References

[0] B. Banaschewski, *Prime elements from prime ideals*, Order 2 (1985), 211–213.

[1] B. Banaschewski and R. Harting, *Lattice aspects of radical ideals and choice principles*, Math. Proc. Cambridge Phil. Soc. Proc. London Math. Soc. (3) 50 (1985), 385–404.

[2] S. Feferman, *Some applications of the notions of forcing and generic sets*, Fund. Math. 56 (1965), 325–345.

[3] J. D. Halpern, *The independence of the axiom of choice from the Boolean prime ideal theorem*, Fund. Math. 55 (1965), 57–66.

[4] J. D. Halpern and A. Lévy, *The Boolean prime ideal theorem does not imply the axiom of choice*, in *Axiomatic Set Theory*, Part I (Proc. Symp. Pure Math. XIII-1) ed. D. Scott, 83–134.

[5] L. Henkin, *Metamathematical theorems equivalent to the prime ideal theorems for Boolean algebras*, Bull. Amer. Math. Soc. 60 (1954) 387–388.

[6] W. Hodges, *Krull implies Zorn*, J. London Math. Soc. (2) 19 (1979), 285–287.

[7] T. Jech, *The Axiom of Choice*, North-Holland 1973.

[8] P. T. Johnstone, *Almost maximal ideals*, Fund. Math. 123 (1984), 197–209.

[9] J. L. Kelley, *The Tychonoff product theorem implies the axiom of choice*, Fund. Math. 37 (1950), 75–76.

[10] G. Klimovsky, *El teorema de Zorn y la existencia de filtros y ideales maximales en los reticulados distributivos*, Rev. Un. Mat. Argentina 18 (1958), 160–164.

[11] J. Łoś and C. Ryll-Nardzewski, *On the application of Tychonoff's theorem in mathematical proofs*, Fund. Math. 38 (1951), 233–237.

[12] A. Mostowski, *Über die Unabhängigkeit des Wohlordnungssatzes vom Ordnungsprinzip*, Fund. Math. 32 (1939), 201–252.

[13] H. Rubin and J. Rubin, *Equivalents of the Axiom of Choice*, North-Holland 1963.

[14] D. Scott, *Prime ideal theorems for rings, lattices, and Boolean algebras*, Bull. Amer. Math. Soc. 60 (1954), 390.

[15] B. L. van der Waerden, *Beweis einer Baudetschen Vermutung*, Nieuw Arch. Wisk. 15 (1927), 212–216.

MATHEMATICS DEPARTMENT
THE UNIVERSITY OF MICHIGAN
Ann Arbor, Michigan 48109-1003

Received 13 May 1985

Counting $\varDelta_0$ sets

J. Paris and **A. Wilkie** (Manchester)

Abstract. In this paper we consider the following well-known problem "Let B be a $\varDelta_0$-definable set of natural numbers. Is the function $G(n) = |B\cap n|$ also $\varDelta_0$-definable?".

We shall show that the answer is *yes* if B is a very sparse set. We shall also show that for any B we can obtain a fair approximation to G which is $\varDelta_0$ definable.

Notation. The notation we shall use is entirely standard, see for example [1], [2]. In particular we use $\varDelta_0^N$ to denote the class of subsets of N^k, $k\in N$, definable in the standard model by a $\varDelta_0$ formula in the language of first order arithmetic. For a finite set B, $|B|$ denotes the number of elements in B. All logarithms are to the base 2 and in expressions like $\log(x)$, x^α (α rational), etc. we shall always mean the integer parts of these quantities, whenever they appear in $\varDelta_0$ formulae.

Introduction. The following problem was previously considered in [1].

"Let $B\in\varDelta_0^N$, $B\subseteq N$. Is the function G defined by $G(n) = |B\cap n|$ also in $\varDelta_0^N$?"

The general feeling is that the answer to this problem is *no*, for example for B = set of primes. However we shall show in Theorem 5 that the answer is *yes* if B is very sparse. In Corollary 7 we show that in any case we can always obtain a fair approximation to G which is in $\varDelta_0^N$.

In what follows let $A\in\varDelta_0^N$, $A\subseteq N^{\nu+2}$ and let

$$A_n(\vec{x}) = \{m\,|\,\langle\vec{x}, m, n\rangle\in A\ \&\ m<n\}\subseteq n\,.$$

In the lemmas which follow we shall be trying to count $|A_n(\vec{x})|$. To simplify matters we shall omit mention of the parameters $\vec{x}$ although as we shall see it will be critical that our results are uniform in the parameters.

Throughout n will stand for a large natural number. It should be clear that our results are trivial for n small. Throughout this paper we use the notation $f\colon A \Vdash\!\!\twoheadrightarrow B$ $f\colon A \Vdash\!\!\rightarrow B$, $f\colon A \twoheadrightarrow B$ to denote that f is respectively a bijective, injective, surjective function from A to B.

