ in the subscript) for cardinalities or integral parts evaluated in $\mathcal{N}$, so as to avoid confusion with $b^{\mathbb{N}}$.

If $\mathcal{N}$ is a model and f is a function, $\mathcal{N}'$ is some other model, but f' is the derivative of f. $\mathcal{N} \preccurlyeq_J \mathcal{N}'$ means: $\mathcal{N}'$ is an elementary extension of $\mathcal{N}$ not containing any new elements below the cut J.

A bar, as in $\bar{x}$, indicates a tuple; rcl stands for real closure, acl for algebraic closure. We write $||x||$ for absolute value, to distinguish it from the $|x|$ symbol of L_{BA}.

In any model of BASIC, a power of 2 is an element satisfying the quantifier-free formula $x = \lfloor x/2 \rfloor \# 1$. The relation $y = 2^x$ also has a quantifier-free definition: $y = \lfloor y/2 \rfloor \# 1 \wedge |y| = x + 1$.

There is an annoying discrepancy between conventions on models of reasonably strong arithmetic and models of very weak theories studied by algebraic means. The latter are often viewed as discrete ordered rings, the former as discrete ordered semirings. We largely ignore this issue, and trust the reader's common sense to correctly interpret phrases such as "the ring R satisfies T_2^0" and the like.

3 Open induction: two old results and a method

Open induction, *IOpen*, is the theory consisting of axioms for discrete ordered rings (or non-negative parts thereof) and the induction scheme for open (= quantifier-free) formulas of L_{PA}.

The main aim of this section is to review a broad-purpose technique for constructing models of *IOpen*, due to Wilkie. However, we first recall a simple but important criterion given by Shepherdson.

Theorem 3.1. *[She64] A discrete ordered ring R satisfies IOpen iff it is an integer part of its real closure, i.e. iff for every $\alpha \in \mathrm{rcl}(R)$ there is $x \in R$ such that $||x - \alpha||$ is finite.*

Note that nothing will change if we write "$||x - \alpha|| < 1$" instead of "$||x - \alpha||$ is finite".

A $\mathbb{Z}$*-ring* is a discrete ordered ring in which division with remainder by every (non-zero) element of $\mathbb{Z}$ is possible. Wilkie's technique was first applied to prove the following theorem:

Theorem 3.2. *[Wil78] Every $\mathbb{Z}$-ring can be extended to a model of IOpen.*

The construction used to prove the theorem plays a crucial role in the rest of the paper, so we sketch the proof.

The first step is to embed a given countable $\mathbb{Z}$-ring R in a suitably saturated, say $\aleph_1$-saturated, real closed field F (oddly, the saturation assumption is missing from the original paper [Wil78]). The extension satisfying *IOpen* is the union of a chain $R \subseteq R_1 \subseteq R_2 \ldots$ of discrete ordered subrings of F, where each R_{n+1} is obtained by adding to R_n a witness for an instance of open induction—i.e. an element finitely close to some $\alpha \in \mathrm{rcl}(R_n)$.

The way to do this is to find $x \in F$ which is finitely close to α but not infinitesimally close to any element of $\mathrm{acl}(R_n)$. The existence of x is guaranteed by the $\aleph_1$-saturation of F. It then follows from the $\mathbb{Z}$-ring properties of R_n that all nonconstant polynomials from $R_n[X]$ have infinite values at x, which means that $x, x/2, x/3, x/4 \ldots$ (or, if one prefers, $x, (x-1)/2, (x-1)/3, (x-3)/4 \ldots$ or anything of the kind) can be safely added to R_n without losing discreteness. This gives R_{n+1}.

The basic idea behind this construction has many applications. By interweaving it with other constructions and/or by carefully choosing the remainders $\bmod 2$, $\bmod 3$ etc. of newly added elements, it is possible to build a

great variety of "pathological" models of $IOpen$ and its extensions, and to obtain a number of interesting independence results. See e.g. [vdD80], [Ada87], [MM89], [Smi93], [BO96] for a sample of such applications. A particularly detailed study of Wilkie's technique is carried out in [MM89], where variants of the construction are used to show that $IOpen$ puts rather few limitations on the behaviour of nonstandard primes.

4 Transferring the method

We will now describe how to transfer Wilkie's construction to a nonstandard setting where $\mathbb{Z}$ is replaced by a nonstandard cut in a model of arithmetic and the finite/infinite distinction is replaced by bounded by the cut/above the cut. If care is taken, the new setting makes it possible to construct pathological models which satisfy not just $IOpen$, but also T_2^0.

Let $\mathcal{N}_0 \models PA$ be countable and nonstandard, and let $J \subseteq_e \mathcal{N}_0$ be a cut of the form $a^{\mathbb{N}}$ for some $a > \mathbb{N}$. The elements of J should be thought of as "small" or "logarithmic". The only really important feature required of J is that it should be closed under $+$ and $\cdot$, but not under 2^x.

Throughout the rest of paper, J *will remain fixed* and all models of arithmetic we consider will contain J as an initial segment. On the other hand, though $\mathcal{N}_0$ *also remains fixed*, we will work with various $\mathcal{N} \models PA$ such that $\mathcal{N} \succcurlyeq_J \mathcal{N}_0$.

Definition 4.1. Let $\mathcal{N} \succcurlyeq_J \mathcal{N}_0$. A discrete ordered ring $R \subseteq \mathrm{rcl}(\mathcal{N})$ is a *J-ring* if:

(a) $R \supseteq J$,

(b) R is closed under division with remainder by elements of J, i.e. for every $x \in R$ and $0 \neq j \in J$, there exists a (necessarily unique) $q \in R$ such that $x/j - 1 < q \leq x/j$ (this q is denoted by $\lfloor x/j \rfloor_R$),

(c) R contains $\{2^j : j \in J\}$ as a cofinal subset.

The idea of transferring Wilkie-style methods to nonstandard models of arithmetic is not entirely new: Boughattas and Ressayre [BR10] (followed by [BK10]) use the concept of a *log-euclidean chain*, a kind of stratified structure coded in $\mathcal{N}$ from which a J-ring in our sense can be recovered. The main difference between their approach and ours is that we do not demand that

the ring itself (as opposed to its elements) be coded in $\mathcal{N}$ in any way. On the one hand, this precludes applications to some theories, such as the very restricted Σ^b_1 and Σ^b_2 induction schemes considered in [BR10]. On the other hand, it provides much more flexibility when working with sharply bounded induction and some of its extensions.

