数理解析研究所講究録
912巻 1995年 47-56

FORCING ON A NONSTANDARD MODEL OF ARITHMETIC

SATORU KURODA
(黒田 覚)

Graduate School of Human Informatics, Nagoya University
(名古屋大学人間情報学研究科)

1. INTRODUCTION

One of the main subjects in the study of weak fragments of arithmetic is to determine which arithmetical or combinatorial proposition is provable in the weak theories.

The first significant advance in the research of weak fragments was done by R.Parikh [4]. He proved that $I\Delta_0$ cannot treat functions of exponential growth, while most of proofs in the elementary number theory, such as the infinitude of primes, require exponentiation.

J.Paris and A.Wilkie [6] pointed out that Δ_0-PHP implies the infinitude of primes and asked whether $I\Delta_0$ proves Δ_0-PHP, where Δ_0-PHP states that no Δ_0-formula can define a bijection from n to $n-1$. A positive answer to this problem suggests that there is an essentially new proof of the infinitude of primes since, as stated before, all known proofs require exponentiation.

Paris, Wilkie and Woods [5] proved that $I\Delta_0 + \Omega_1$ can prove a weak version of PHP namely, $\neg\exists f : n^{1+\varepsilon} \xrightarrow{1\text{-}1} n$. But the original problem remains unsolved.

M.Ajtai [1] proved the relativized version of this problem, i.e. if we extend the language by a function symbol f, then $I\Delta_0(f)$ cannot prove that f is not a bijection from n to $n-1$. He used the forcing method to construct $f : n \xrightarrow{1\text{-}1} n-1$ and the proof used the following fact by Paris and Wilkie [6].

Fact. *The following statements are equivalent*

1. $I\Delta_0(f) \nvdash \neg f : n \xrightarrow{1\text{-}1} n-1$.

2. There is no propositional proof for PHP of constant depth and polynomial size.

In this note, we modify Ajtai's method and construct a concrete "generic" model of $I\Delta_0(f)$.

2.Preliminaries

We use the language $\mathcal{L} = \{0, 1, +, \cdot, <, =\}$. PA$^-$ is the $\mathcal{L}$-theory Peano Arithmetic less induction. For a set of formulae Γ we denote the induction scheme for all $\varphi \in \Gamma$ by Γ-IND. Similarly, the least number principle scheme is denoted by Γ-LNP. It is easily seen that Δ_0-IND and Δ_0-LNP are equivalent over PA$^-$. $I\Delta_0$ is the $\mathcal{L}$-theory PA$^-$ $+\Delta_0$-IND.

Let f be a function symbol. $\mathcal{L}(f) = \mathcal{L} \cup \{f\}$. $I\Delta_0(f)$ is the $\mathcal{L}(f)$-theory defined in the same manner as $I\Delta_0$. PHP(f) denotes the statement "f is not a bijection from n to $n-1$."

Let M be a countable nonstandard model of PA and fix $n \in M \setminus \omega$.

Definition. (Forcing condition) Let $M_n = \{x \in M \ : \ M \models x < n\}$, then we call the following set $\mathbb{P}$ a forcing condition. First define H_n as,

$$H_n = \left\{ g \ : \ \begin{matrix} \text{a bijection from } A \subset M_n \text{ to } B \subset M_{n-1} \\ \text{and } g \text{ is definable in M} \end{matrix} \right\}.$$

For $\varepsilon > 0$ let $P_\varepsilon = \{g \in H_n \ : \ M \models |\text{dom}(g)| \leq n - n^\varepsilon\}$ and $\mathbb{P} = \bigcup_{\substack{\varepsilon \in Q \\ \varepsilon > 0}} P_\varepsilon$.

For $g, h \in \mathbb{P}$ we define a order relation in $\mathbb{P}$ by $g \leq h$ iff $h \subseteq g$.

Definition. Let $D \subseteq \mathbb{P}$. We say D is dense in $\mathbb{P}$ iff for all $g \in \mathbb{P}$ there exists $h \in D$ such that $h \leq g$.

For $p \in \mathbb{P}$, D is dense below p iff for all $g \leq p$ there exists $h \in D$ such that $h \leq g$.

Definition. Let $D \subseteq \mathbb{P}$. D belongs to M iff for some $\mathcal{L}$-formula $\psi(x, y)$ $g \in D \Leftrightarrow \exists k \in \omega \ M \models \psi(c_g, k)$.

