Записки научных
семинаров ПОМИ
Том 304, 2003 г.

S. Boughattas, J-P. Ressayre

NEW MODELS OF BOUNDED INDUCTION AXIOMS

Abstract. We construct models of the integers, to yield: witnessing, independence and separation results for weak systems of bounded induction.

Introduction

Notations

$\mathcal{L}_B$:= language of Arithmetic, including the functions x (= identity), $x+y$, $x-y$, $x.y$, $\lfloor x/2 \rfloor$, $|x|$, $2^{|x|^2}$.

Basic:= the basic axioms of Buss for this language basic term:= term of $\mathcal{L}_B$.

Let τ denote a basic term with the single variable x; for any formula $\varphi = \varphi(x)$ with additional parameters $\bar{u}$ and any set Γ of formulas

$$\varphi\text{-ind}^\tau := \forall x[\varphi(x) \to \varphi(x+1)] \to [\varphi(0) \to \forall x \leq \tau \varphi(x)]$$

$$\Gamma\text{-ind}^\tau := \{\forall \bar{u}(\varphi\text{-ind}^\tau); \varphi \in \Gamma\}.$$

The main cases will be:

- $\tau \geq x$; then Γ-ind$^\tau$ is just Γ-ind.
- $\tau = |x|$; Basic + Σ_n^b-ind$^{|x|}$ is the system denoted S_2^n by Buss.
- $\tau = |x|_p$ where $|x|_0 := x$ and $|x|_{p+1} := ||x|_p|$.

For $n \geq 2$ we call $\Sigma_n^{b'}$ a slight modification of the Σ_n^b formulas: $\Sigma_1^{b'} = \Sigma_1^b$, and a formula is $\Sigma_{n+1}^{b'}$ iff it is obtained by bounded existential quantification from a boolean combination of $\Sigma_n^{b'}$ formulas. For f, $g : \omega \to \omega$ we write $f^\omega < g$ to mean that g (eventually) *dominates* every power of f.

Independence results We show that if $\exp(\tau^\omega) < |x|_2$ (for instance if $\tau = |x|_4$), then Basic + $\Sigma_2^{b'}$-ind$^\tau$ does *not* prove any of the following statements:

1. for all x and $i < |x|$ $\lfloor x/2^i \rfloor$ exists;

2. every divisor of a power of 2 is itself a power of 2;
3. S^1_2;
4. the set of primes is NP;
5. NP=co-NP (more precisely $\Sigma^b_2 = \Sigma^b_3$, the collapse of the polynomial hierarchy on its third level) and generally for any $p < \omega$:
6. $\Sigma^b_p = \Sigma^b_{p+1}$.

We have a similar result for each $n \geq 1$: in the conclusion $\Sigma^{b'}_2$-ind$^\tau$ is replaced by $\Sigma^{b'}_n$-ind$^\tau$, but in the hypothesis $\exp(\tau^\omega)$ is replaced by $\exp_{n-1}(\tau^\omega)$ where $\exp_0(x) := x$, $\exp_{i+1}(x) := \exp(\exp_i(x))$.

For the unprovability of the statement (6) about collapse, we were inspired by the work of Pollett [2]. He proves a similar result for the theories EBASIC +strictΣ^b_n-ind$^{|x|_{n+3}}$. Our result is different above all because it makes an almost doubly exponential win on the length of induction that we allow. In fact for any n, any further progress on the length of $\Sigma^{b'}_n$ induction would yield the above independence results w.r.to the theory Basic + Σ^b_1-ind$^{|x|_2}$. Now the latter theory "captures" in some sense parallel computability in polylog time. So that the result would be significant for Algorithmic Complexity. We hope that the situation where one stops short of this improvement is provisional. But here, another series of our results comes into the picture to explain why the desired improvement is difficult to obtain.

Witnessing results of $\forall\Sigma^b_1$ formulas by basic terms of low depth. We set

$$D_0(x,c) := \{y : y < |x| \ \text{ or } \ y = x\}; D_{i+1}(x,c) := \mathcal{L}_B D_i(x,c) \restriction c,$$

where

$$\mathcal{L}_B X := \{f(x,y); x, y \in X \quad \text{and} \quad f \in \mathcal{L}_B\}.$$

Thus $y \in D_i(x,c)$ implies that y is the value on x of some basic term with parameters in $D_0(x,c)$, of *depth* $\leq i$ and hereditarily bounded by c. Given any Σ^b_1 formula φ we show for instance

1. if $\forall x \exists y \varphi$ is provable in Basic + Σ^b_1-ind$^{|x|_3}$, then for some $K < \omega$:

$$\forall x \exists y [\varphi \ \text{ and } \ y \in D_{|x|_3^K}(x, x^{|x|^K})]$$

is true (in the standard model ω)

2. if $\forall x \exists y \varphi$ is provable in Basic $+ \Sigma_2^{b'}$-ind$^{|x|_4}$ then for some $K < \omega$

$$\forall x \exists y [\varphi \ \text{ and } \ y \in D_{\exp(|x|_4^K)}(x, x^{|x|^K})]$$

is true.