Condition (c) in the definition of a J-ring, which states that the ring is "well-positioned", does not have an analogue for $\mathbb{Z}$-rings and could be placed outside the definition. Our reason for including it is that J-rings satisfying (c) have a natural expansion to structures for Buss' language satisfying BASIC: $\lfloor x/2 \rfloor$ is determined by the J-ring structure, $|x|$ is defined to be $|\lfloor x \rfloor_{\mathcal{N}}|$ and $x\#y$ is $2^{|x|\cdot|y|}$ (the closure of R under $|x|$ and $x\#y$ is then guaranteed by (c)). Perhaps more strikingly, such "well-positioned" rings have a decent chance of satisfying T^0_2:

Lemma 4.2. *Let $\mathcal{N} \succcurlyeq_J \mathcal{N}_0$. Let $R \subseteq \mathrm{rcl}(\mathcal{N})$ be a J-ring. If $R \models IOpen$, then $R \models T^0_2$.*

Proof. It is straightforward though tedious to verify that all J-rings satisfy BASIC. The proof that a J-ring R satisfying $IOpen$ also satisfies the Σ^b_0 induction scheme is based on the following claim, which states roughly that if remainders modulo some finite power of 2 are taken into account, then the set defined in R by a sharply bounded formula is the union of "logarithmically many" intervals with endpoints in $\mathrm{rcl}(R)$.

Claim. Let $\varphi(x, \bar{q})$ be a Σ^b_0 formula, where $\bar{q}$ is a tuple of parameters from R. Let n be the nesting depth of $\lfloor \cdot/2 \rfloor$ in φ. For every $m \in \mathbb{N}$ and $r = 0, 1, \ldots, 2^n - 1$ there exists $M \in \mathbb{N}$ and a set U^r of the form

$$\bigcup_{j<a^M} I^r_j,$$

where for each r the sets I^r_j are disjoint intervals in $\mathrm{rcl}(\mathcal{N})$ with endpoints from $\mathrm{rcl}(J \cup \{2^j : j \in J\} \cup \{\bar{q}\})$, such that for every $x \in \mathrm{rcl}(\mathcal{N})$, $x < 2^{a^m}$: if $x \in R$ and $(x \bmod 2^n)_R = r$, then $R \models \varphi(x, \bar{q})$ exactly if $x \in U^r$.

The proof of the claim is almost identical to that of Lemma 3.1 in [BK10] (a very similar result was proved for the standard model in [Man91]). We provide a sketch (see below) and refer to [BK10] for the details.

Once we have the claim, the argument is completed as follows. Assume φ is sharply bounded and $R \models \varphi(0, \bar{q})$ but $R \models \neg\varphi(b, \bar{q})$. Consider two cases. The first is that for some $j \in J$, $R \models \neg\varphi(j, \bar{q})$ or $R \models \varphi(b - j, \bar{q})$. If, say,

$R \models \varphi(b-j, \bar{q})$, then use the claim to express $R \models \varphi(b-z, \bar{q})$ for $0 \leq z \leq j$ by an $L_{\mathcal{N}}$-formula $\psi(z)$. $\mathcal{N} \models \neg\psi(0) \wedge \psi(j)$, so induction for $\neg\psi$ in $\mathcal{N}$ finds an element witnessing induction for φ in R.

The second case is that for all $j \in J$, $R \models \varphi(j, \bar{q})$ and $R \models \neg\varphi(b-j, \bar{q})$. Consider the set $U^0 = \bigcup_{j<a^M} I^0_j$ given by the claim. Note that $[0,b]_{\mathrm{rcl}(\mathcal{N})} \setminus U^0$ has the form $\bigcup_{l<a^M} I^*_l$ where the I^*_l are intervals disjoint from the I^0_j. Say that an interval is large if its length is at least 2^n+1, where n is the nesting depth of $\lfloor \cdot/2 \rfloor$ in φ. By our case assumption, there is at least one large I^0_j below some large I^*_l. Among all pairs of large I^0_j and I^*_l such that $I^0_j < I^*_l$, find one for which the distance between the two intervals is minimal. This minimal distance has to be bounded by J, as there are at most $2a^M$ intervals between I^0_j and I^*_l, and none of them is large.

Since the right endpoint of I^0_j is in $\mathrm{rcl}(R)$, and $R \models IOpen$, by the remark after Theorem 3.1 there is an element c of $R \cap I^0_j$, divisible by 2^n in R, at distance at most 2^n from the right endpoint of I^0_j. Similarly, there is an element d of $R \cap I^*_l$, divisible by 2^n in R, at distance at most 2^n from the left endpoint of I^*_l. We have $R \models \varphi(c, \bar{q})$, $R \models \neg\varphi(d, \bar{q})$ and $||d-c|| < J$, so, as in the first case, induction in $\mathcal{N}$ finds an element witnessing induction for φ in R.

Proof of claim — sketch. The argument is by induction on the complexity of a Σ^b_0 formula, but most of the work is in the base step. The inductive steps for $\neg$, $\vee$ and sharply bounded $\exists$ are trivial, while the steps for $\wedge$ and $\forall$ rely on the fact that the intersection of a union of j intervals and a union of l intervals is a union of at most $j+l$ intervals.

The base step, for an atomic formula $t(x, \bar{q}) \leq t'(x, \bar{q})$, uses the following observation. Let $t_1, \ldots, t_s$ be a list of all the subterms of t and t'. Assume that the values of $|t_1(x, \bar{q})|, \ldots, |t_s(x, \bar{q})|$ are known to be $j_1, \ldots, j_s$, respectively. Then with some additional information on the remainders of x modulo powers of 2 (it turns out that the necessary information is $x \bmod 2^n$), we can inductively rewrite $t_1, \ldots, t_s$ as L_{PA}-terms with parameters $\bar{q}, j_i$ and $2^{j_i \cdot j_k}$. The steps for $+$ and $\cdot$ are obvious, $|t_i|$ is j_i, $t_i \# t_k$ is $2^{j_i \cdot j_k}$ and $\lfloor t_i/2 \rfloor$ is $t_i/2$ or $t_i/2 - 1/2$ depending on the parity of t_i. So, for a fixed value $r = (x \bmod 2^n)$ and fixed $j_1, \ldots, j_s$, the set defined by $t(x, \bar{q}) \leq t'(x, \bar{q})$ is a finite union of intervals. Existentially quantifying over $j_1, \ldots, j_s$ increases the number of intervals by a factor of at most a^M for some $M \in \mathbb{N}$. $\square$

To be able to use Lemma 4.2, we have to know that J-rings can be extended by adding witnesses for instances of $IOpen$:

Lemma 4.3. *Assume $\mathcal{N} \succcurlyeq_J \mathcal{N}_0$ is countable and R is a J-ring contained in* $\mathrm{rcl}(\mathcal{N})$. *Let $\alpha \in \mathrm{rcl}(R)$. Then there exists a countable $\mathcal{N}' \succcurlyeq_J \mathcal{N}$ and a J-ring $R' \supseteq R$ contained in* $\mathrm{rcl}(\mathcal{N}')$ *which has an element x with $||x - \alpha|| < 1$.*

Most of the proof of Lemma 4.3 is obtained from the proof of Theorem 3.2 simply by changing "finite" to "bounded by J" in almost all contexts. The one issue that requires some care is finding an element close to some $\alpha \in \mathrm{rcl}(R)$ but not too close to $\mathrm{acl}(R)$. In Theorem 3.2, such an element is given by the saturation properties of the underlying real closed field F. However, naïve attempts to embed $\mathcal{N}$ and R in e.g. some $\aleph_1$-saturated structure are likely to cause the disruption of J (a problem which does not arise with $\mathbb{Z}$), whereas the idea of a model of arithmetic "saturated with respect to a nonstandard initial segment" does not seem to make sense.

