A note on Δ_1 induction and Σ_1 collection

Neil Thapen*

May 23, 2005

Abstract

Slaman recently proved that Σ_n collection is provable from Δ_n induction plus exponentiation, partially answering a question of Paris. We give a new version of this proof for the case $n = 1$, which only requires the following very weak form of exponentiation: "x^y exists for some y sufficiently large that x is smaller than some primitive recursive function of y".

Mathematics subject classification: 03F30, 03H15

By Δ_n induction, or $I\Delta_n$, we mean the usual induction scheme for every Σ_n formula ϕ which is equivalent in the model to a Π_n formula. That is, the scheme

$$[\forall x\, (\phi(x) \leftrightarrow \psi(x))] \rightarrow [\phi(0) \wedge \forall x\, (\phi(x) \rightarrow \phi(x+1)) \rightarrow \forall x\, \phi(x)]$$

for every Σ_n formula ϕ and every Π_n formula ψ (both possibly with parameters). By Σ_n collection, or $B\Sigma_n$, we mean the scheme

$$\forall x\!<\!y\, \exists z\, \phi(x,z) \rightarrow \exists w\, \forall x\!<\!y\, \exists z\!<\!w\, \phi(x,z)$$

for every Σ_n formula ϕ (with parameters).

It is reasonably straightforward to prove that $B\Sigma_n \vdash I\Delta_n$ (over a suitable algebraic fragment of PA). Paris posed the question [1] whether the other direction also holds. Slaman [4] showed recently that $I\Delta_n + \exp \vdash B\Sigma_n$,

*St Hilda's College, University of Oxford, Oxford OX1 4DY, UK; `neil.thapen@st-hildas.ox.ac.uk`. This work was done while visiting the Mathematical Institute of the Academy of Sciences of the Czech Republic.

where exp is the axiom "$\forall x, y,\ x^y$ exists". This answers the question completely for $n \geq 2$, since exp is provable in $I\Delta_2$. We improve the result for $n = 1$, by replacing exp with the assumption "x^y exists for some y such that $x < p(y)$" where p can be any primitive recursive function. This is theorem 2 below.

We will not give any more background here. See Slaman [4] for a more complete introduction to this problem, or [3] or [2] for a general introduction to the relevant model theory of arithmetic.

Our proof is similar to Slaman's, with two new ideas. The first is that we can use a function with bounded domain but unbounded range to define a very fast-growing function on a cut. This allows us to reduce the amount of exponentiation needed in the proof, and show that $I\Delta_1 + \forall x\,(x^{\log^k x}$ exists$) \vdash B\Sigma_1$, for any $k \in \mathbb{N}$ (see the remark after lemma 9). The second is to show that this cut is closed under the primitive recursive functions. This lets us reduce it further, to "x^y exists for some y that is not very much smaller than x", where "very much smaller" is defined in terms of primitive recursive functions. It is still open whether it is possible to get rid of exponentiation altogether.

Acknowledgements: This work arose from discussions with Zofia Adamowicz, Andrés Cordón-Franco, Leszek Kołodziejczyk, Jeff Paris, Alex Wilkie and Konrad Zdanowski. I would also like to thank the organizers of the Fall School of the Prague logic seminar at Pec pod Sněžkou.

I am grateful to Leszek Kołodziejczyk for reading and commenting on an earlier version of this note.

Let M be a model of $I\Delta_1$ with a distinguished element a. We will be considering two kinds of sequence of elements of M. The first kind is simply the sequence of numbers in $[0, a)$ obtained by writing a number $w \in M$ in base a notation, and we will write the ith element of such a sequence as $(w)_i$.

The second kind is not directly coded in the model, in that it is indexed by a cut and so has no last element. We will call it a Σ_1 sequence, and formally it is a Σ_1 function w^* from a Σ_1 cut I to M. For $i \in I$ we write the ith element of the sequence as w^*_i.

We first give a lemma due to Slaman, relating these two kinds of sequence.

Lemma 1 *Let w^* be a Σ_1 sequence of elements of $[0,a)$, indexed by a Σ_1 cut I in M. Suppose it has the extra property that its initial segments are uniformly coded in M, which means that there is a Σ_1 sequence s^* such that, for $i \in I$, s^*_i codes (via its base a expansion) the sequence $w^*_0 \ldots w^*_i$.*

Suppose that there is $b \in M$ with $I < b$ and such that a^b exists. Then there exists $e < a^b$ coding w^* in M, in the sense that for all $i \in I$, $(e)_i = w^*_i$.

Proof We make the additional assumption that every element of w^* is strictly less than $a-1$. This can be removed easily, for example by taking a^2 as the parameter in place of a.