Remarks.

1. If $|x|_2$ dominates τ^ω then $D_{\tau^K}(x, x^{|x|^K})$ is of cardinal $< x$ for every $K < \omega$. This prevents the above results to follow from Parikh's well known result implying $\forall x \exists y [\varphi \ \text{ and } \ y < x^{|x|^K}]$.
2. If $\exp_{n-1}(\tau^\omega) < |x|_2$ we can prove a similar result for Basic $+ \Sigma_n^{b'}$-ind$^\tau$.
3. This witnessing phenomenon is not particularly surprising, in view of the weakness of the theories involved. But *any* improvement on the length of $\Sigma_n^{b'}$ induction that is allowed, would actually yield the same result for Σ_1^b-ind$^{|x|_2}$. And that would be very surprising: for *every* parallel computation in uniform polylog time and for each argument x, (the code of) the computation applied to x would then be obtainable as the value of some basic term of SUBlogarithmic depth applied to x!

This gives an instructive partial explanation of why it is so difficult to prove our independence results for stronger and hence more significant theories: the ultimate and decisive progress would not only prove an independence that everybody expects to hold. Unless a substantial refinment of our method is invented, the progress would at the same time prove a mysterious and strong witnessing result ... which may be false. The other difficulty we have to overcome (for the results to become *practically* meaningful) is that one is more interested in *satisfying* (1) than in falsifying it as we did; but the former is harder to obtain.

So much for the results; as to the methods, we hope that the new ones we introduce will be a lasting source of interest for the present work.

1. (See Theorems 2 and 4 below) These methods involve the use of non standard *reals* to construct models of the integers. And they introduce a notion of *resource in depth* which we think is resourceful.

2. (See Theorems 1 and 3) They use indiscernibles to let a structure *control* in some ways what is satisfied in an *undefinable* part of that structure. This is inspired by Jeff Paris' proof of the Harrington–Paris theorem; but many complements are needed to make the idea work in the present context of weak arithmetic.

The main steps.

To give an idea of our constructions, below we state five theorems.

Let N denote a countable model of Peano's Arithmetic and let $\omega \subset N$ denote the standard integers. If x denotes any integer of N, we often also use x to denote the set of its predecessors – letting the context indicate which one of the two senses is being used.

Theorem 1. *Assume that in N we have: $n < \omega < \ell$ and $exp_{n-1}(\ell^k) < d$ for each $k < \omega$. Below d there is an ω-sequence (ν_m) and for each relation ϕ on $|\ell| \times d^n$ which is coded in N there is an integer $p = p(\phi) < \omega$ such that $\{\nu_m;\ m > p\}$ is* `indiscernible w.r.t. to` ϕ `over` *$i < |\ell|$ (in the sense: for each fixed $i < |\ell|$ and if $v_1 < \ldots < v_n$, the value of $\phi(i, v_1, \ldots, v_n)$ is* `constant` *over $\{\nu_m;\ m > p\}$).*

Theorem 1 rests on a refinment of the Erdos–Rado partition theorem. We apply this refinment only in the finitary case: then "Erdos–Rado" reduces to "finite Ramsey", but gives another proof to elaborate on. Moreover we apply this inside N; and using the recursive saturation of the initial segments of N is necessary in order to boost the purely combinatorial result to the above form.

Theorem 2. *Given $a > \omega$ apply Theorem 1 when $n = 2$, $\ell = \tau(a)$ where $\exp(\tau^\omega) < |x|_2$ (hence there is d such that $\exp(\ell^\omega) < d$ and $d^\omega < |a|_2$). Set*

$$I := \{x;\ \exists m\ x < \nu_m\},$$
$$D_I(a, c) := \bigcup_{i \in I} D_i(a, c) \restriction a^{|a|^\omega}.$$

where $c > a^{|a|^\omega}$. Then $D_I(a, c)$ is a model of Basic $+\ \Sigma_2^{b'}$-ind$^\tau$.

Note that this model takes place in $D_d(a, c)$: as only *"resource"*, it uses basic terms of *depth* $< d$. Part (2) of the witnessing results announced in the introduction is a corollary to Theorem 2. Part (1) uses an analog of Theorem 2 where the indiscernibility of (ν_m) holds with $n = 1$. The proof of Th. 2 combines a dichotomic construction (to win one exponential on the length of induction), with *"quantifier control"* induced by indiscernibility – as introduced below.