These difficulties can be resolved by extending the ambient model of PA. We isolate the relevant part of the proof into a separate lemma:

Lemma 4.4. *Assume $\mathcal{N} \succcurlyeq_J \mathcal{N}_0$ is countable and R is a J-ring contained in* $\mathrm{rcl}(\mathcal{N})$. *Let $\alpha \in \mathrm{rcl}(\mathcal{N})$ be such that for every $r \in R$, $||\alpha - r|| > J$.*

Then there exists a countable $\mathcal{N}' \succcurlyeq_J \mathcal{N}$ and an element $x \in \mathrm{rcl}(\mathcal{N}')$ such that $||x - \alpha|| < 1$, but for every $\beta \in \mathrm{acl}(\mathcal{N})$ there exists $j \in J$ such that $||x - \beta|| > 1/j$.

Proof of Lemma 4.4. We use a variation on a standard theme in the study of models of PA: elementary extensions which preserve some given initial segment (for a plethora of such constructions, see Chapters 2 and 3 of [KS06]). The simplest kind of extension of $\mathcal{N}$ — called, incidentally, a *simple* extension — is the closure of $\mathcal{N}$ and a single element $c \notin \mathcal{N}$ under Skolem functions (recall that PA has definable Skolem functions). The usual way to specify c is to construct the type over $\mathcal{N}$ it realizes, $p(z)$, as an intersection of large definable subsets $Z_0 \supseteq Z_1 \supseteq \ldots$ of $\mathcal{N}$. The exact notion of "large" is tailored to one's specific needs. In our case, we fix a number $d \in \mathcal{N} \setminus J$ and say that a set Z is large if $\mathrm{card}_{\mathcal{N}}(Z \cap [0, d)) \geq d/j$ for some $j \in J$.

The sequence of sets $Z_0, Z_1, \ldots$ is built as follows. Enumerate all $L_{\mathcal{N}}$-formulas with one free variable as $\varphi_0(z), \varphi_1(z), \ldots$. Let Z_0 be $[0, d)$. Given large Z_n, consider $\varphi_n(v)$ and let Z_{n+1} be some large definable set contained in either $Z_n \cap \varphi_n^{\mathcal{N}}$ or $Z_n \cap \neg\varphi_n^{\mathcal{N}}$ (at least one of the two must be large) satisfying an additional condition: if φ_n happens to be $t(z) < j$ for some $j \in J$ and Skolem term t, then Z_{n+1} should either be disjoint from $t^{-1}([0, j))$ or contained in $t^{-1}(\{l\})$ for some specific $l = 0, 1, \ldots, j - 1$. This condition

can always be satisfied: by an obvious counting argument, if $Z_n \cap t^{-1}([0,j))$ is large, then so is $t^{-1}(\{l\})$ for some $l < j$.

As mentioned above, the type $p(z)$ is the intersection of the Z_ns, or more formally:

$$p(z) = \{\varphi(z) : \exists n \in \mathbb{N}\,(Z_n \subseteq \varphi^{\mathcal{N}})\}.$$

Let $\mathcal{N}'$ be the Skolem closure of $\mathcal{N} \cup \{c\}$ for some c realizing $p(z)$. $\mathcal{N}'$ has the following properties:

(i) $\mathcal{N}' \succcurlyeq_J \mathcal{N}$,

(ii) $\mathcal{N} \setminus J$ is downwards cofinal in $\mathcal{N}' \setminus J$.

Property (i) follows from our choice of the type $p(z)$: every element of $\mathcal{N}'$ is of the form $t(c)$ for some Skolem term t, and if $t(c) < j$ for some $j \in J$, p guarantees that $t(c) = l$ for some $l \in J$. Property (ii) holds for general reasons (see the remark after the statement of Lemma 6.3), but perhaps the simplest argument is this: if there was a new element strictly between J and $\mathcal{N} \setminus J$, then by the closure of J under addition some new power of 2 would also have to be there. It would have to be 2^l for some l bounded by J; however, there are no new elements bounded by J.

Now take $x = \alpha - (c/d) \in \mathrm{rcl}(\mathcal{N}')$. We claim that x is as required. Clearly, $||x - \alpha|| < 1$. Assume that for some $\beta \in \mathrm{acl}(\mathcal{N})$, $||x - \beta|| \leq 1/j$ for all $j \in J$. We can write an $L_{\mathcal{N}'}$-formula

$$\varphi(w) = ||(\alpha - (c/d)) - \beta|| \leq 1/w.$$

Overspill for φ gives some $b \in \mathcal{N}' \setminus J$ such that $||(\alpha - (c/d)) - \beta|| \leq 1/b$. By (ii), we can assume that b actually belongs to $\mathcal{N} \setminus J$.

Consider the $L_{\mathcal{N}}$-formula

$$\psi(z) = ||(\alpha - (z/d)) - \beta|| \leq 1/b.$$

Since $\psi(c)$ holds, $\psi(z)$ must belong to $p(z)$ and thus $\psi^{\mathcal{N}}$ must contain some Z_n. But that is impossible: Z_n is large, while $\psi^{\mathcal{N}}$ has no more than $(2d+1)/b$ elements. □

Proof of Lemma 4.3 from Lemma 4.4. Let $\mathcal{N}$, R and α be given. We may assume that $||\alpha - r|| > J$ for all $r \in R$; otherwise, since $J \subseteq R$, there already is an element of R at distance less than 1 from α. So, take $\mathcal{N}'$ and x as provided by Lemma 4.4.

We claim that for every non-constant polynomial $f(X) \in R[X]$, the value $||f(x)||$ is above J. To see this, present f as

$$f(X) = b(X - \beta_1) \dots (X - \beta_n),$$

where $b \in R$, and $\beta_1, \dots, \beta_n \in \mathrm{acl}(R)$ are all the roots of f. Now, $||b|| \geq 1$, and there is some $j \in J$ such that $||x - \beta_i|| > 1/j$ for each i; thus, if $||f(x)|| < J$, then $||b|| < J$ and each $||x - \beta_i|| < J$ (since J is closed under multiplication). We therefore have:

$$||nbx - b\sum_{i=1}^{n} \beta_i|| < J.$$

However, $-b\sum_{i=1}^{n} \beta_i$ lies in R, being a coefficient of f. Also, since R is a J-ring, $b \in R$ and $||b|| < J$ actually implies $\pm b \in J$ and $\pm nb \in J$. But this means that x, and hence α, is at distance bounded by J from an element of R, namely

$$\lfloor b\sum_{i=1}^{n} \beta_i/nb \rfloor_R.$$

So, $||f(x)||$ must be greater than J and the claim is proved.