Our first lemma was previously proved in [1] but for the sake of completeness we repeat the proof here.

Lemma 1. *Let $k \in N$, $0 < \alpha < 1$, $\delta = \log(n)^{(1-\alpha)/2}$ and assume that $A_n \subseteq 2^{\log(n)^\alpha}$ for all $n \in N$. Then the function*

$$H(n) = \min(|A_n|, \delta^k + 1)$$

is in Δ_0^N.

So if $|A_n|$ is small and the elements of A_n are small then we can count $|A_n|$.

Proof. By induction on k for all such A simultaneously. For $k = 1$ we have

$$m = \min(|A_n|, \delta+1) \Leftrightarrow \exists f,\ f\colon m \Vert\!\!\twoheadrightarrow A_n \ \&\ m \leqslant \delta$$
$$\text{or no such } f \text{ exists } \&\ m = \delta+1\,.$$

Since we can code f by the number

$$(1+\max(A_n))^m + \sum_{i<m} f(i)(1+\max(A_n))^i \leqslant 2(2^{\log(n)^\alpha})^\delta < 2n\,,$$

this expression is Δ_0. (Notice that since the graph of exponentation is in Δ_0^N we can recapture the values of f from this code using just Δ_0 formulae. Henceforth we shall use this fact without explicit mention.)

Now assume the result for k and all such A. Then

$$m = \min(|A_n|, \delta^{k+1}+1) \Leftrightarrow \exists\ 0 = i_0 \leqslant \ldots \leqslant i_\delta = 2^{\log(n)^\alpha} \text{ such that}$$
$$\sum_{0 \leqslant t < \delta} |A_n \cap [i_t, i_{t+1})| = m \quad \&$$
$$\text{for } 0 \leqslant t < \delta,\ |A_n \cap [i_t, i_{t+1})| \leqslant \delta^k$$
$$\text{or no such } \vec{i} \text{ exists and } m = \delta^{k+1}+1$$
$$\Leftrightarrow \exists 0 = i_0 \leqslant \ldots \leqslant i_\delta = 2^{\log(n)^\alpha} \exists\ 0 = m_0 \leqslant m_1 \leqslant \ldots \leqslant m_\delta = m\,,$$

such that, for $0 \leqslant t < \delta$,

$$m_{t+1} - m_t = \min(|A_n \cap [i_t, i_{t+1})|, \delta^k+1) \leqslant \delta^k$$

or no such $\vec{i}$, $\vec{m}$ exist and $m = \delta^{k+1}+1$.

Using the inductive hypothesis and the fact that the sequence $\vec{i}$ can be coded by a number $\leqslant 2(2^{\log(n)^\alpha})^\delta < 2n$ and the sequence $\vec{m}$ by a number $\leqslant 2(\delta^{k+1})^\delta < 2\log(n)^{(k+1)\sqrt{\log(n)}} < 2n$, we see that this yields the required Δ_0 definition. ■

Corollary 2. *Let $q \in N$. Then there is a function $H \in \Delta_0^N$ such that whenever $A_n \subseteq \log(n)^q$,*

$$H(n) = |A_n|\,.$$

Proof. First notice that $A_n \cap \log(n)^q \subseteq 2^{\sqrt{\log(n)}}$ and $|A_n \cap \log(n)^q| \leqslant \log(n)^q$. Hence applying Lemma 1 to $A_n \cap \log(n)^q$ with $\alpha = 1/2$, $k = 4q+1$ gives a function $H \in \Delta_0^N$ such that

$$H(n) = \min(|A_n \cap \log(n)^q|, (\log(n)^{1/4})^{4q+1}) = |A_n \cap \log(n)^q|$$

and the result follows. ■

Lemma 1 gives counting for A_n small, provided that the elements of A_n are also small. We could remove this latter condition if we could define a function $F \in \Delta_0^N$ such that $F_n\colon A_n \Vert\!\!\rightarrow \beta_n$ for some small β_n. This we now do.

Lemma 3. *There is a function $F \in \Delta_0^N$ such that*

$$F_n\colon A_n \Vert\!\!\rightarrow |A_n|^2 \log(n)^3\,.$$

Proof. Let $C = \{a_1 - a_2 |\ a_1, a_2 \in A_n \text{ and } a_1 > a_2\}$ so $|C| \leqslant |A_n|^2$. Each $b \in C$ is divisible by at most $\log(b)$ $(\leqslant \log(n))$ primes so

$$|\{p | p \text{ prime and } p | b \text{ some } b \in C\}| \leqslant |A_n|^2 \log(n)\,.$$

