A combinatorial method of tackling the problem of hierarchy collapse, and a theorem of Ajtai

A. J. Wilkie

June 16, 2010

0. The language L^r consists of the binary relation $<$, binary functions $+$ and $\cdot$, unary function $'$ (successor) and the constant 0. The set of genuinely finite natural numbers is denoted by ω.

1. Since we have no idea how to solve the problem of hierarchy collapse (without an oracle) described in the previous sections, we will mention a theorem concerning the same problem for hierarchies with an oracle. For $n \in \omega$ and a unary relation symbol R, let us denote by E_n^R the set of formulas of the form

$$\exists \vec{x}_1 < x \, \forall \vec{x}_2 < x \; \ldots \; Q\vec{x}_n < x \, \Delta(\vec{x}_1, \ldots, \vec{x}_n, x),$$

where Δ is an open formula of the language $L^r \cup \{R\}$. Also, for $B \subseteq \omega$ let

$$E_n^B = \{\varphi(x)^{(\mathbb{N},B)} : \varphi(x) \in E_n^R\}.$$

Here $\varphi(x)^{(\mathbb{N},B)}$ is the set of x for which φ is true when L^R is interpreted by $\mathbb{N}$, and R by B. The sets A_n^R and A_n^B are defined analogously by letting the first quantifier be $\forall$. Their corresponding intersections are denoted Δ_0^R and Δ_0^B.

2. *Proposition.*

For all $n \in \omega$ there exists a subset B of ω such that $E_n^B \neq E_{n+1}^B$.

This proposition follows from a theorem of M. Sipser about Boolean circuits (see "Borel Sets and Circuit Complexity", JACM 1983, pp. 61–69), whose presentation we closely follow. On the way, we study a theorem of Ajtai about the structure of classes of sets of the form E_n^B that uses an analogue of the Borel hierarchy.

3. Let $M \supsetneq \mathbb{N}$. We work "inside M", and it will be clear when we consider elements of M as elements, and when as M-bounded sets or M-bounded functions. Moreover, whenever we use expressions like $s \subseteq M$ and $f\colon s \longrightarrow M$, it should be understood that s and f are coded inside M (and so M-bounded).

Let $s \subseteq M$. We denote by $|s|$ the size of s, by 2^s the set of Boolean functions on s, and by $2^{\subseteq s}$ the set of partial Boolean functions on s. The domain of a function f is denoted by $\mathrm{dom}(f)$. We denote by B_f^s the set of partial functions extending f. A set of functions $\alpha \subseteq 2^s$ is called a *basic subset* of 2^s if $\alpha = \varnothing$ or $\alpha = \bigcup_{i=0}^{n} B^s_{f_i}$ for some $n \in \omega$, where all functions f_i have genuinely finite domain (i.e. $|\operatorname{dom}(f_i)| \in \omega$). In other words, a basic subset is defined by a DNF.

The classes $\tilde{E}^s_n$ and $\tilde{A}^s_n$, for $n \in \omega$, are defined by recursion on n as follows:

(i) $\tilde{E}^s_0$ and $\tilde{A}^s_0$ consist of all basic subsets of 2^s.

(ii) $\tilde{E}^s_{n+1}$ contains all sets of the form $\bigcup_{i<A} \alpha_i$, where the sequence α_i is coded inside M, all α_i belong to $\tilde{A}^s_n$, and $A < |s|^m$ for some $m \in \omega$.

(iii) $\tilde{A}^s_{n+1} = \{2^s \setminus \alpha : \alpha \in \tilde{E}^s_{n+1}\}$.

(iv) $A^s = \bigcup_{n\in\omega} \tilde{E}^s_n$.

We mention the connection (not used in what follows) between A^s and the theory of finite models, as described in 4 and 5:

4. If $\mathcal{L}$ is a finite relational language (that is, $\mathcal{L}$ contains only a (truly) finite number of relation symbols), one denotes by $\mathcal{L}(R)$ the language obtained by adding to $\mathcal{L}$ a new unary relation symbol R. If $\tilde{s} \in M$ is an $\mathcal{L}$-structure with domain $s \subseteq M$, and $f \in 2^s$, then we denote by $(\tilde{s}, f)$ the resulting structure when R is interpreted by the zero-set of f, i.e. $\{a \in s : f(a) = 0\}$. I leave the proof of the following proposition, which isn't difficult, as an exercise.