By the claim, we know $R[x]$ is a discrete ordered ring. Since we are looking for a J-ring and not just a discrete ordered ring, we must decide what the remainders of x modulo elements of J should be. At this point, we may choose the simplest option: let x be divisible by all non-zero elements of J. Hence, we let R' be $R[\{x/j : 0 \neq j \in J\}]$. Clearly, R is cofinal in R'. It also follows easily from the claim and the closure of J under multiplication that R' is a discrete ordered ring; therefore, it is a J-ring. □

Remark. In the above proof, we made the new element x divisible by all elements of J, but in various contexts other choices of x mod j for $j \in J$ are needed. In general, any internally consistent choice of remainders would be possible, where an "internally consistent" choice can be identified with an element of the inverse limit

$$\varprojlim_{j \in J \setminus \{0\}} R/jR.$$

The situation here is not quite as simple as in the case of $\mathbb{Z}$-rings, because the choices of remainders modulo different primes are not independent. For

example, if $p_1, \ldots, p_k$ are the first k primes where k is small nonstandard, then a given choice of remainders $\bmod p_1, \ldots, \bmod p_k$ might not correspond to any residue $\bmod (p_1 \cdot \ldots \cdot p_k)$ present in J. Nevertheless, quite a bit of freedom is still available. We make use of it in Section 6.

The work of this section can be summarized as follows:

Theorem 4.5. *Every countable J-ring can be extended to a model of T_2^0.*

Proof. Let R be a countable J-ring. For Skolem-Löwenheim reasons, R is contained in the real closure of a countable $\mathcal{N} \succcurlyeq_J \mathcal{N}_0$. Iterating Lemma 4.3, build a chain $R \subseteq R_1 \subseteq R_2 \ldots$ of J-rings and an associated chain $\mathcal{N} \preccurlyeq_J \mathcal{N}_1 \preccurlyeq_J \mathcal{N}_2 \ldots$ of models so that $R_\infty = \bigcup_{n\in\mathbb{N}} R_n$ is an integer part of its real closure and thus, by Theorem 3.1, a model of $IOpen$. R_∞ is a J-ring contained in the real closure of $\mathcal{N}_\infty = \bigcup_{n\in\mathbb{N}} \mathcal{N}_n$, and $\mathcal{N}_\infty \succcurlyeq_J \mathcal{N} \succcurlyeq_J \mathcal{N}_0$, so we can invoke Lemma 4.2 and conclude that $R_\infty \models T_2^0$. □

5 The Shepherdson model

The *Shepherdson model* M_{Shep} for $IOpen$ consists of sums of the form

$$\sum_{k=0}^{n} \alpha_k X^{k/m},$$

where $m > 0$ is a natural number, $\alpha_k \in \text{rcl}(\mathbb{Q})$ for each k, and $\alpha_0 \in \mathbb{Z}$. The ordering is defined by setting $X > \mathbb{Z}$.

Shepherdson showed in [She64] that M_{Shep} is a recursive model of $IOpen$, which implies that Tennenbaum's Theorem fails for $IOpen$. M_{Shep} also witnesses a number of interesting independence results for $IOpen$: e.g., there are no nonstandard primes, $\sqrt{2}$ is rational (as $(\sqrt{2}X)^2 = 2X^2$) and Fermat's Last Theorem fails already for exponent 3 (as $(\sqrt[3]{2}X)^3 = X^3 + X^3$).

Our aim now is to prove:

Theorem 5.1. *M_{Shep} can be extended to a model of T_2^0.*

Proof. Most of the work has already been done in the previous section. All that remains is to show that M_{Shep} can be embedded in a J-ring. Consider the structure R_{Shep} contained in $\text{rcl}(\mathcal{N}_0)$ and consisting of sums of the form

$$\sum_{k=1}^{n} \alpha_k 2^{j_k}, \tag{1}$$

where for each k: $j_k \in J$, $0 \neq \alpha_k \in \mathrm{rcl}(J)$, and additionally $\pm\alpha_k \in J$ if $j_k \in \log J$.

Clearly, R_{Shep} is a ring, inherits an order from $\mathrm{rcl}(\mathcal{N}_0)$, embeds M_{Shep} (send X to any 2^j such that $j \in J \setminus \log J$) and satisfies conditions (a) and (c) from Definition 4.1. We claim that it actually is a J-ring, so we have to show discreteness and condition (b).

Discreteness: write an element r of R_{Shep} in the form (1) in such a way that $j_1 < j_2 \ldots < j_n$ and for each k, $2^{j_{k+1}} > j2^{j_k}$ for all $j \in J$. This can be done by joining all terms within a J-bounded factor of each other into one (note that the coefficients α_k and their reciprocals are bounded by J). It is now clear that if $j_n > \log J$, then also $||r|| > J$, while if $j_n \in \log J$ (hence necessarily $n = 1$), then $\pm r \in J$. In either case, $r \notin (0, 1)$.

Condition (b): write $r \in R_{\mathrm{Shep}}$ in the form (1) exactly as above. Consider $0 \neq j \in J$. If $j_1 > \log J$, then $r/j \in R_{\mathrm{Shep}}$. Otherwise, the integer part of r/j in R_{Shep} is:

$$\lfloor(\alpha_1 2^{j_1})/j\rfloor_{\mathcal{N}_0} + \sum_{k=2}^{n}(\alpha_k/j)2^{j_k}.$$

□

Corollary 5.2. *T_2^0 does not prove:*

(i) a power of 2 is not divisible by 3,

(ii) $\sqrt{2}$ is irrational,

(iii) $(x > 0 \wedge y > 0) \Rightarrow x^3 + y^3 \neq z^3$.

Proof. Items (ii) and (iii) follow immediately from Theorem 5.1, while (i) follows from its proof: if $j \in J \setminus \log J$, then $2^j/3$ is an element of the J-ring R_{Shep}. □

The independence of "a power of 2 has no non-trivial odd divisors" from (a slight strengthening of) T_2^0 was the main result of [BK10]. However, the method used there does not seem to make 3 divide a power of 2: the divisors it gives are nonstandard and rather large.

The independence of "$\sqrt{2}$ is irrational" from T_2^0 was first proved by Boughattas (unpublished).