Let p be the least prime not in this set. Then $p \leqslant |A_n|^2 \log(n)^3$ since by the prime number theorem there are more than $|A_n|^2 \log(n)$ primes below $|A_n|^2 \log(n)^3$. Then for $a_1, a_2 \in A$, $a_1 < a_2$, $a_1 \bmod p \neq a_2 \bmod p$ since $a_1 - a_2 \in C$ and $p \nmid a_1 - a_2$. Now let F_n be the map sending $a \in A_n$ to $a \bmod p$. ■

We now have

Corollary 4. *Let $q \in N$. Then the function G is in Δ_0^N where*

$$G(n) = \min(|A_n|, \log(n)^q + 1)\,.$$

Proof. By Lemma 3 there is $F \in \Delta_0^N$ such that

$$F_n\colon A_n \Vert\!\!\rightarrow |A_n|^2 \log(n)^3\,.$$

If $\max(F_n'' A_n) \geqslant (\log(n)^q + 1)^2 \log(n)^3$ then certainly $|A_n| \geqslant \log(n)^q + 1$ and we can set $G(n) = \log(n)^q + 1$.

Otherwise, $F_n'' A_n \subseteq (\log(n)^q + 1)^2 \log(n)^3 \subseteq \log(n)^{2q+4}$, and by Corollary 2 there is a function $H \in \Delta_0^N$ such that, for such n, $H(n) = |F_n'' A_n| = |A_n|$. In this case then set $G(n) = \min(H(n), \log(n)^q + 1)$. ■

By taking $A_n = B \cap n$ for $B \in \Delta_0^N$, $B \subseteq N$ we now have immediately

Theorem 5 (The Counting Theorem). *Let $B \in \Delta_0^N$, $B \subseteq N$ and suppose that for some $k \in N$, $|B \cap n| \leqslant \log(n)^k$ for all n. Then the function G defined by*

$$G(n) = |B \cap n|$$

is in Δ_0^N. ■

This theorem shows that we can count very sparse sets. We conjecture that this result cannot be improved (even though the best 'oracle independence' results known are not this fine, see [1]).

However we shall later show that we can always find a 'fair' approximation to G which is in Δ_0^N. This will be an immediate corollary to Theorem 6 which is an improvement on Lemma 3.

Before proving Theorem 6 however we shall reconsider Theorem 5 from a different viewpoint.

An unfortunate feature of the proof of Theorem 5 is its reliance on the prime number theorem. Consequently at this time the proof cannot easily be extended from the standard model to other weak number systems. To remedy this we shall give an alternate proof of Theorem 5 which does generalize. (The reader who thinks that one proof of Theorem 5 is more than enough can skip to Theorem 6 without loss of continuity.)

We first introduce some notation. Let $I\Delta_0$ be Peano's Axioms but with induction restricted to Δ_0 formulae. Let $M \models I\Delta_0$ and let Δ_0^M be those subsets of M^k $(k \in N)$ definable in M using a Δ_0 formula and parameters from M. Generalizing for the moment the earlier notations let $A \subseteq M^{s+2}$, $A \in \Delta_0^M$ and for $n \in M$ let

$$A_n(\vec{x}) = \{m|\ \langle \vec{x}, n, m\rangle \in A \ \&\ m < n\}.$$

Again we suppress mention of $\vec{x}$. Also $n \in M$ is always assumed large and standard or nonstandard.

We now wish to prove Theorem 5 with M in place of N. An immediate difficulty, however, is that for $n \in M$ the size of A_n, "$|A_n|$", may have no meaning in M. So instead of talking about size we must talk about bijections, injections etc. Notice that Lemma 1 holds for M using essentially the same proof. Precisely:

LEMMA 1′. *Let $k \in N$, $\alpha < 1$, α standard rational, and assume that for all $n \in M$, $A_n \subseteq 2^{\log(n)^\alpha}$. Then there is an increasing function $G \in \Delta_0^M$ such that for all $n \in M$ either $\exists \beta \leqslant n$, G_n: $\log(n)^k \mathrel{\|\!\!\twoheadrightarrow} A_n \cap \beta$ or $\exists \beta < \log(n)^k$, G_n: $\beta \mathrel{\|\!\!\twoheadrightarrow} A_n$.* ■

A second difficulty in the proof of Theorem 5 for M is that since it is still open whether the Δ_0 pigeon hole principle, Δ_0-PHP, (see [1]) holds in M it would seem possible that A_n could have several different 'sizes'. Fortunately for small sets this cannot occur. This is a consequence of the following result which is proved in [1].

log-Δ_0PHP. *Let $F \in \Delta_0^M$, $a \in M$, $k \in N$. Then F does not map* $\log(a)^k+1$ 1—1 *into* $\log(a)^k$. ■

We shall use this result repeatedly in what follows. We are now ready to prove:

THEOREM 5′. *Let $k \in N$, $A \in \Delta_0^M$. Then there is a function $F \in \Delta_0^M$ such that for all $n \in M$, either F_n: $\log(n)^k \mathrel{\|\!\!\rightarrow} A_n$ or $\exists \beta < \log(n)^k$, F_n: $\beta \mathrel{\|\!\!\twoheadrightarrow} A_n$.*

Proof. We shall prove the theorem with k replaced by α for an unbounded set of standard rational α. More exactly we shall prove the result for $\alpha = 1/2$ and then show that if the theorem holds for α then it holds for $\alpha+1/4$.