Definition. (Generic filter) Let $G \subseteq \mathbb{P}$. G is a $\mathbb{P}$-generic over M iff the following conditions hold:

(1) $\forall g \in G \ \forall h \in \mathbb{P} \ g \leq h \rightarrow h \in G$.
(2) $\forall g, g' \in G \ \exists h \in G \ h \leq g \ \& \ h \leq g'$.
(3) D is dense in $\mathbb{P}$ & belongs to $M \rightarrow G \cap D \neq \emptyset$.

Proposition 1. *For all $g \in \mathbb{P}$ there exists a $\mathbb{P}$-generic over M G such that $g \in G$.*

Definition. Let $f, g \in \mathbb{P}$. f and g are compatible iff for some $h \in \mathbb{P}$ $h \leq f$ and $h \leq g$ holds. Otherwise g and h are incompatible. We denote $f \perp g$ if f and g are incompatible.

Proposition 2. *Let D belongs to M and G be a $\mathbb{P}$-generic over M then*

(1) *either $G \cap D \neq \emptyset$ or $\exists h \in G \ \forall f \in D \ f \perp h$*
(2) *$g \in G$ & G is dense below $g \rightarrow G \cap D \neq \emptyset$.*

Definition. If $G \subseteq \mathbb{P}$ is a $\mathbb{P}$-generic over M we call $\tilde{f} = \bigcup_{f \in G} f$ a generic map.

Proposition 3. *A generic map $\tilde{f}$ is a bijection from M_n to M_{n-1}.*

For the proof of Proposition 1 to 3, refer e.g. Kunen [3].

3. Main Proof

Let $N_k = \{x \in M : M \models x < n^k\}$ and $N = \bigcup_{k \in \omega} N_k$. We consider N_k as a submodel of N by regarding $+$ and $\cdot$ as relation symbols. Our main theorem is stated as follows.

Main Theorem. *If $\tilde{f}$ is a generic map then $(N, \tilde{f}) \models I\Delta_0(f)$.*

Main theorem is a consequence of the following theorem.

Theorem 1. *For all $k \in \omega$, $(N_k, \tilde{f}) \models$ IND.*

Proof of Main Theorem. Let $\varphi \in \Delta_0(f)$. It suffices to show that

$$(N, \tilde{f}) \models \exists x \varphi(x) \to \exists x (\varphi(x) \wedge \forall y < x \neg\varphi(y)).$$

Suppose $(N, \tilde{f}) \models \exists x \varphi(x)$. Then there exists $k \in \omega$ and $a \in N_k$ such that $(N, \tilde{f}) \models \varphi(a)$ and all parameters in $\varphi(a)$ are from N_k. As $N_k \subseteq_e N$,

$$(N_k, \tilde{f}) \models \varphi \text{ iff } (N, \tilde{f}) \models \varphi$$

holds for any Δ_0-formula φ. So $(N_k, \tilde{f}) \models \exists x \varphi(x)$. By Theorem 1

$$(N_k, \tilde{f}) \models \exists x (\varphi(x) \wedge \forall y < x \neg\varphi(y)).$$

Therefore there exists $a_0 \in N_k$ such that $(N_k, \tilde{f}) \models \varphi(a_0) \wedge \forall y < a_0 \neg\varphi(y)$. As $\varphi(a_0) \wedge \forall y < a_0 \varphi(y) \in \Delta_0(f)$, $(N, \tilde{f}) \models \varphi(a_0) \wedge \forall y < a_0 \neg\varphi(y)$. So

$$(N, \tilde{f}) \models \exists x \varphi(x) \wedge \forall y < x \neg\varphi(y).$$

QED.

Next we prove Theorem 1. First let us sketch the proof.

Let $S = \{x \in N_k : (N_k, \tilde{f}) \models \varphi(x)\}$ for $\varphi \in \mathcal{L}(f)$. It suffices to prove that S is definable in M since we can apply the least number principle in M to get the minimal element of S. In the first step we show that it is enough to consider $S' = \{x < k \log n : (N_k, \tilde{f}) \models \varphi(x)\}$ instead of whole S. Secondly, we prove that there exists a M-definable function d such that for all $u \leq k \log n$

$$(N_k, \tilde{f}) \models \varphi(u) \text{ iff } d(u) = 1.$$

We use the property of generic set in the proof but we have a little difficulty since we don't have a "forcing relation" which is definable in M so forcing lemma cannot be proved. Instead we prove a modified forcing lemma using the method of partial assignment developed by Ajtai.