5. *Proposition.*

Suppose that $s \subseteq M$, $\alpha \subseteq 2^s$ and $n \in \omega$. Then α belongs to $\tilde{E}^s_n$ (respectively, $\tilde{A}^s_n$) if and only if there exists a finite relational language $\mathcal{L}$, an $\mathcal{L}$-structure $\tilde{s} \in M$ with domain s, an $\exists_n$ (respectively $\forall_n$) formula $\varphi(x_1, \ldots, x_k)$ of $\mathcal{L}(R)$, and $a_1, \ldots, a_k \in \tilde{s}$ such that

$$\alpha = \{f \in 2^s : (\tilde{s}, f) \models \varphi(a_1, \ldots, a_k)\}.$$

Moreover, if $n \geq 1$ then the formula φ can be chosen without free variables.

In order to explain Ajtai's theorem we need the following definition:

6. *Definition.*

Let $s \subseteq M$. A set $S \subseteq 2^{\subseteq s}$ is called s-complete if

(i) For all $f, g \in S$, $|\operatorname{dom}(f)| = |\operatorname{dom}(g)|$. We denote the common value by $\|S\|$.

(ii) For all $f, g \in S$, if $f \neq g$ then $B^s_f \cap B^s_g = \varnothing$.

(iii) $\bigcup_{f\in S} B^s_f = 2^s$. In other words, S is a collection of partial functions, all having the same domain size, such that $\{B^s_f : f \in S\}$ is a partition of 2^s. Alternatively, S is a $\|S\|$-DNF tautology, all of whose clauses are mutually exclusive.

7. *Theorem.* (Ajtai)

Let $s \subseteq M$ such that $|s|$ is non-standard, and let $\alpha \in A^s$. Then there exists a $k \in \omega$, an s-complete set S with $\|S\| \leq |s| - |s|^{1/k}$, and a subset $\mathcal{S}$ of S such that

$$\left| \alpha \triangle \bigcup_{f\in\mathcal{S}} B^s_f \right| \leq 2^{|s|-|s|^{1/k}}.$$

Before proving 7, we deduce an important corollary.

8. *Corollary.*

Let $s \subseteq M$ such that $|s|$ is non-standard. Suppose that $\alpha \in A^s$ and $|\alpha| \geq 2^{|s|-|s|^{1/\ell}}$ for all $\ell \in \omega$. Then there exist $f \in 2^{\subseteq s}$ and $m \in \omega$ such that $|\operatorname{dom}(f)| \leq |s| - |s|^{1/m}$ and $B^s_f \subseteq \alpha$.

Proof. We first comment that if S is s-complete, $t \in M$ and for all $f \in S$, $a_f \subseteq s$ is such that $\operatorname{dom}(f) \cap a_f = \varnothing$ and $|a_f| = t$, then $S' = \{f \cup g : f \in S,\, g \in 2^{a_f}\}$ is clearly s-complete with $\|S'\| = \|S\| + t$. Thus one can assume that the S given by 7 satisfies

$$|s| - |s|^{1/k} - 1 \leq \|S\| \leq |s| - |s|^{1/k}.$$

Let $u = \min\{|B^s_f \setminus \alpha| : f \in \mathcal{S}\}$. Using 7 and 6(ii), we have

$$2^{|s|-|s|^{1/k}} \geq \left|\alpha \triangle \bigcup_{f \in \mathcal{S}} B^s_f\right| \geq \left|\bigcup_{f \in \mathcal{S}} (B^s_f \setminus \alpha)\right| \geq u \cdot |\mathcal{S}|.$$