For each $i \in I$, let $c^*_i = s^*_i \cdot a^{b-i-1}$, which, written out in base a, looks like

$$w^*_0 \ldots w^*_i 0 \ldots 0$$

where there are b numerals altogether. Then c^*_i is an increasing Σ_1 sequence, but not necessarily strictly increasing, since some w^*_is might be 0. However we may assume that it has no greatest element, since otherwise we could use that element as our desired number e.

For each $i \in I$, let $d^*_i = (s^*_i + 1) \cdot a^{b-i-1}$, which, written out in base a, looks like

$$w^*_0 \ldots w^*_{i-1}(w^*_i + 1)0 \ldots 0$$

(here we use the assumption that each w^*_j is less than $a-1$). Then d^*_i is a decreasing Σ_1 sequence.

Now define C to be the proper Σ_1 cut $\{x : \exists i \in I\, x < c^*_i\}$ and define D to be the Σ_1 upwards-closed set $\{x : \exists i \in I\, x > d^*_i\}$.

Clearly C and D do not intersect, and any e with $C < e < D$ will be such that $(e)_i = w^*_i$ for all $i \in I$. But there must be some such e, since otherwise $D = M \setminus C$ which means that C is a Δ_1-definable proper cut, which is impossible in a model of $I\Delta_1$. $\square$

We now give our main theorem.

Theorem 2 *Let M be a model of $I\Delta_1$, and $a \in M$. Suppose that there is $b \in M$ such that a^b exists and $p(b) > a$ for some primitive recursive function p. Then Σ_1 collection holds at a in M, that is, for any Δ_0 formula ϕ,*

$$M \models \forall x < a\, \exists y\, \phi(x,y) \to \exists z\, \forall x < a\, \exists y < z\, \phi(x,y).$$

The proof takes up the rest of this note. It is by contradiction, so our assumption from now on is that M is such that the theorem fails. In particular collection fails, so we cannot bound the witnesses y for ϕ for $x < a$.

Lemma 3 *There is a injective function $f : a \to M$ with a Δ_0 graph and with range unbounded in M.*

Proof Map $x < a$ to the number coding the pair $\langle x, y\rangle$ where y is least such that $\phi(x, y)$ holds. $\square$

Definition 4 *Let $\theta(i, w, t)$ express the following:*

1. *w codes a sequence $(w)_0, \ldots, (w)_i \subseteq [0, a)$*
2. *For all $j \leq i$, $f((w)_j) \leq t$*
3. *$f((w)_0)$ is the least element of the range of f that is bigger than a*
4. *For all $j \leq i$, $f((w)_{j+1})$ is the least element of the range of f that is bigger than $f((w)_j)^2$.*

The formula θ is Δ_0, since we include the bound t as a parameter. Let $I = \{i : \exists w\, \exists t\, \theta(i, w, t)\}$.

Lemma 5 *I is a cut and for all $i \in I$ there is a unique w such that $\exists t\, \theta(i, w, t)$.*

Proof I is clearly closed downwards. To show that it is closed under successor, suppose $i \in I$ with witnesses w and t. Since the range of f is unbounded in M, there must be some $x < a$ with $f(x) > f((w)_i)^2$. Using $f(x)$ as an upper bound, Δ_0 induction is enough to find $z < a$ such that $f(z)$ is the least thing bigger than $f((w)_i)^2$ in the range of f. Note that this is the only place in the proof where we use the unboundedness of the range of f.

For uniqueness, suppose $\theta(i, w, t)$ and $\theta(i, w', t')$, and, without loss of generality, that $t \geq t'$. Then, using t as a bound, Δ_0 induction is enough to show that $f((w)_j) = f((w')_j)$ for all $j \leq i$. So $w = w'$, since f is injective. $\square$

Uniqueness means that we can define a Σ_1 sequence w^*, where for each $i \in I$ we take w^*_i to be $(w)_i$ for the unique w such that $\exists t\, \theta(i, w, t)$.

Lemma 6 *For all $i \in I$, a^{2^i} exists in M and is less than $f(w_i^*)$.*

Proof Let w, t be such that $\theta(i, w, t)$. We use induction to show that for all $j \leq i$, $a^{2^j} < f((w)_j)$. Only Δ_0 induction is needed, because we can bound everything by t. Formally, the inductive hypothesis is

$$\exists y \leqslant t \, \exists p < y \, (a^{2^j} = p \wedge f((w)_j) = y).$$

Here we are using the fact that exponentiation can be defined by a Δ_0 formula. The induction step follows from the definition of w. $\square$

Lemma 7 *$I < a$.*

Proof Suppose not. Then $a \in I$ so there exist w, t such that $\theta(a, w, t)$. So w codes a sequence of elements of $[0, a)$, and they must all be distinct because $f((w)_j)$ strictly increases as j increases. Hence we have an injection from $a + 1$ to a, violating the pigeonhole principle. However $a \in I$ implies that a^{2^a} exists in M, by lemma 6, which means that Δ_0 induction is enough to carry out the standard proof of the pigeonhole principle at a.[1] $\square$

Lemma 8 *a^I is cofinal in M.*

Proof Suppose not. Then there exists a b such that a^b exists and $I < b$.