Theorem 3. *Let I be the cut of Theorem 2*

(a) *for every formula ψ interpreted in $D_I(a, c)$ and of the form $\exists x \varphi(x)$ where $\varphi(x)$ is Σ_1^b, there is a formula θ – interpreted in N – such that ψ iff $\exists v \in I\ \exists x\ \forall w \in I\ \theta$*

(b) *moreover* $\exists v \in I\ \exists x\ \forall w \in I\ \theta$ *holds inside* (N, I) *iff* $\exists v < \nu_p\ \exists x\ \forall w < \nu_{p+1}\ \theta$, *where* p *only depends on the parameters of* ψ *that are* $> |\ell|$.

The (a) *is natural and easy to prove when* $\varphi(x)$ *is strict* Σ_1^b; *its general case as well as (b) are proved by overspill arguments in* N.

We let Q denote the field of fractions of N; we can *"counterfeight"* the construction of the resource $D_d(a, c)$ used to define $D_I(a, c)$ in Theorem 1. That is we can do an analogous construction of D_i, $i < d$ and D_I where a non integer element $r \in Q$ is put in D_0; so as to provide a divisor of a that does not exist in N yet behaves in D_I as a *"forgery"* of an *integer*:

Theorem 4.

1. *Given* a, $d > \omega$ *in* N *such that* $d^k < |a|_2$ *for each* $k < \omega$, *there exist* r, r' *in* Q *satisfying:*
   - $r \notin N$
   - $rr' = a$ *(resp:* $(2r+1)r' = 2^{|a|}$*)*
   - *there exists a "resource of depth* d*"* $(D_i)_{i \leq d}$ *as above but with* $D_d \subset Q$ *and starting from* $D_0 := |a| \cup \{a, r, r'\}$, *such that*

     i) D_d *is disjoint from* $]0, 1[$

     ii) *for* $x \in D_i$ *there is a unique couple* $y, z \in D_{i+1}$ *for which* $2y \leq x < 2(y+1)$ *and* $2^{z-1} \leq x < 2^z$ *(in this way* $\lfloor x/2 \rfloor = y$ *and* $|x| = z$ *are defined)*
2. *Let* D_I *be defined as* $D_I(a, c)$ *in Theorem 2 but from the new resource* $(D_i)_{i<d}$: $D_I := \cup_{i<I} D_i \restriction a^{|a|^\omega}$. *It is again a model of* Basic $+\ \Sigma_2^{b'}$-ind$^\tau$, *but also of:*
   - *"a is divisible" – even if a is prime according to* N
   - *resp: "*$2^{|a|}$ *has an odd divisor" – even though* $2^{|a|}$ *is power of 2 inside* D_I.
3. *For any* $x \in D_I$ *that is not in* N *– in particular* $x = r$, *"*$\forall i < |x| \lfloor x/2^i \rfloor$ *exists" is false.*

Part (1 to 5) of the independence results w.r.to Basic $+\ \Sigma_2^{b'}$-ind$^\tau$ announced in the introduction is a corollary to Theorem 4. And the remaining part (6) follows from Theorem 5 below, which is obtained by *iterating* the above use of a "resource in depth": we construct *inside* D_I another resource $D'_{d'}$ where D'_0 still contains the "forgery" r, r', and d' is notably smaller than d but where in compensation each set D'_{i+1} has witnesses for all Σ_1^b sentences with parameters from D'_i and interpreted in D_I. When we apply the construction made in Theorem 2 to this new resource $D'_{d'}$ in place of D_d, we obtain a model $D'_{I'}$ which satisfies in addition to the conclusion of 4.b some amount of Σ_3^b-induction. The amount is modest but in compensation it concerns the full class Σ_3^b, not only the strict or $\Sigma_3^{b'}$ ones. And by repeating n times such iterations we obtain:

Theorem 5. *The model D_I of Theorem 4 contains a Σ_0^b elementary submodel which in addition to the conclusion of Theorem 4 satisfies $S_2 + \ldots + S_n$, where*

- $S_2 := \Sigma_3^b - ind^{|x|_6}$,

more generally for $i \geq 2$

- $S_i := \Sigma_{i+1}^b - ind^{|x|_{3i}}$.

References

1. S. R. Buss, *Bounded Arithmetic*. Bibliopolis, Naples (1986).
2. C. Pollett, *Multifunction Algebras and the Provability of $PH\downarrow$*. in: *Annals of Pure and Applied Logic* Vol. 104, July 2000, pp. 279–303.

CNRS and Paris 7 University
ressayre@logique.jussieu.fr

Поступило 20 декабря 2002 г.