Also, for all $\ell \in \omega$ we have

$$\begin{aligned} 2^{|s|-|s|^{1/\ell}} \leq |\alpha| &\leq \left|\bigcup_{f \in \mathcal{S}} B^s_f\right| + 2^{|s|-|s|^{1/k}} \\ &= |\mathcal{S}| \cdot 2^{|s|-\|S\|} + 2^{|s|-|s|^{1/k}} \\ &\leq |\mathcal{S}| \cdot 2^{|s|^{1/k}+1} + 2^{|s|-|s|^{1/k}}. \end{aligned}$$

Since $|s|$ is non-standard, it follows that $u \leq 2^{|s|^{1/\ell}}$ for all $\ell \in \omega$. In particular, there exists an $h \in 2^{\subseteq s}$ with $|s| - |s|^{1/k} - 1 \leq |\operatorname{dom}(h)| \leq |s| - |s|^{1/k}$ such that $|B^s_h \setminus \alpha| \leq 2^{|s|^{1/3k}}$. Let $\beta \subseteq s$ satisfy $\beta \cap \operatorname{dom}(h) = \varnothing$ and $|s|^{1/2k} \leq |\beta| \leq |s|^{1/2k} + 1$. Then

$$2^{|s|^{1/3k}} \geq |B^s_h \setminus \alpha| = \left|\left(\bigcup_{g \in 2^\beta} B^s_{h \cup g}\right) \setminus \alpha\right| = \sum_{g \in 2^\beta} |B^s_{h \cup g} \setminus \alpha|.$$

Therefore, if $|B^s_{h\cup g} \setminus \alpha| \geq 1$ for all $g \in 2^\beta$, then $2^{|s|^{1/3k}} \geq |2^\beta| \geq 2^{|s|^{1/2k}}$, a contradiction. Thus there exists a $g \in 2^\beta$ such that $B^s_{h\cup g} \subseteq \alpha$. Moreover,

$$|\operatorname{dom}(h \cup g)| \leq |s| - |s|^{1/k} + |s|^{1/2k} + 1 \leq |s| - |s|^{1/2k}.$$

□

One can use 8 to prove that certain natural sets of functions do not belong to A^s, and therefore are not first-order definable in the sense of 4 and 5. For example, it follows immediately from 8 that the set

$$\{f \in 2^s : |\{a \in s : f(a) = 0\}| \text{ is even}\}$$

doesn't belong to A^s (for non-standard s).

9. *Remark.*

Ajtai proved a theorem stronger than 7, where "there exists a $k \in \omega$" is replaced by "for each standard rational number η such that $0 < \eta < 1$". However, the proof that I give of 7 is much simpler than Ajtai's, and 7 is sufficient for most applications.

10. In order to prove 7, we shall need the following definitions and lemmas. We fix $s \subseteq M$ such that $|s|$ is non-standard.

If σ is a non-trivial basic subset of 2^s (i.e. not $\varnothing$ or 2^s), then clearly there exists a unique minimal subset $X \subseteq s$ which is genuinely finite such that $\sigma = \bigcup_{i<n} B^s_{f_i}$, where $n \in \omega \setminus \{0\}$ and $f_i \in 2^X$ for all $i < n$. We denote this X by $\mathrm{supp}(\sigma)$, and we write $\|\sigma\|$ for $|X|$. If σ is trivial then we use the convention $\mathrm{supp}(\sigma) = \varnothing$ and $\|\sigma\| = 0$. Thus we have

11.
$$|\sigma| \leq \left(1 - \frac{1}{2^{\|\sigma\|}}\right) 2^{|s|} \text{ if } \sigma \neq 2^s.$$

If $\alpha \in \tilde{A}^s_1$, we can write $\alpha = \bigcap_{i<C} \sigma_i$, where for certain $n, m \in \omega$ we have that $|C| < |s|^m$, that for all $i < C$, σ_i is a basic subset of 2^s with $0 < \|\sigma_i\| \leq n$, and that for all different $i, j < C$ we have $\mathrm{supp}(\sigma_i) \neq \mathrm{supp}(\sigma_j)$. Note that $n \in \omega$ since $\|\sigma_i\| \in \omega$ for all $i < C$ and the sequence $\langle \sigma_i : i < C \rangle$ is M-coded. We denote by $\|\alpha\|$ the smallest value of n. If α is trivial, we put $\|\alpha\| = 0$. Let us choose now a subset D_α of $\{0, 1, \ldots, C-1\}$ which is maximal under the property that for all different $i, j \in D_\alpha$, $\mathrm{supp}(\sigma_i) \cap \mathrm{supp}(\sigma_j) = \varnothing$. Using 11, we get that