The two steps described above are expressed as the following two lemmas.

Lemma 1. *Suppose for all $\varphi \in \mathcal{L}(f)$,*

$$(N_k, \tilde{f}) \models \exists x < k \log n \varphi(x) \rightarrow \exists x(\varphi(x) \wedge \forall y < x \neg\varphi(y)).$$

Then $(N_k, \tilde{f}) \models \mathrm{LNP}$.

proof. Let $m = n^k$. Assume $(N_k, \tilde{f}) \not\models \mathrm{LNP}$, then for some $\varphi(x) \in \mathcal{L}(f)$ with parameters from N_k $S = \left\{x \in N_k : (N_k, \tilde{f}) \models \varphi(x)\right\}$ satisfies the following conditions.

(1). $S \neq \emptyset$.

(2). S does not have the least element.

Claim 1. We can assume that

(3). For all $x, y \in M$ if $x \leq y$ and $x \in S$ then $y \in S$.

proof. Replace φ by $\psi(x) \equiv \exists z \leq x \varphi(z)$. Then ψ trivially satisfies the condition.

Claim 2. We can assume that

(4). if $x \notin S$ then $[x, 2x] \cap S = \emptyset$.

proof. Let $\psi(x) \equiv \exists w, z(x = w - z \wedge \varphi(w) \wedge \neg\varphi(z))$ and

$$S' = \left\{x < m : (N_k, \tilde{f}) \models \psi(x)\right\}.$$

It suffices to prove that ψ satisfies the conditions (1) to (4).

(1). Since $S \neq \emptyset$ there exists $x \in S$ and since S does not have the least element, $0 \notin S$. So $x = x - 0 \in S'$.

(2). Let $x \in S'$ and $x = w - z \wedge \varphi(w) \wedge \neg\varphi(z)$. Then there exists $w' < w$ such that $\varphi(w')$ holds. So $x' = w' - z \in S'$ and $x' < x$.

(3). Let $x \in S'$, $x \leq y$ and w, z be witnesses for x. Let $z' = z - (y - x)$ then $z' \leq z$. So $\neg\varphi(z')$ holds since otherwise S does not satisfy (3). Therefore $y = w - z' \in S'$.

(4). Assume $x \notin S'$ and $y \in [x, 2x] \cap S'$. Then $x \leq y \leq 2x \wedge \psi(y)$ holds. Let w, z be witnesses for $\psi(y)$ and let $u = \left[\frac{w+z}{2}\right]$.

Suppose $(N_k, \tilde{f}) \models \varphi(u)$. Since $\neg\varphi(z)$, $\psi(u - z)$ holds. But as

$$w - z < \frac{w + z}{2} - z = \frac{w - z}{2} = \frac{y}{2} \leq x,$$

$\psi(x)$ holds, which is a contradiction.

Suppose otherwise, then $\psi(w - u)$ holds. But again

$$w - u < w - \left(\frac{w + z}{2} - 1\right) = \frac{w - z}{2} + 1 = \frac{y}{2} + 1 \leq x + 1$$

leads a contradiction.

Now assume S satisfies (1) to (4). Let $\psi(x) \equiv \exists z(z = w^x \wedge \varphi(z))$ and

$$S' = \left\{ x < m : (N_k, \tilde{f}) \models \psi(x) \right\}.$$

Let $x \in M$ be the maximal element such that $2^x < m$. If $2^x \notin S$ then by (4) $S \cap [2^x, 2^{x+1}] = \emptyset$. So this is a contradiction since $S \neq \emptyset$. So $(N_k, \tilde{f}) \models \varphi(2^x)$. Therefore $S' \neq \emptyset$. Trivially $x < k \log n$ holds. So it suffices to show that S' does not have the least element. Let $x \in S'$ and $\varphi(2^x)$ holds. Then by (4) $\varphi(2^{x-1})$ holds. Therefore $x - 1 \in S'$. QED.

Lemma 2. *Let $k \in \omega$, $\varphi \in \mathcal{L}(f)$ and $g \in \mathbb{P}$. Consider the following condition $(*)$ for $h \in P$:*

$(*)$ There exists a function d definable in M such that for all $u < k \log n$ and for all generic $f = \bigcup G$ with $h \in G$,

$$(N_k, \tilde{f}) \models \varphi(u) \text{ iff } d(u) = 1$$

holds.

and let $E_g = \{h \in \mathbb{P} : h \text{ satisfies } (*)\}$. Then there exists $D_g \subseteq E_g$ which is dense below g and belongs to M.