Firstly though we introduce a little notation. Throughout we will be working with elements of M so when we talk of subsets of elements of M we shall mean subsets coded in M. With this convention let $S \subseteq \log(n)+1$. Then by Lemma 1′ and the log-Δ_0PHP there is a unique function in Δ_0^M which enumerates S in increasing order, uniformly in S. So for such small S we can unambiguously talk about '$|S|$' and 'the jth element of S'. Let $S = \{i_0, \ldots, i_e\}$ in ascending order.

For $a < n$, $a = \sum\limits_{i \leqslant \log(n)} a_i 2^i$ in binary let

$$a[S] = \sum_{j \leqslant e} a_{i_j} 2^j (< 2^{|S|}).$$

Proof of the theorem for $\alpha = 1/2$. Let S be as above and define

$$T(S, n) = \{t < 2^{|S|}|\ \exists a \in A_n,\ a[S] = t\},$$
$$V(S, n) = \{a \in A_n|\ \exists t \in T(S, n)\ (a[S] = t \wedge \forall y \in A_n\ (y < a \rightarrow y[S] \neq t))\}.$$

Then, uniformly in the parameter, by Lemma 1′ there is a Δ_0^M function from $T(S, n)$ 1—1 onto $V(S, n) \subseteq A_n$. Furthermore if we limit ourselves to those S with $|S| \leqslant \log(n)^{\frac12}$ then $T(S, n) \subseteq 2^{\log(n)^{\frac12}}$ so by Lemma 1′ there is a function $G \in \Delta_0^M$ such that for such S either

$$G(S, n)\colon \log(n)^{\frac12} \mathrel{\|\!\!\rightarrow} V(S, n)$$

or

$$G(S, n)\colon \beta \mathrel{\|\!\!\twoheadrightarrow} V(S, n) \text{ some } \beta < \log(n)^{\frac12}.$$

If the former holds for some such S let $F_n = G(S, n)$ for the least such S. Otherwise, let β be maximal such that the latter condition holds for some S, $|S| \leqslant \log(n)^{\frac12}$. We claim that for this S, $G(S, n)$ maps β onto A_n.

To see this assume not. Let $a_j = G(S, n)(j)$ for $j < \beta$ and let $a_\beta \in A_n - G(S, n)``\beta$. Then by induction on $i \leqslant \beta$

$$\exists S_i \subseteq \log(n)+1,\ |S_i| \leqslant i \ \&\ \forall j_1, j_2 \leqslant i(j_1 \neq j_2 \rightarrow a_{j_1}[S_i] \neq a_{j_2}[S_i]).$$

This is clear for $i = 0$. Assuming the result for $i < \beta$ it follows that there is at most one $j < i+1$ such that $a_j[S_i] = a_{i+1}[S_i]$. So adding at most one number to S_i gives S_{i+1} with the required property.

Now for $i \leqslant \beta$ let $b_i \in A_n$ be minimal such that $b_i[S_\beta] = a_i[S_\beta]$. Then the function sending $i \leqslant \beta$ to b_i is in Δ_0^M and maps $\beta+1$ 1—1 into $V(S_\beta, n)$. But $|S_\beta| \leqslant \beta+1 \leqslant \log(n)^{1/2}$ so

$$G(S_\beta, n)\colon \delta \mathrel{\|\!\!\twoheadrightarrow} V(S_\beta, n)$$

for some $\delta \leqslant \beta$ (by choice of β) and by the log-Δ_0PHP we have a contradiction.

Hence $G(S, n)$ maps β 1—1 onto A_n and we can put $F_n = G(S, n)$.

Proof of the theorem for $\alpha+1/4$ assuming it for α. We first introduce a little more notation. Let B be the set of maps $f\colon S \rightarrow 2$ where $S \subseteq \log(n)+1$ and $|S| \leqslant \log(n)^{1/3}$. Notice that $f \in B$ can be coded by a number $\leqslant (2\log(n)+1)^{\log(n)^{1/3}} < 2^{\log(n)^{2/5}}$. For $f \in B$ and $a \in A_n$ let $a = \sum\limits_{i \leqslant \log(n)} a_i 2^i$ in binary and let

$$a \in A_{n,f} \Leftrightarrow \forall i \in \operatorname{dom}(f),\ f(i) = a_i.$$