Let $S = \{f(w_i^*) : i \in I\}$. We first show that S is unbounded in M. Otherwise there is some upper bound t for S, but then

$$i \in I \iff \exists w < a^b \, \theta(i, w, t).$$

Here we can use a^b to bound the size of the sequence w, because $I < b$. But this means that I is a Δ_0-definable proper cut, which is impossible.

We can also apply lemma 1 to get a number e such that $(e)_i = w_i^*$ for all $i \in I$.

Now consider the function $g : i \mapsto f((e)_i)$. Restricted to I, this function is increasing and its range S is unbounded in M. So I can be defined as exactly the initial segment on which g is increasing. Formally,

$$i \notin I \iff \exists i' \exists t, t' \, (i' < i \wedge f((e)_{i'}) = t' \wedge f((e)_i) = t \wedge t' > t).$$

This is now a contradiction with Δ_1 induction, because we have Σ_1 definitions of I and of its complement, but I is a proper cut. $\square$

[1]In fact $I\Delta_0$ by itself is enough to prove the pigeonhole principle for any *coded* function.

Lemma 9 *I is closed under exponentiation.*

Proof Suppose not. Then there exists $\beta \in I$ with $2^\beta > I$. But then a^{2^β} exists, by lemma 6. This is a contradiction, since a^I is cofinal in M. $\square$

At this point we could finish the proof by replacing the assumption "a^b exists" in theorem 2 with "$a^{\log^k a}$ exists" for some $k \in \mathbb{N}$ (where $\log^k$ means iterated log). This gives a contradiction, because if I is closed under exponentiation we must have $I < \log^k a$.

We go on to prove the stronger version of the theorem by showing that I is closed under all primitive recursive functions. We do this indirectly, by showing that I is a model of $I\Sigma_1$.

Lemma 10 $I \models I\Sigma_1$.

Proof Suppose induction fails in I for some formula $\exists y\, \phi(x,y)$, where ϕ is Δ_0. Let $\psi(x,z)$ be the formula

$$\forall u \leqslant x\, \exists y \leqslant z\, \phi(u,y) \wedge \text{“}z \text{ is least such that } \forall u \leqslant x\, \exists y \leqslant z\, \phi(u,y)\text{”}.$$

Let $J = \{j \in I : \exists z \in I\, \psi(j,z)\}$. Then J is a Σ_1 proper cut in I (and in M) and ψ is the Δ_0 graph of a function $g : J \to I$.

The range of g must be unbounded in I, for suppose there is an upper bound s. Then $j \in J \Leftrightarrow \exists z < s\, \psi(j,z)$, so J is a Δ_0 proper cut, which is impossible.

Since J is a proper cut in I, there exists β with $J < \beta < I$, and $\beta \in I$ implies a^β exists (in fact a^{2^β} does).

Consider the function $h : I \to M$ given by $i \mapsto f(w_i^*)$. This has range unbounded in M, as a^I is cofinal in M and for all $i \in I$ we have $a^i < f(w_i^*)$ (by lemma 6).

For $j \in J$, let v_j^* be the sequence

$$w^*_{g(0)} \dots w^*_{g(j)}.$$

Then v^* is a Σ_1 sequence, so since a^β exists, by lemma 1 there is a number e such that for all $j \in J$, $(e)_j = w^*_{g(j)}$.

Now consider the function $k : j \mapsto f((e)_j)$. On J, k is the composition $h \circ g$. The function h on I is increasing and has range unbounded in M, and the function g on J is increasing and has range unbounded in I. So, restricted to J, k is increasing and has range unbounded in M. Therefore, as in lemma 8, we can now write the complement of J in a Σ_1 way:

$$j \notin J \iff \exists j' \exists t, t' \, (j' < j \wedge f((e)_{j'}) = t' \wedge f((e)_j) = t \wedge t' > t).$$

Hence J is a Δ_1 proper cut in M, which is impossible. $\square$

To complete the proof of theorem 2, we now use the assumption there is $b \in M$ such that a^b exists in M and $a < p(b)$ for some primitive recursive function p. Since $I < a$ and I is closed under primitive recursive functions, we must have $I < b$. But then $a^I < a^b$ and so a^I is not cofinal in M, giving a contradiction.

References

[1] P. Clote and J. Krajíček. Open problems. In P. Clote and J. Krajíček, editors, *Arithmetic, Proof Theory, and Computational Complexity*, pages 289–319. Oxford University Press, 1993.

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

[3] Richard Kaye. *Models of Peano Arithmetic*. Clarendon Press, Oxford, 1991.

[4] T. Slaman. Σ_n-bounding and Δ_n-induction. *Proceedings of the American Mathematical Society*, 132:2449–2456, 2004.