Proof of Theorem 1. By Lemma 1, it suffices to show that $S = \{x < k \log n : (N_k, \tilde{f}) \models \varphi(x)\}$ is definable in M, hence we can apply LNP in M. Fix $g \in G$ and consider D_g in Lemma 2. Then since G is generic there exists $h \in D_g \cap G$. So h satisfies the condition $(*)$. Therefore for some M-definable function d,

$$x \in S \text{ iff } x < k \log x \wedge (N_k, \tilde{f}) \models \varphi(x) \text{ iff } d(u) = 1.$$

QED.

3.Combinatorial Proof.

To prove Lemma 2 it suffices to show that $\{\varphi(0), \cdots, \varphi(k \log n - 1)\}$ is definable in M for each $\varphi(x) \in \mathcal{L}(f)$. The essential part is that we can express the definability in terms of Boolean formula. First we introduce some notions on Boolean formulae.

Let $|D_0| = n, |D_1| = n - 1$. We describe Boolean formulae by the language

$$\wedge, \vee, \neg, 0, 1, x_{ij} \ (i \in D_0, j \in D_1).$$

Let B be the set of all Boolean formulae over the above language.

Definitions.

(1) $\kappa \in B$ is a k-map iff $\kappa = \wedge x_{u,g(u)}$, where $g \subset D_0 \longrightarrow D_1$ is a partial 1-1 map and $|\operatorname{dom}(g)| = k$.

(2) Let $\kappa = \wedge x_{u,g(u)}$ be a k-map and $V \subset D = D_0 \cup D_1$. We say V covers κ iff for all $u \in \operatorname{dom}(g)$ either $u \in V$ or $g(u) \in V$ hold.

(3) Let $\kappa = \wedge x_{u,g(u)}$, $\kappa' = \wedge x_{u,g'(u)}$ be k, k'-map respectively. κ and κ' are contradictory iff $g \cup g'$ is not a (partial) function.

(4) $\varphi \in B$ is a k-disjunction iff $h = \bigvee_{\kappa \in K} \kappa$,where all $\kappa \in K$ are k'-map for some $k' \leq k$. We call φ a map disjunction if it is a k-disjunction for some k. V covers φ iff V covers all $\kappa \in K$. Define

$$\operatorname{Cover}(\varphi) = \min\{|V| : V \text{ covers } \varphi\}.$$

(5) $B(D_0, D_1) \subset B$ is defined as follows:
   (i) If φ is a map disjunction then $\varphi \in B(D_0, D_1)$.
   (ii) If for all $\kappa \in K \mu_\kappa \in B(D_0, D_1)$ then $\bigvee_{\kappa \in K} \mu_\kappa \in B(D_0, D_1)$.
   (iii) If $\mu \in B(D_0, D_1)$ then $\neg\mu \in B(D_0, D_1)$.
   (iv) $B(D_0, D_1)$ is the smallest set satisfying (i) to (iii).

(6) For $\varphi \in B$, depth(φ) is the maximal number of nesting of connectives. size(φ) is the number of all connectives in φ.

The next definition plays a important role in transforming a Boolean formula.

Definition. Let $\varphi = \bigvee_{\kappa \in k} \kappa$ be a k-disjunction, V covers φ and $|V| = l$. Then define $c(\varphi, V) = \bigvee_{\mu \in K'} \mu$, where

$$K' = \left\{ \mu : \begin{array}{c} \mu \text{ is a } j\text{-map for some } j \leq l,\ V \text{ covers } \varphi \\ \text{and } \mu \text{ and } \kappa \text{ are contradictory for all } \kappa \in K. \end{array} \right\}$$

Definition. Let e be a 0-1 assignment and $V \subseteq D$. We say e is 1-1 on V iff e defines a partial 1-1 map f such that $V \subseteq \operatorname{dom}(f) \cup \operatorname{range}(f)$.

Proposition 4. *If a evaluation e is 1-1 on V then* $e(\neg\varphi) = e(c(\varphi, V))$.

The essential idea of the rest of the argument is to reduce the complexity of a given Boolean formula. To do this, we use partial assignment and apply the procedure which we will define later. We borrow techniques from probabilistic combinatorics to show that there exists a partial assignment that is suitable for our need. Therefore we need to define a probabilistic space over partial assignments.