Applying the theorem for α to these $A_{n,f}$ sets gives a function $R \in \Delta_0^M$ such that for $f \in B$

$$R_{n,f}\colon \log(n)^\alpha \mathrel{\|\!\!\rightarrow} A_{n,f} \text{ (written } |A_{n,f}| \geqslant \log(n)^\alpha)$$

or

$$\exists \beta < \log(n)^\alpha,\ R_{n,f}\colon \beta \twoheadrightarrow A_{n,f} \text{ (written } |A_{n,f}| = \beta).$$

Let Q be the set of coded subsets T of B such that T has code less than n and if $f \in T$ and $f = \{\langle a_0, i_0\rangle, \ldots, \langle a_p, i_p\rangle\}$ with $a_0 < a_1 < \ldots < a_p$ then

(i) for $q < p$, $\{\langle a_0, i_0\rangle, \ldots, \langle a_q, i_q\rangle\} \in T$;
(ii) $\{\langle a_0, i_0\rangle, \ldots, \langle a_{p-1}, i_{p-1}\rangle, \langle a_p, 1-i_p\rangle\} \in T$;
(iii) a_p is the least $b > a_{p-1}$ such that $|A_{n,g_0}|, |A_{n,g_1}| \geqslant \log(n)^\alpha$ where

$$g_0 = \{\langle a_0, i_0\rangle, \ldots, \langle a_{p-1}, i_{p-1}\rangle, \langle b, 0\rangle\},$$
$$g_1 = \{\langle a_0, i_0\rangle, \ldots, \langle a_{p-1}, i_{p-1}\rangle, \langle b, 1\rangle\}.$$

Concerning the coding of $T \in Q$ we assume that T is coded as $\sum_{i \leqslant r} e_i 2^{i \log(n)^{2/5}}$ where $T = \{e_i |\ i < r\}$. Notice this code gives a size to T, $(|T|)$ namely $r+1$ and, since $r \leqslant \log(n)^{3/5}$ by the log-Δ_0PHP this size is unambiguous.

Having introduced this notation we start on the proof proper. Let $T \in Q$ and

$$T' = \{f \in T |\ \neg\exists g \in T, g \supset f\}$$

that is T' is the set of tips of the tree T. Since $T' \subseteq 2^{\log(n)^{2/5}}$, by Lemma 1′ there is a Δ_0^M function H such that for each $T \in Q$,

$$H_{n,T}\colon \log(n)^{1/3} \mathrel{\|\!\!\rightarrow} T'$$

or

$$\exists\beta < \log(n)^{1/3}, \quad H_{n,T}\colon \beta \mathrel{\|\!\!\twoheadrightarrow} T'.$$

We now consider two cases

Case 1. For some $T \in Q$, $H_{n,T}\colon \log(n)^{1/3} \mathrel{\|\!\!\rightarrow} T''$.

Pick the least such T. Then since $\{A_{n,f} | f \in T'\}$ form a partition of A_n (proved by induction on $T \in Q$) and since $|A_{n,f}| \geqslant \log(n)^\alpha$ for $f \in T'$, we can easily define a Δ_0^M function mapping from $\log(n)^{1/3} \cdot \log(n)^\alpha$ 1--1 into A_n. From this we can easily construct $F_n\colon \log(n)^{\alpha+1/4} \mathrel{\|\!\!\rightarrow} A_n$.

Case 2. Not case 1.

Let β be maximal such that for some $T \in Q$, $H_{n,T}\colon \beta \mathrel{\|\!\!\twoheadrightarrow} T'$. Notice $\beta < \log(n)^{1/3}$. Pick the least such T and let $f \in T'$.

Claim. *Let $b \in (\log(n)+1) - \mathrm{dom}(f)$ and let*

$$f_0^b = f \cup \{\langle b, 0\rangle\}, \quad f_1^b = f \cup \{\langle b, 1\rangle\}.$$

Then it is not the case that $|A_{n,f_0^b}|, |A_{n,f_1^b}| \geqslant \log(n)^\alpha$.

Proof of the claim. By (iii) in the definition of Q this is true if $b < \max(\mathrm{dom}(f))$ so assume the claim fails and $b > \max(\mathrm{dom}(f))$ is the least b for which $|A_{n,f_0^b}|$, $|A_{n,f_1^b}| \geqslant \log(n)^\alpha$. Let

$$T^+ = T \cup \{f_0^b, f_1^b\}.$$

Then $T^+ \in Q$. To see this first notice that $f_0^b \in B$ (and similarly $f_1^b \in B$) since if $|\mathrm{dom}(f_0^b)| > \log(n)^{1/3}$, then $|\mathrm{dom}(f)| \geqslant \log(n)^{1/3}$. But then if

$$f = \{\langle a_0, i_0\rangle, \ldots, \langle a_p, i_p\rangle\}$$

with $a_0 < a_1 < \ldots < a_p$, then the Δ_0^M map sending $j < \log(n)^{1/3}$ to the least $g \in T'$ such that