12.
$$|\alpha| \leq \left(1 - \frac{1}{2^{\|\alpha\|}}\right)^{|D_\alpha|} 2^{|s|}.$$

Moreover, since D_α is maximal we have:

13. For all $f \in 2^{\subseteq s}$ such that $\bigcup_{i \in D_\alpha} \mathrm{supp}(\sigma_i) \subseteq \mathrm{dom}(f)$, we have that $B^s_f \cap \alpha = B^s_f \cap \alpha_f$ for some $\alpha_f \in \tilde{A}^s_1$ with $\|\alpha_f\| \leq \|\alpha\| - 1$.

We define $\mathrm{supp}(\alpha) = \bigcup_{i \in D_\alpha} \mathrm{supp}(\sigma_i)$, so that

14. $|\mathrm{supp}(\alpha)| \leq \|\alpha\| \cdot |D_\alpha|$.

We need the following combinatorial lemma:

15. *Lemma.*

Let $\beta_1, \beta_2, \ldots, \beta_t \subseteq s$, $m \in \omega$ and p, q be standard natural numbers such that $p, q > 0$ and $p + q < 1$. Suppose that $t \leq |s|^m$ and that $|\beta_i| \leq |s|^p$ for $i = 1, \ldots, t$. Then there exist $H \subseteq s$ and $\ell \in \omega$ such that $|H| \geq |s|^q$ and $|H \cap \beta_i| < \ell$ for $i = 1, \ldots, t$.

Proof. Suppose, for the sake of contradiction, that for all $\ell \in \omega$ and $H \subseteq s$ with $|H| = \lfloor |s|^q \rfloor + 1 \triangleq u$ there exists an i, where $1 \leq i \leq t$, such that $|H \cap \beta_i| \geq \ell$. Then for all $\ell \in \omega$,

$$\binom{|s|}{u} \leq \sum_{i=1}^{t} \binom{|\beta_i|}{\ell} \binom{|s| - \ell}{u - \ell}.$$

(We suppose, of course, that the function $i \mapsto \beta_i$ is coded inside M.)

Thus for all $\ell \in \omega$,

$$\binom{|s|}{u} \leq |s|^m \binom{|s|^p}{\ell} \binom{|s|}{u - \ell}.$$

It follows that $|s|^\ell \leq |s|^m |s|^{p\ell} u^\ell$ for all $\ell \in \omega$. Taking ℓ big enough, this contradicts the facts that $u = \lfloor |s|^q \rfloor + 1$, $p + q < 1$, $p + q$ is standard and s is non-standard. $\square$

We will now prove the following theorem, from which 7 clearly follows.

16. *Theorem.*

Let $N, m \in \omega$ and $\langle \alpha_i : i < A \rangle$ be an M-coded sequence such that $A < |S|^m$ and either all α_i belong to $\tilde{A}^s_N$, or all α_i belong to $\tilde{E}^s_N$. Then there exist $k \in \omega$ and an s-complete set $\mathcal{S}$ with $\|\mathcal{S}\| \leq |s| - |s|^{1/k}$ such that for all $i \in A$ the following property holds:

$$\left| \alpha_i \triangle \bigcup_{f \in \mathcal{S}} (B^s_f \cap \sigma_{f,i}) \right| \leq 2^{|s| - |s|^{1/k}}, \qquad (*)$$

where for all $i < A$ and for all $f \in \mathcal{S}$, $\sigma_{f,i}$ is a basic subset of 2^s (and the function $(f, i) \mapsto \sigma_{f,i}$ is coded inside M).