Definition.

$$\Omega^{n,\varepsilon} = \left\{ \rho = < r, s > : \begin{array}{c} s \subset D \text{ s.t.} |s_0| = |s \cap D_0| = n^\varepsilon + 1, |s_1| = |s \cap D_1| = n^\varepsilon \\ r : D_0 \setminus s_0 \longrightarrow D_1 \setminus s_1 \text{ bijection.} \end{array} \right\}$$

$\rho \in \Omega^{n,\varepsilon}$ is considered as a 0-1 assignment defined by

$$\rho(x_{ij}) = \begin{cases} x_{ij} & \text{if } i \in s_0 \text{ and } j \in s_1 \\ 1 & \text{if } r(i) = j \\ 0 & \text{otherwise.} \end{cases}$$

We denote the probability over the space $\Omega^{n,\varepsilon}$ by $\Pr_{\rho}^{n,\varepsilon}[*]$.

If $\rho =< r, s >$ is a partial assignment then we denote ρ by val(r) and r by map(ρ).

Next we define a transformation rule of $\varphi \in B(D_0, D_1)$.

Definition. Let φ be a map disjunction. min(φ) is a map disjunction consisted by all minimal maps in φ.

Definition. Let $\varphi \in B(D_0, D_1)$, depth$(\varphi) = d$ and $\rho \in \Omega^{n,\varepsilon}$. Define a transformation rule of Boolean formulae as follows:

(1). Apply ρ to φ and take min of each map disjunction in φ.
(2). For each map disjunction μ in $\varphi\restriction_\rho$, replace all occurrences of $\neg\mu$ by $c(\mu, V)$.
(3). Merge all $\bigvee$'s at level 2 and 3.

We denote $\varphi \underset{\rho}{\twoheadrightarrow} \psi$ iff ψ is obtained from φ by applying the above rule more than once with partial assignments $\rho_0, \cdots, \rho_t$ and $\rho = \rho_0 \cdots \rho_t$.

Notice that this rule is definable in M for each fixed $\rho \in \Omega^{n,\varepsilon}$.

Theorem 2. *Let* $\varphi \in B(D_0, D_1)$ *be such that* depth$(\varphi) = d$, size$(\varphi) \le n^s$ *and* mapsize$(\varphi) = t$, *then for all* u *there exists* $\varepsilon > 0$ *such that for sufficiently large* n

$$\Pr{}_{<r,s>}^{n,\varepsilon}\left[\begin{array}{l}\exists g:\ k\text{-}disjunction\ s.t.\\ \text{Cover}(g) \le k\ and\ \varphi \underset{\rho}{\twoheadrightarrow} g\end{array}\right] \le 1 - n^{-u}.$$

Theorem is proved from the following Covering Lemma.

Lemma 3. *(Covering Lemma)*

Let g *be a* t*-disjunction,* $0 < \varepsilon < 1/16$, $t = o(\log\log n)$ *and* $8/\varepsilon \le k \le 2n^{\varepsilon^{2t}}$. *Then for a sufficiently large* n

$$\Pr{}_{\rho}^{n,\varepsilon^{2t}}[\text{Cover}(\min(g\restriction_\rho)) > k] \le \alpha_k^{n,t}$$

holds, where $\alpha_k^{n,t} = n^{-\varepsilon^{2t}k/11}$.

Covering Lemma was proved in Bellantoni, Pitassi and Urquhart [2].

Proposition 5. *Let* $0 < \varepsilon < 1/16$, $\varphi \in B(D_0, D_1)$, size$(\varphi) \le n^s$ *and* $8/\varepsilon \le k$ *be a constant such that* $k >$ mapsize$(\varphi) = t$. *Then there exists* $\rho \in \Omega^{n,\varepsilon^{2t}}$ *such that* $\varphi \underset{\rho}{\twoheadrightarrow} \psi$ *and* mapsize$(\psi) \le k$.

proof. Let g be a map disjunciton in φ. Then by the Covering Lemma,

$$\Pr{}_{\rho}^{n,\varepsilon^{2t}}[\exists g \text{ in } \varphi\, \text{Cover}(\min(g\restriction_\rho)) > k] \le n^s \alpha_k^{n,t} < 1.$$

So there exists $\rho \in \Omega^{n,\varepsilon^{2t}}$ such that for all map disjunction g in φ Cover(min$(g\restriction_\rho$ $)) \le k$. This ρ satisfies the requirement of Proposition. QED.