$$\{\langle a_0, i_0\rangle, \ldots, \langle a_{j-1}, i_{j-1}\rangle, \langle a_j, 1-i_j\rangle\} \subseteq g$$

maps $\log(n)^{1/3}$ 1—1 into T' which is impossible by the log-Δ_0PHP. So to show $T^+ \in Q$ it only remains to show that T^+ has a code less than n. But condition (ii) in the definition of Q ensures that $|T| \leqslant 2|T'|$ (proved by the induction on $T \in Q$) so $|T^+| \leqslant 2\beta + 2 < 2\log(n)^{1/3} + 2$. Hence T^+ can be suitably coded by a number less than

$$(2^{\log(n)^{2/5}})^{\log(n)^{1/3}} < n.$$

Hence $T^+ \in Q$. But clearly we have a Δ_0^M map from $\beta+1$ 1—1 onto $(T^+)'$ whilst

$$H_{n,T^+}\colon \delta \mathrel{\|\!\!\twoheadrightarrow} (T^+)' \text{ some } \delta \leqslant \beta$$

so this is a contradiction by the log-Δ_0PHP. This proves the claim.

Now let $f \in T'$. We shall describe a Δ_0^M function K such that

$$K_{n,f}\colon A_{n,f} \mathrel{\|\!\!\rightarrow} \log(n)^{2+\alpha}.$$

There are two subcases.

Subcase 2a. $\exists b \in (\log(n)+1) - \mathrm{dom}(f)$ such that $|A_{n,f_0^b}|, |A_{n,f_1^b}| < \log(n)^\alpha$. In this case the required function $K_{n,f}$ is clear since

$$A_{n,f} = A_{n,f_0^b} \cup A_{n,f_1^b}.$$

Subcase 2b. Not subcase 2a.

Then there is a map $r\colon (\log(n)+1) \rightarrow 2$, $r \in M$, extending f such that for all $b \in (\log(n)+1) - \mathrm{dom}(f)$

$$|A_{n,f_{r(b)}^b}| \geqslant \log(n)^\alpha, \quad |A_{n,f_{1-r(b)}^b}| < \log(n)^\alpha.$$

It is now easy to see that we can define a Δ_0^M map from $\bigcup_{\substack{b \leqslant \log(n) \\ b \notin \mathrm{dom}(f)}} A_{n,f_{1-r(b)}^b}$ 1—1 into $(\log(n)+1)\log(n)^\alpha < \log(n)^{2+\alpha}$.

Hence since this set differs by at most the element r from $A_{n,f}$, we can define the required Δ_0^M map $K_{n,f}$ from $A_{n,f}$ 1—1 into $\log(n)^{2+\alpha}$.

Having now defined K and noticing that $\{A_{n,f} | f \in T'\}$ form a partition of A_n, we can combine K with H^{-1} to give a Δ_0^M map from A_n 1—1 into $\beta\log(n)^{\alpha+2} \leqslant \log(n)^{7/3+\alpha}$. By Lemma 1′ and the log-Δ_0PHP we have a Δ_0^M function from δ 1—1 onto A_n for some $\delta \leqslant \log(n)^{7/3+\alpha}$ and the required F_n is easily obtained. ■

Theorem 6 (The Collapsing Theorem). *Let $1 < k \in N$. Then there is a constant α depending only on k and a function $F \in \Delta_0^N$ such that*

$$F_n\colon A_n \mathrel{\|\!\!\rightarrow} \alpha|A_n|^{1+\beta}\log(n)$$

where $\beta = \dfrac{\log|A_n|}{k\log(n)}$.

Proof. We first explain the idea of the proof and then apply it several times with different values for the parameters to give the required result.

To simplify the notation we shall write A for A_n. Let $\gamma \geqslant 1/2$ and let B be the set of primes between $n^{1/2}$ and $n^{\gamma}\log(n)$ so by the prime number theorem (for n large), $|B| \geqslant n^{\gamma}$. (Recall all logs are to base 2). For $x \in A$ let

$$Z_x = \{p \in B \mid \exists y \in A, y \neq x \,\&\, y \equiv x \bmod p\}.$$

Then $|Z_x| < |A|$ since if $|Z_x| \geqslant |A|$ there would be $y \in A$, $y \neq x$ and distinct primes $p, q \in B$ such that $x \equiv y \bmod p$ and $x \equiv y \bmod q$. But then since $p, q \geqslant n^{1/2}$,

$$n \leqslant pq \leqslant |y-x| < n$$

giving a contradiction.