6 An extension of sharply bounded induction

Theorem 5.1 and Corollary 5.2 reveal that T_2^0 is a pathologically weak theory. In particular, its understanding of numbers as sequences of bits is embarassingly poor. T_2^0 can define the function $\lfloor x/2^y \rfloor$ and thus also the i-th bit function $bit(x,i) = \lfloor x/2^i \rfloor - 2\lfloor x/2^{i+1} \rfloor$, but it does not even know that every (non-zero) number has a least 1 bit. For example, in any J-ring extending the structure R_{Shep} from the proof of Theorem 5.1, the element $2^j/3$ for $j > \log J$ will have 0 bits at all positions $j - l$ for $j \geq l > \log J$ and alternating 0 and 1 bits at higher positions, up to $j - 2$.

This leads to the natural question whether *IOpen*-style methods could yield independence results for theories which are not quite as weak. We take a first step in this direction by considering T_2^0 extended by the following axiom *LeastBit*:

"for every $x \neq 0$, there is a smallest power of 2 which does not divide x."

LeastBit is, of course, provable from the Σ_0^b minimum principle or even LIND for Σ_0^b formulas if $\lfloor x/2^y \rfloor$ is in the language. It is conceivable that over T_2^0, *LeastBit* is strictly stronger than just "every non-zero number has a least 1 bit". On the other hand, *LeastBit* is equivalent in extremely weak theories (certainly in BASIC) to the axiom that every number can be presented as $q2^j$ where q is odd.

A good feature of $T_2^0 + LeastBit$ is that it does rule out the most glaring pathologies consistent with T_2^0, such as parts (i) and (ii) of Corollary 5.2:

Proposition 6.1. *$T_2^0 + LeastBit$ proves:*

(i) a power of 2 has no non-trivial odd divisors,

(ii) $\sqrt{2}$ is irrational.

Proof. Before dealing with (i) and (ii), we point out two simple statements which are provable in BASIC and T_2^0, respectively.

Firstly, BASIC proves that if $2^x < 2^y$, then $x < y$. Use the axiom $u \leq v \Rightarrow |u| \leq |v|$ to get the non-strict inequality, and then the axiom $|u| = |v| \Rightarrow u\#w = v\#w$ to conclude that if $x = y$, then $2^x\#1 = 2^y\#1$. But for all z, $2^z\#1 = 2 \cdot 2^z$.

Secondly, T_2^0 proves that if $2^x < 2^y$, then $2^y = 2^x \cdot 2^{y-x}$. An easy application of Σ_0^b induction shows that if y is in the range of $|\ |$, then so is any

number below y, in particular $y - x$. The rest of the argument needs only BASIC, most prominently the axiom $|u| = |v| + |w| \Rightarrow u\#z = (v\#z) \cdot (w\#z)$.

To prove (i), assume $2^j = q(2s+1)$ where $s > 0$. By *LeastBit*, q can be written as $2^l(2r+1)$, so

$$2^j = 2^l(2r+1)(2s+1). \tag{2}$$

Since $s > 0$, we must have $l < j$. Divide both sides of (2) by 2^l. We get $2^{j-l} = (2r+1)(2s+1)$, but 2^{j-l} is even.

In the case of (ii), the traditional proof goes through: if $\sqrt{2}$ is rational, use *LeastBit* to write it as p/q with at least one of p, q odd. A contradiction follows. □

The rest of this section is devoted to the proof of:

Theorem 6.2. *$T_2^0 + LeastBit \nvdash$ there are infinitely many primes.*

The proof of the theorem will, once again, rely on transferring a technique from open induction: this time, we borrow methods used by Smith [Smi93] to show that the infinity of primes is unprovable in *IOpen* extended by the GCD axiom, "every pair of elements has a greatest common divisor".

The infinity of primes is an interesting statement to study in this context, as it may well be independent of reasonably strong theories, such as S_2^1 and beyond. Full S_2 does prove that there are infinitely many primes [PWW88], but the proof makes essential use of the weak pigeonhole principle, and it is likely that S_2^1 and, in fact, S_2^2 does not prove WPHP even for polynomial time functions. The proof of infinity of primes as done in [PWW88] actually uses T_2^3 [Jeř].

The first thing to check is that J-rings can be extended by adding divisors of primes.

Lemma 6.3. *Assume $\mathcal{N} \succcurlyeq_J \mathcal{N}_0$ is countable, R is a J-ring contained in* $\mathrm{rcl}(\mathcal{N})$ *and $q \in R$ is prime, $q > J$. Then there exists a countable $\mathcal{N}' \succcurlyeq_J \mathcal{N}$, a J-ring $R' \supseteq R$ contained in* $\mathrm{rcl}(\mathcal{N}')$ *and an element x such that $x, q/x \in R'$.*

Remark. In [MM89] an analogous statement for $\mathbb{Z}$-rings is proved by taking $x > \mathbb{Z}$ smaller than all infinite elements of R (cf. Lemma 3.22 in that paper). In our case, this approach does not work. The existence of $\mathcal{N}' \succcurlyeq_J \mathcal{N}$ with some element strictly between J and $\mathcal{N} \setminus J$ would imply that J is a so-called *regular* cut. However, all regular cuts satisfy a rather strong fragment of PA called $B\Sigma_2$. In particular, they are closed under exponentiation, which renders them useless for our purposes.

Proof. We construct $\mathcal{N}'$ like in the proof of Lemma 4.4, as a simple extension of $\mathcal{N}$ by an element c. The type $p(z)$ realized by c is built as before, except that the element $d \in \mathcal{N} \setminus J$ used to define the notion of "large" is chosen so that $d^{\mathbb{N}} < q$. This implies:

$$\text{for each } b < d, ||q/b - q/(b+1)|| > 1. \tag{3}$$

Another change is that this time, x is c itself.

We need to verify that $R[c, q/c]$ is a discrete ordered ring. As a matter of fact we need, and prove, a bit more:

$$||f(c, q/c)|| > J, \tag{4}$$

for every non-constant $f(X, Y) \in R[X, Y]$.

If $f(X, Y)$ is such that $f(X, q/X)$ actually belongs to $R[X]$, then (4) follows directly from the work of Section 4. By the properties of the type p, we know that for every $\beta \in \text{acl}(R)$, $||c - \beta|| > J$, and that this already implies $||f(c, q/c)|| > J$.