Proof of Theorem. Let $\varphi \in B(D_0, D_1)$ satisfies the condition. Then applying Proposition 5 $d-2$ times there exists a map disjunciton g such that $\varphi \underset{\rho}{\twoheadrightarrow} g$. Notice that each map in g are coverrable by a set of constant size. So mapsize(g) is constant. Hence we can apply Covering Lemma to g to get a map disjunction with suitable size of cover. QED.

4.Proof of Lemma 2

Lemma 4. *Let $\delta > 0$. Consider $\varphi_i \in B(D_0, D_1)$ for $1 \le i \le k \log n$ such that* size$(\varphi_i) \le n^s$*,* depth$(\varphi_i) = d$ *and* mapsize$(\varphi_i) = t$ *and let $\rho \in \Omega^{n,\delta}$. Then there exists $\rho' \in \Omega^{n,\varepsilon}$ such that ρ' is an extension of ρ and $\varphi_i \underset{\rho'}{\twoheadrightarrow} 0$ or $\varphi_i \underset{\rho'}{\twoheadrightarrow} 1$ for all $1 \le i \le k \log n$.*

Proof. Let $\rho \in \Omega^{n,\delta}$, $D'_0 = D_0 \setminus \mathrm{dom}(\rho)$ and $D'_1 = D_1 \setminus \mathrm{range}(\rho)$. Then $\varphi_i \restriction_\rho \in B(D'_0, D'_1)$. Let $(*)_i$ be the condition

$$\exists g_i : k\text{-disjunction s.t.} \,\mathrm{Cover}(g_i) \le k \text{ and } \varphi_i \underset{\rho'}{\twoheadrightarrow} g_i.$$

Then by Theorem $\Pr^{n^\delta,\varepsilon}_{\rho'}[(*)_i \text{ holds}] \ge 1 - n^{-u}$ for all $1 \le i \le k \log n$. So

$$\begin{aligned}\Pr^{n^\delta,\varepsilon}_{\rho'}[\exists i \le k \log n \; (*)_i \text{ does not hold}] &\le \Sigma_{1 \le i \le k \log n} \Pr^{n^\delta,\varepsilon}_{\rho'}[(*)_i \text{ does not hold}] \\ &\le k \log n \cdot n^{1-u}\end{aligned}$$

Therefore taking $u > 1$ we have

$$\Pr^{n^\delta,\varepsilon}_{\rho'}[\forall i \le k \log n \; (*)_i \text{ holds}] \ge 1 - k \log n \cdot n^{1-u} > 0$$

for sufficiently large n. Now fix such $\rho' \in \Omega^{n^\delta,\varepsilon}$ and let V_i cover g_i and $|V_i| \le k$. Then we can take an extension ρ'' of ρ' such that

$$\bigcup_{1 \le i \le k \log n} V_i \subseteq \mathrm{dom}(\rho'') \cup \mathrm{range}(\rho'').$$

Then either $\varphi_i \underset{\rho''}{\twoheadrightarrow} 0$ or $\varphi_i \underset{\rho''}{\twoheadrightarrow} 1$ holds for all $1 \le i \le k \log n$.

Proposition 6. *For all $\varphi \in \mathcal{L}(f)$ there exists $\mu \in B(D_0, D_1)$ such that for any generic $\tilde{f} = \bigcup G$*

$$(M_n, \tilde{f}) \models \varphi \textit{ iff } \exists g \in G \; \mu \underset{\mathrm{val}(g)}{\twoheadrightarrow} 1.$$

Furthermore, mapsize(μ) *depends only on the complexity of φ.*

Proof. Induction on the complexity of φ.

1. φ is atomic.

Case 1. φ does not contain f.

Let

$$\mu = \begin{cases} 1 & \text{if } N_k \models \varphi, \\ 0 & \text{otherwise.} \end{cases}$$

Case 2. φ contains f.

First notice that terms are of the form $f \cdots f(a)$ $a \in M$, since f is the only function symbol in N_k. Now if φ is of the form $R(f^{(k)}(a), f^{(l)}(b), f^{(m)}(c))$ then it is equivalent to

$$f^{(k)}(a) = a_0 \wedge f^{(l)}(b) = b_0 \wedge f^{(m)}(c) = c_0 \wedge R(a_0, b_0, c_0).$$

So it suffices to consider the case $\varphi \equiv f^{(k)}(a) = b$. We can handle this case by induction on the number of f and it can be seen that φ is equivalent to some k-map.