Now suppose that $t \in N$ is such that $|A|^{1+t} < n^{\gamma t}$. Then

$$|\bigcup_{x \in A} Z_x^t| \leqslant |A|^{1+t} < n^{\gamma t} \leqslant |B^t|$$

and so $B^t - \bigcup_{x \in A} Z_x^t \neq \emptyset$. Hence there is a sequence p_i, $i<t$ of primes from B such that for each $x \in A$ there is a (least) $i<t$ such that for all $y \in A-\{x\}$, $y \not\equiv x \bmod p_i$. Thus if $K(x) = \langle i, x \bmod p_i \rangle$ then

$$K\colon A \Vert\!\!\rightarrow t\max B \leqslant tn^{\gamma}\log(n).$$

The idea is to show that there exist t, γ such that this range is small and $K \in \Delta_0^N$. Of course, K will depend on the sequence p_i, $i<t$. However, this dependence will be uniform so by taking the best K we can obtain the required function F_n.

We now consider a number of cases.

Case 1. $|A| \geqslant n^{1/2}$. Put $\gamma = \dfrac{\log|A|}{\log(n)} + \dfrac{(\log|A|)^2}{k(\log(n))^2}$ and

$$t = 1 + \left[\frac{(k+1)\log(n)}{\log|A|}\right].\ \text{Then } \gamma > \tfrac{1}{2} \text{ and } n^{\gamma t} > |A|^{1+t}.$$

In this case the sequence p_i, $i<t$ can be coded by a number at most $n^t \leqslant n^{2k+3}$ so $K \in \Delta_0^N$. Also

$$tn^{\gamma}\log(n) = \left(1 + \left[\frac{(k+1)\log(n)}{\log|A|}\right]\right)\log(n)\, n^{\frac{\log|A|}{\log(n)} + \frac{(\log|A|)^2}{k(\log(n))^2}} \leqslant \alpha\log(n)\cdot|A|^{1+\frac{\log|A|}{k\log(n)}}$$

as required.

Case 2. $n^{49/100} \leqslant |A| < n^{1/2}$. Put $\gamma = 53/100$, $t = 20$. Then we obtain a map $K_0 \in \Delta_0^N$,

$$K_0\colon A \Vert\!\!\rightarrow 20n^{53/100}\log(n) < n^{11/20}.$$

Put $A_0 = K_0``A \subseteq n^{11/20} = n_0$. Then $|A_0| = |A| \geqslant n^{49/100} > n_0^{1/2}$.

Applying Case 1 with $2k$ in place of k now gives a map in Δ_0^N from A_0 1—1 into $\alpha\log|A_0|\cdot|A_0|^{1+\frac{\log|A_0|}{2k\log(no)}}$ and the required map K exists.

Case 3. $|A| < n^{49/100}$. If $|A| < \log(n)^j$ for some sufficiently large j then obviously the theorem follows by Theorem 5. Otherwise by Lemma 3 there is $L \in \Delta_0^N$,

$$L\colon A \Vert\!\!\rightarrow |A|^{100/49}.$$

Put $A_1 = L``A$, $n_1 = \max A_1 + 1$ so $A_1 \subseteq n_1$ and $|A_1| \geqslant n_1^{49/100}$. Now as in Case 2 produce $K_0 \in \Delta_0^N$, $K_0\colon A_1 \Vert\!\!\rightarrow n_2 \leqslant |A|^2$ and put $A_2 = K_0``A_1$. Finally apply the main construction with n_2, A_2 in place of n, A and

$$t = 1 + \left[\frac{(k+1)\log(n)}{\log|A|}\right], \qquad \gamma = \frac{\log|A|}{\log(n_2)} + \frac{\log(n_2)}{k\log(n)}$$

to obtain $K\colon A_2 \Vert\!\!\rightarrow tn_2^{\gamma}\log(n_2)$. Then $K \in \Delta_0^N$ since the sequence p_i, $i<t$ can be coded by $n_2^{\gamma}\log(n_2)$ and a number at most $2(n_2^{\gamma}\log(n_2))^t$ $(<n^c)$ for some fixed c. Finally, since

$$tn_2^{\gamma}\log(n_2) \leqslant \alpha\log(n)|A|^{1+\frac{4\log|A|}{k\log(n)}},$$

the result follows by replacing k by $4k$. ■

Remarks (i). Suppose $|A| \leqslant 2^{\sqrt{\log n}}$. If we now proceed as in Case 3 but using instead

$$t = 1 + [(k+1)\log|A|], \qquad \gamma = \frac{\log|A|}{\log(n_2)} + \frac{\log(n_2)}{k(\log A)^2}$$

we obtain a Δ_0^N function from A 1—1 into $\alpha|A|(\log|A|)^2$.