If, on the other hand, $f(X, q/X)$ contains at least one term in q/X, reason as follows. Assume $||f(c, q/c)|| \leq j$ where $j \in J$. Consider the function $g(X) = f(X, q/X)$. Since $g^{-1}([-j, j])$ is a union of finitely many intervals with endpoints in $\text{rcl}(\mathcal{N})$, there are $\gamma_1^0, \gamma_2^0 \in \text{rcl}(\mathcal{N})$ with $\lfloor \gamma_2^0 - \gamma_1^0 \rfloor$ large such that $(\gamma_1^0, \gamma_2^0) \subseteq g^{-1}([-j, j])$ and $c \in (\gamma_1^0, \gamma_2^0)$. Now consider g': the interval (γ_1^0, γ_2^0) splits into finitely many subintervals on which $||g'||$ is either constantly bounded by 1 or constantly above 1. By basic calculus, subintervals of the latter kind cannot have large length. So, we find $\gamma_1^1, \gamma_2^1 \in \text{rcl}(\mathcal{N})$ such that $\lfloor \gamma_2^1 - \gamma_1^1 \rfloor$ is large, $(\gamma_1^1, \gamma_2^1) \subseteq (g')^{-1}([-1, 1])$ and $c \in (\gamma_1^1, \gamma_2^1)$. We can repeat this argument for $g'', g^{(3)}$ etc. Thus, $||g^{(n)}(c)|| \leq 1$ for all $n \geq 1$.

Take n such that $g^{(n)}(X)$ contains only terms in $1/X$ and no constant term. $X^{n+1} g^{(n)}(X)$ equals $qh(q/X)$ for some non-zero $h(X) \in R[X]$. We can write $h(X)$ as $b(X - \beta_1) \ldots (X - \beta_k)$, where b is in R and the $\beta_i \in \text{acl}(R)$ are all the roots of h. By (3) and the construction of $p(z)$, $||(q/c) - \beta|| > 1$ for all $\beta \in \text{acl}(R)$, in particular for $\beta = \beta_i$, so $||h(q/c)|| > 1$. Moreover, $q > d^{\mathbb{N}}$ and $0 < c < d$. Hence:

$$||g^{(n)}(c)|| = ||(1/c^{n+1}) qh(q/c)|| > ||q/c^{n+1}|| > d^{\mathbb{N}} > J.$$

This is a contradiction, and we have now proved (4) for all f.

Having done this, we know that $R[c, q/c]$ is a discrete ordered ring; to make it a J-ring, we need to determine the behaviour of c and q/c modulo elements of J. Create R' by letting $c \equiv 1 \pmod{j}$ and $q/c \equiv q \pmod{j}$ for all $j \in J$, that is, add elements of the form $c/j - 1/j$ and $q/(cj) - r/j$ where $r = (q \bmod j)$. By (4) and the closure of J under multiplication, R' remains discrete, so it is a J-ring. □

Of course, even if R satisfies *LeastBit*, indiscriminate use of Lemma 6.3 will not preserve it in R'. We now apply a trick stemming from [Smi93] in order to show that both here and in Lemma 4.3, R' *can* be chosen so that *LeastBit* is preserved.

The idea which let Smith build models of *IOpen* + GCD was to work only with $\mathbb{Z}$-rings without elements divisible by infinitely many finite integers. In our case, the role of $\mathbb{Z}$ is played by J, and we are mainly interested in divisibility by powers of 2, so a direct analogue would be to disallow elements divisible by all powers of 2 from J. This obviously cannot work, because of powers of 2 above J, but a slight modification of the approach does fine.

Lemma 6.4. *In Lemmas 4.3 and 6.3, if $R \models$ LeastBit, then we can choose R' so that also $R' \models$ LeastBit.*

Proof. The only necessary change in the proofs concerns the divisibility of x (and q/x, in the case of Lemma 6.3) by elements of J. Set $x \equiv 1 \pmod{j}$ and $q/x \equiv q \pmod{j}$ for every odd $j \in J$. It remains to deal with divisibility by powers of 2. The idea is to make each new element of R' not divisible by some power of 2 in J, unless there is a specific reason why that cannot be done. We first describe the details for Lemma 4.3 and then explain how to extend the argument so that it works for Lemma 6.3.

Enumerate all non-constant polynomials from $R[X]$ with at least one odd coefficient as $f_0(X), f_1(X), f_2(X) \ldots$ where $f_0(X) = X$. We define an increasing sequence $i_0 < i_1 < i_2 \ldots$ cofinal in $\log J$ and the values $x \bmod 2^{i_0}, x \bmod 2^{i_1}, x \bmod 2^{i_2} \ldots$ so that each $f_n(x)$ is not divisible by 2^{i_n}.

Let $i_0 = 1$ and set $x \bmod 2^1 = 1$. Assuming i_n and $x \bmod 2^{i_n}$ have been determined, consider $f_{n+1}(X)$. We have to find some $i_{n+1} > i_n$ and $x \bmod 2^{i_{n+1}}$ such that $f_{n+1}(x) \not\equiv 0 \pmod{2^{i_{n+1}}}$.

Consider the ring

$$S = \varprojlim_{i \in \log J} J/(2^i J)$$

(the "J-2-adic integers"). S is an integral domain: if $u, v \in S$ are non-zero at coordinates corresponding to $2^i, 2^k$, respectively, then uv is non-zero at coordinate 2^{i+k}, and $\log J$ is closed under $+$. Moreover, $\bar{f}_{n+1}(X)$, the polynomial obtained from f_{n+1} by applying to all coefficients the canonical remainder homomorphism from R to S, is not the zero polynomial (because some coefficient of f_{n+1} is odd). So, there are no more than $\deg f_{n+1}$ zeroes of $\bar{f}_{n+1}$ in S. Choose some $u \in S$ such that $\bar{f}_{n+1}(u) \neq 0$ and u agrees with $x \bmod 2^{i_n}$ at coordinate 2^{i_n}. Take k such that $\bar{f}_{n+1}(u)$ is non-zero at coordinate 2^k. Let i_{n+1} be $\max(i_n, k, n|a|)$ (recall that J is of the form $a^{\mathbb{N}}$, so the elements $n|a|$ are cofinal in $\log J$). Set $x \bmod 2^{i_{n+1}}$ to be the value of u at coordinate $2^{i_{n+1}}$.

This completes the description of $x \bmod j$ for $j \in J$, and thus of R'. It is clear that for every $f(X)$ with an odd coefficient there is some $i \in \log J$ such that 2^i does not divide $f(x)$. We now verify that *LeastBit* holds in R'.

By *LeastBit* in R and the definition of R', an element of R' can be presented in the form $2^l f(x)/j$ for some $j, l \in J$ and some $f(X) \in R[X]$ with at least one odd coefficient. We can write $j = 2^i(2s+1)$ and $f(x) = 2^k(2t+1)$ for some $j, k \in \log J$. This is obvious in the case of j. To see it for $f(x)$, note that for some $\tilde{k} \in \log J$, $(f(x) \bmod 2^{\tilde{k}}) = r$ where $0 \neq r \in J$. Now, residue arithmetic $\bmod 2^{\tilde{k}}$ in R' is inherited from $\mathcal{N}'$, so r is an odd multiple of 2^k for some $k < \tilde{k}$. The same k works for $f(x)$.