2. Induction step

Let $\mu, \nu \in B(D_0, D_1)$ be what we get by inductive hypothesis for $\varphi, \psi \in \mathcal{L}(f)$. Then for $\neg\varphi$, $\varphi \vee \psi$, $\varphi \wedge \psi$ assign $\neg\mu$, $\mu \vee \nu$, $\neg(\neg\mu \vee \neg\nu)$ respectively.

For the case $\forall x \varphi(x)$ and $\exists x \varphi(x)$. Let $\mu_x \in B(D_0, D_1)$ be what we get by inductive hypothesis for $\varphi(x)$. First remark that in N_k all quantifiers are bounded by n^k. So assign $\neg \bigvee_{x<n^k} \neg\mu_x$, $\bigvee_{x<n^k} \mu_x$ respectively. The sizes of these Boolean formulae are easily seen to be bounded by some polynomial. QED.

Proof of Lemma 2. Let $\varphi(x) \in \mathcal{L}(f)$ and $g \in \mathbb{P}$. For each $1 \leq u \leq k \log n$, let $\mu_u \in B(D_0, D_1)$ satisfy the condition of Proposition 5. Now let $\rho = \mathrm{val}(g)$ be as in Lemma 4. Then there exists $\varepsilon > 0$ and $\rho' \in \Omega^{n,\varepsilon}$ such that ρ' is an extension of $\mathrm{val}(g)$ and $\mu_u \underset{\rho'}{\twoheadrightarrow} 0$ or $\mu_u \underset{\rho'}{\twoheadrightarrow} 1$ for all $1 \leq u \leq k \log n$. Let

$$W(\varepsilon) = \left\{ \rho \in \Omega^{n,\varepsilon} : \begin{array}{c} \rho \text{ is an extension of } \mathrm{val}(g) \text{ and} \\ \forall u \leq k \log n \ \mu_u \underset{\rho}{\twoheadrightarrow} 0 \text{ or } \mu_u \underset{\rho}{\twoheadrightarrow} 1 \end{array} \right\}$$

and $D_g = \{\mathrm{map}(\rho) : \exists \varepsilon > 0 \ \rho \in W(\varepsilon)\}$. It suffices to show that D_g satisfies the requirements for Lemma 2.

(1). D_g is dense below g.

Let $h \in \mathbb{P}$ and $h \leq g$. If $h \notin D_g$ then by Lemma 4 there exists an extension ρ of $\mathrm{val}(h)$ such that $\mathrm{map}(\rho) \in D_g$ and $\mathrm{map}(\rho) \leq h$.

(2). D_g belongs to M.

This is trivial by the fact that the relation $\rho \in W(\varepsilon)$ is definable in M.

(3). $D_g \subseteq E_g$.

Let $h \in D_g$ and $\tilde{f} = \bigcup G$ be a generic such that $h \in G$. Now define d by

$$d(u) = 1 \text{ iff } \mu_u \underset{\mathrm{val}(h)}{\twoheadrightarrow} 1.$$

Then clearly

$$(M_n, \tilde{f}) \models \varphi(u) \text{ iff } d(u) = 1$$

holds. QED.

References

1. M.Ajtai, *The complexity of the Pigeonhole Principle*, 29th Annual Symposium on Foundations of computer science (1988).
2. S.Bellantoni, T.Pitassi, and A.Urquhart, *Approximation and Small-depth Frege Proofs*, SIAM J.Comput. **21** (1992), 1161–1179.
3. K.Kunen, *Set Theory-An introduction to independence proofs*, North-Holland, 1980.
4. R.Parikh, *Existence and feasibility in arithmetic*, J. Symbolic Logic **36** (1971), 494–508.
5. J.B.Paris, A.J.Wilkie and A.R.Woods, *Provability of the Pigeonhole Principle and the existence of infinitely many primes*, J. Symbolic Logic **53** (1988), 1235–1244.
6. J.Paris and A.Wilkie, *Counting Problems in Bounded Arithmetic*, Methods in Mathematical Logic, Lecture Notes in Mathematics **1130** (1985), 317–340.
7. A.J.Wilkie, and J.B.Paris, *On the scheme of induction for bounded arithmetic formulas*, Annals of Pure and Applied Logic **35** (1987), 261–302.