(ii) The method of proof of Theorem 6 was inspired by the proof of a theorem due to Sipser, see [3]. Sipser shows that if $A \subseteq n$ and $|A| \leqslant 2^{m-1}$ then, treating $2^{\log(n)+1}$ as an n dimensional vector space over Z_2 there is a linear map $L\colon 2^{\log(n)+1} \rightarrow 2^m$ such that

$$|\{x \in A \mid \forall y \in A-\{x\},\ L(x) \neq L(y)\}| \geqslant |A|/2.$$

By repeated use of this we can obtain a 1—1 map from A into $4(1+\log|A|)|A|$ and furthermore if $|A| \leqslant 2^{\log(n)^{1/3}}$ then this map is (uniformly) in Δ_0^N. For such small A this appears to be better than results obtained by using Theorem 6. Clearly, then this area begs to be tidied up.

COROLLARY 7. *Given $\varepsilon > 0$ there is a function $G \in \Delta_0^N$ such that for all n*

$$|A_n| \leqslant G(n) \leqslant |A_n|^{1+\varepsilon}. ■$$

COROLLARY 8. *Given $\varepsilon > 0$ there is a function $G \in \Delta_0^N$ such that whenever $(\log\log(n)\cdot\log|A_n|)^2 \leqslant \log(n)$, then*

$$|A_n| \leqslant G(n) \leqslant (1+\varepsilon)|A_n|.$$

Proof. Assume that $(\log\log(n)\cdot\log|A_n|)^2 \leqslant \log n$. Then applying Theorem 6 and simplifying there is $F \in \Delta_0^N$ such that $F_n\colon A_n \Vert\!\!\rightarrow 2^{\sqrt{2\log(n)\log\log(n)}}$. Let $B_n = F_n``A_n$ and let $C_n = B_n^{b[\log\log(n)]}$ where $b \in N$ is large. Then again by Theorem 6 with $k = b$

there is $K \in \Delta_0^N$ such that

$$K_n\colon\ C_n \Vdash\!\!\to \alpha\log(n)\cdot|C_n|^{1+\sqrt{\frac{2}{\log(n)}}} \leqslant 4\alpha\log(n)\cdot|C_n|\,.$$

Let $E(n) = \max K_n``C_n$, $G(n) = [E(n)^{1/b[\log\log n]}]$. Then $|C_n| \leqslant E(n) \leqslant 4\alpha\log(n)|C_n|$ so

$$|A_n| = |B_n| = |C_n|^{1/b[\log\log(n)]} \leqslant G(n) \leqslant \big(4\alpha\log(n)\cdot|B_n^{b[\log\log(n)]}|\big)^{1/b[\log\log(n)]}$$
$$\leqslant (4\alpha\log(n))^{1/b[\log\log(n)]}\cdot|B_n| \leqslant (1+\varepsilon)|B_n| = (1+\varepsilon)|A_n|$$

since b is large. ∎

Conclusion. In conclusion we state a couple of problems which are related to this theme.

(i) Let $B \in \Delta_0^N$, $B \subseteq N$. By considering the case $\exists i < n^{1/2}$, $[in^{1/2}, (i+1)n^{1/2}) \cap B = \emptyset$ and its negation it is easy to see that there is a function $F \in \Delta_0^N$ such that for all n, $F_n\colon\ n^{1/2} \Vdash\!\!\to B\cap n$ or $F_n\colon\ n^{1/2} \Vdash\!\!\to (n-B)$. Using our results $n^{1/2}$ can be improved to $n^{1/2}\log(n)^k$ is this best possible?

(ii) Let M be a nonstandard model of true arithmetic and let $a \in M$ be a nonstandard. Say that $c < a$ is Δ_0-definable from a in M if for some Δ_0 formula $\theta(x, y)$

$$M \vDash \theta(a, c) \wedge \exists! y\ \theta(a, y)\,.$$

Now suppose that $\psi(x, y, z)$ is a Δ_0 formula, $c < a$ and

$$M \vDash |\{b < a|\ \psi(a, c, b) \wedge \exists! y\ \psi(a, y, b\}| \text{ is `large'}\,.$$

Is c Δ_0-definable from a?

Of course, this depends on what we mean by 'large'. Using the second counting theorem the answer is yes when 'large' means $\geqslant a - a^{1-\varepsilon}$ for some standard $\varepsilon > 0$. However, the answer is no if we take 'large' to mean $\geqslant a/t$ for some fixed nonstandard $t \in M$. We conjecture that the answer is yes when by 'large' we mean $\geqslant a/n$ for some $n \in N$.

References

[1] J. Paris, A. Wilkie, *Counting problems in bounded arithmetic*, to appear in the proceedings of the VI-th Latin American Logic Conference, Caracus 1983.

[2] — — *Δ_0 sets and induction* in *Open Days in Model Theory and Set Theory*, Proceedings of the Jadwisin, Poland, Logic Conference 1981. Published by Leeds University, 1983.

[3] M. Sipser, *A complexity theoretic approach to randomness*, Proc. A.C.M. 1983, 330–335.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF MANCHESTER
Manchester M12 9PL
England

Received 17 July 1985