So, we have:

$$\frac{2^l f(x)}{j} = \frac{2^{l+k}(2t+1)}{2^i(2s+1)}.$$

It must be the case that $l+k \geq i$. This is because $2^{l+k}(2t+1)$ is congruent to $0 \pmod{2^i}$, $2t+1$ is odd, and, again, residue arithmetic $\bmod 2^i$ is the same in R' as in $\mathcal{N}'$.

Similarly, $2^{l+k}(2t+1)$ is congruent to $0 \pmod{(2s+1)}$, but 2^{l+k} is a unit $\bmod (2s+1)$ in R and thus in R' (since in a J-ring satisfying *LeastBit*, such as R, 2^{l+k} cannot have a non-trivial odd divisor). Therefore, $2t+1$ must be congruent to $0 \pmod{(2s+1)}$. This implies that $(2t+1)/(2s+1) \in R'$, and hence 2^{l+k-i} divides $2^l f(x)/j$.

Finally, $(2t+1)/(2s+1)$ is obviously odd, so 2^{l+k-i} is the greatest power of 2 dividing $2^l f(x)/j$. This shows that we can make $R' \models$ *LeastBit* in Lemma 4.3.

In the case of Lemma 6.3, we must additionally deal with q/x. For $j \in J$, the value $(q/x) \bmod j$ is the product of q and the inverse of x taken $\bmod j$

(note that x is a unit mod j). We check that $R' \models \mathit{LeastBit}$. An element of R' can be presented as $2^l f(x, q/x)/j$, where $j, l \in J$, and $f(X, Y) \in R[X, Y]$ has an odd coefficient and does not contain two different monomials with the same difference between X-degree and Y-degree. For some n, $x^n f(x, q/x)$ equals $h(x)$ where $h(X)$ also has an odd coefficient.

As before, we can show that

$$\frac{2^l h(x)}{j} = \frac{2^{l+k}(2t+1)}{2^i(2s+1)}$$

and that 2^{l+k-i} is the greatest power of 2 dividing $2^l h(x)/j$.

We claim that 2^{l+k-i} also divides $2^l f(x, q/x)/j$, which will complete the proof, as no greater power of 2 can divide $2^l f(x, q/x)/j$. To see that the claim holds, observe that if $h(x) = x^n f(x, q/x)$ equals $2^k(2t+1)$ for $k \in \log J$, then 2^k must also divide $f(x, q/x)$, because x^n is odd. □

It is worth pointing out that Lemma 6.3 can be proved for q a power of 2 instead of a prime. Lemma 6.4 should break down in this case, and it does. The place where the proof stops working is: "for some n, $x^n f(x, q/x)$ equals $h(x)$ where $h(X)$ *also has an odd coefficient.*"

Conclusion of proof of Theorem 6.2. Let R be (the ring generated by) the cut determined by the elements $\{2^j : j \in J\}$ in $\mathcal{N}_0$. Obviously, R is a J-ring satisfying $\mathit{LeastBit}$. Using Lemma 6.4, iterate Lemmas 4.3 and 6.3 to build J-rings $R \subseteq R_1 \subseteq R_2 \ldots$, all satisfying $\mathit{LeastBit}$, and associated PA-models $\mathcal{N}_0 \preccurlyeq_J \mathcal{N}_1 \preccurlyeq_J \mathcal{N}_2 \ldots$. Do it in such a way that $R_\infty = \bigcup_{n \in \mathbb{N}} R_n$ is a model of IOpen without any primes above J. By Lemma 4.2, $R_\infty \models T_2^0$. Moreover, the decomposition of an element of R_n into a power of 2 and an odd number remains unchanged in R_m for $m > n$, so $R_\infty \models \mathit{LeastBit}$. □

The proof of Theorem 6.2 has the following corollary, which implies that $T_2^0 + \mathit{LeastBit}$ does not prove Matiyasevich's Theorem.

Corollary 6.5. *There is no (even non-strict) Σ_1^b formula definining primality in all models of $T_2^0 + \mathit{LeastBit}$.*

Proof. Consider the models R and R_∞ from the proof of Theorem 6.2. Let $\varphi(x)$ be a Σ_1^b formula true of all primes in R. For a prime $b \in R \setminus J$, $\varphi(b)$ still holds in R_∞, but b is no longer prime. □

7 Conclusion: remarks and open problems

Apologia pro pigritudine sua. It is natural to ask why we only prove an independence result for an extension of T_2^0 by the *LeastBit* axiom, since [Smi93] obtains analogous results for extensions of *IOpen* by the full GCD property and even the so-called Bézout property (every two numbers have a GCD which is their linear combination with integer coefficients).

We do in fact conjecture that T_2^0 + GCD does not prove the infinity of primes, and that this can be shown by an appropriate modification of Smith's methods. However, such a modification will have to overcome a number of annoying problems due mainly to the fact that many elements of J have infinitely many prime divisors. More to the point, we are not convinced that proving further independence results for extensions of T_2^0 by successively stronger algebraic axioms is a good research direction. A direction we consider more important is dicussed in Open Problem 1 below.

Remark. Our constructions used rings cofinal with $\{2^j : j \in J\}$, i.e. with $\{2^{a^k} : k \in \mathbb{N}\}$, which gave us models of T_2^0. However, all the proofs work just as well for rings barely longer than J, e.g. cofinal with $\{2^{|a|^k} : k \in \mathbb{N}\}$. This means that the independence results of Corollary 5.2 and Theorem 6.2 hold also for a theory in which the Σ_0^b induction scheme is replaced by induction for all formulas bounded by terms representing functions dominated by $\sqrt{x}, \sqrt[3]{x}, \ldots$. Acceptable bounds include $|t|\#|t|$ or even $t^{1/\log^* t}$ (the latter example requires an extension of the language).

We conclude the paper by mentioning some open problems. The three problems we discuss seem to us, on the one hand, at least somewhat interesting, on the other, not obviously beyond reach.

Open Problem 1. Does S_2^0 prove that there are infinitely many primes?

This problem represents the more general question, "can *IOpen*-style algebraic methods work for S_2^0?". The motivation for studying the issue is the perhaps unlikely, but not altogether excluded possibility that methods of this sort could be modified so as to work for theories with significant computational content, such as (the one-sorted version of) VTC^0 (see Chapter 9 of [CN10]). If that is to happen, the methods will first have to be able to handle S_2^0 and its stronger cousin $S_2^0(\lfloor x/2^y \rfloor)$.

S_2^0 and $S_2^0(\lfloor x/2^y \rfloor)$ are of course known to be extremely weak theories (e.g. [Tak90], [Joh98]), but the techniques used to prove their weakness are very different from the ones studied here, and they do not appear to work

for infinity of primes. Moreover, S_2^0 knows more about the bit structure of numbers than T_2^0: it excludes odd divisors of powers of 2 ([BK10]), and $S_2^0(\lfloor x/2^y \rfloor)$ also excludes a rational $\sqrt{2}$.

If attacking S_2^0 directly proves too difficult, an even weaker theory to study in this context is PIND for open formulas of L_{BA}. Already this theory rules out odd divisors of powers of 2.

Open Problem 2. Does $IOpen(\lfloor x/y \rfloor)$ prove that there are infinitely many primes?

More generally, "prove an interesting independence result for $IOpen(\lfloor x/y \rfloor)$." Here, $IOpen(\lfloor x/y \rfloor)$ is induction for quantifier-free formulas in the language $L_{PA} \cup \{\lfloor x/y \rfloor\}$. This theory was shown to be strictly stronger than $IOpen$ in [Kay93], but apparently no separation of $IOpen(\lfloor x/y \rfloor)$ from $I\Delta_0$ is known.

We feel that a better understanding of $IOpen(\lfloor x/y \rfloor)$ is a worthy goal, especially in light of the prominence given to $T_2^0(\lfloor x/2^y \rfloor)$ by the results of [Jeř06].

Open Problem 3. Is there a diophantine (or at least $\exists_1$) sentence consistent with $IOpen$ but not T_2^0?

Despite the striking similarity between T_2^0 and $IOpen$, it is not particularly difficult to show that the former is not conservative over the latter. For example, it is consistent with $IOpen$ but not T_2^0 that the numbers split into a well-behaved initial segment satisfying $I\Delta_0 + \exp$ and a badly-behaved higher part where pathologies such as rational presentations of $\sqrt{2}$ appear arbitrarily low. However, the sentence expressing this has rather high quantifier complexity. It would be nice to understand whether the two theories can be separated by a much simpler sentence.

If there is a Diophantine sentence separating $IOpen$ from T_2^0, then, by Theorem 5.1, the Diophantine equation witnessing this is not solvable in M_{Shep} (in this context, it is worth recalling that a characterization of equations solvable in models of $IOpen$ is given in [Wil78], and the two-variable case is studied in more depth in [vdD81]). On the other hand, conservativity for $\exists_1$ sentences would imply that every $\mathbb{Z}$-ring can be extended to a structure with a well-behaved "logarithm".

Acknowledgements. The author is grateful to Sedki Boughattas and Neil Thapen for helpful discussions.

References

[Ada87] Z. Adamowicz, *Open induction and the true theory of rationals*, Journal of Symbolic Logic **52** (1987), 793–801.

[BIK+92] P. Beame, R. Impagliazzo, J. Krajícek, T. Pitassi, P. Pudlák, and A. R. Woods, *Exponential lower bounds for the pigeonhole principle*, Proc. 24th ACM Symposium on Theory of Computing, ACM, 1992, pp. 200–220.

[BK10] S. Boughattas and L. A. Kołodziejczyk, *The strength of sharply bounded induction requires MSP*, Annals of Pure and Applied Logic **161** (2010), 504–510.

[BO96] A. Berarducci and M. Otero, *A recursive nonstandard model of normal open induction*, Journal of Symbolic Logic **61** (1996), 1228–1241.

[BR10] S. Boughattas and J. P. Ressayre, *Bootstrapping, part I*, Annals of Pure and Applied Logic **161** (2010), 511–533.

[Bus98] S. R. Buss, *First-order proof theory of arithmetic*, Handbook of Proof Theory (S. R. Buss, ed.), Elsevier, 1998, pp. 79–147.

[CN10] S. A. Cook and P. Nguyen, *Logical Foundations of Proof Complexity*, Cambridge University Press, 2010.

[HP93] P. Hájek and P. Pudlák, *Metamathematics of First-Order Arithmetic*, Springer-Verlag, 1993.

[Jeř] E. Jeřábek, talk at 29éme Journées sur les Arithmetiques Faibles, Warsaw 2010. Slides available at www.math.cas.cz/ jerabek.

[Jeř06] ———, *The strength of sharply bounded induction*, Mathematical Logic Quarterly **52** (2006), 613–624.

[Joh98] J. Johannsen, *A remark an independence results for sharply bounded arithmetic*, Mathematical Logic Quarterly **44** (1998), 568–570.

[Kay91] R. Kaye, *Models of Peano Arithmetic*, Oxford University Press, 1991.

[Kay93] ———, *Open induction, Tennenbaum phenomena, and complexity theory*, Arithmetic, proof theory, and computational complexity (P. Clote and J. Krajiček, eds.), Oxford University Press, 1993, pp. 222–237.

[Kra95] J. Krajíček, *Bounded Arithmetic, Propositional Logic, and Complexity Theory*, Cambridge University Press, 1995.

[KS06] R. Kossak and J. Schmerl, *The Structure of Models of Peano Arithmetic*, Oxford University Press, 2006.

[Man91] S. G. Mantzivis, *Circuits in bounded arithmetic part I*, Annals of Mathematics and Artificial Intelligence **6** (1991), 127–156.

[Mar02] D. Marker, *Model Theory: An Introduction*, Springer-Verlag, 2002.

[MM89] A. Macintyre and D. Marker, *Primes and their residue rings in models of open induction*, Annals of Pure and Applied Logic **43** (1989), 57–77.

[Pol00] C. Pollett, *Multifunction algebras and the provability of PH↓*, Annals of Pure and Applied Logic **104** (2000), 279–303.

[PWW88] J. B. Paris, A. J. Wilkie, and A. R. Woods, *Provability of the pigeonhole principle and the existence of infinitely many primes*, Journal of Symbolic Logic **53** (1988), 1235–1244.

[RR97] A. A. Razborov and S. Rudich, *Natural proofs*, Journal of Computer and System Sciences **55** (1997), 24–35.

[She64] J. C. Shepherdson, *A non-standard model for a free variable fragment of number theory*, Bulletin de l'Académie Polonaise des Sciences. Série des Sciences Mathématiques, Astronomiques et Physiques **12** (1964), 79–86.

[Smi93] S. T. Smith, *Building discretely ordered Bezout domains and GCD domains*, Journal of Algebra **159** (1993), 191–239.

[Tak90] G. Takeuti, *Sharply bounded arithmetic and the function* $a \dot{-} 1$, Logic and computation (W. Sieg, ed.), Contemporary Mathematics, vol. 106, AMS, 1990, pp. 281–288.

[vdD80] L. van den Dries, *Some model theory and number theory for models of weak systems of arithmetic*, Model Theory of Algebra and Arithmetic. Proc. Conf., Karpacz 1979, Lecture Notes in Mathematics, no. 834, Springer, 1980, pp. 346–362.

[vdD81] ———, *Which curves over $\mathbb{Z}$ have points with coordinates in a discrete ordered ring*, Transactions of the AMS **264** (1981), 181–189.

[Wil78] A. J. Wilkie, *Some results and problems on weak systems of arithmetic*, Logic Colloquium '77 (A. Macintyre et al., ed.), North-Holland, 1978, pp. 285–296.