Proof. First of all, let us consider the case that $\alpha_i \in \tilde{A}^s_1$ for all $i < A$. We comment that $\max_{i<A} \|\alpha_i\| \in \omega$ since $\|\alpha_i\| \in \omega$ for all $i \in A$ and the sequence $\langle \alpha_i : i < A \rangle$ is M-coded. We proceed by induction on $\max_{i<A} \|\alpha_i\|$.

If $\max_{i<A} \|\alpha_i\| = 0$, then $\alpha_i \in \{\varnothing, 2^s\}$ for all $i < A$. Thus, we can define $\mathcal{S} = \{\varnothing\}$, $k = 1$ and $\sigma_{\varnothing,i} = \alpha_i$, which satisfies $(*)$.

Suppose now that $\max_{i<A} \|\alpha_i\| = n + 1$, where $n \in \omega$. Define

$$E = \{i < A : |D_{\alpha_i}| \leq \sqrt{|s|}\}$$

and $t_i = \mathrm{supp}(\alpha_i)$ for $i \in E$. Using 15, we get $H \subseteq s$ and $\ell \in \omega$ so that

17. $|H| \geq \sqrt[4]{s}$ and

18. For all $i \in E$, $|H \cap t_i| \leq \ell$.

Let $u_i = H \cap t_i$ for all $i \in E$. For every $h \in 2^{s \setminus H}$, $i \in E$ and $h^{(i)} \in 2^{u_i}$ we clearly have:

19. $\mathrm{dom}(h) \cap \mathrm{dom}(h^{(i)}) = \varnothing$ and $t_i \subseteq \mathrm{dom}(h) \cup \mathrm{dom}(h^{(i)})$, and so, using 13:

20. $B^s_{h\cup h^{(i)}} \cap \alpha_i = B^s_{h\cup h^{(i)}} \cap \alpha_{h\cup h^{(i)}}$ for some $\alpha_{h\cup h^{(i)}} \in \tilde{A}^s_1$ with $\|\alpha_{h\cup h^{(i)}}\| \leq n$.

We can suppose that the projections of $\alpha_{h\cup h^{(i)}}$ to 2^H, which we denote $\alpha^*_{h\cup h^{(i)}} \in \tilde{A}^H_1$, exist. They also satisfy $\|\alpha^*_{h\cup h^{(i)}}\| \leq n$.

Thus, for fixed $h \in 2^{s\setminus H}$, we can apply the induction hypothesis for the sequence $\langle \alpha^*_{h\cup h^{(i)}} : i \in E,\, h^{(i)} \in 2^{u_i}\rangle$ (since $\alpha^*_{h\cup h^{(i)}} \in \tilde{A}^H_1$ and its size is at most $2^\ell|E| \leq 2^\ell A < |s|^{m+1} \leq |H|^{4(m+1)}$, using 17) to obtain $k_h \in \omega$ and an H-complete set $\mathcal{S}_h$ satisfying $\|\mathcal{S}_h\| \leq |H| - |H|^{1/k_h}$ such that for all $i \in E$ and $h^{(i)} \in 2^{u_i}$:

21.
$$\left|\alpha^*_{h\cup h^{(i)}} \triangle \bigcup_{f\in\mathcal{S}_h} \left(B^H_f \cap \tau_{f,i,h^{(i)}}\right)\right| \leq 2^{|H|-|H|^{1/k_h}},$$

where the $\tau_{f,i,h^{(i)}}$ are basic subsets of 2^H.

We can suppose that the function $h \mapsto k_h$ is coded within M, so that $k^* \triangleq \max\{k_h : h \in 2^{s\setminus H}\}$ belongs to ω. Moreover, we can clearly suppose that for all $h \in 2^{s\setminus H}$, $k_h = k^*$ and $\|\mathcal{S}_h\| = \lfloor |H| - |H|^{1/k^*}\rfloor$ (see the proof of 8) while 21 remains true.

Let $\mathcal{S} = \{h \cup f : h \in 2^{s\setminus H},\, f \in \mathcal{S}_h\}$. Thus $\mathcal{S}$ is s-complete, and by 17:

22. $\|\mathcal{S}\| \leq |s| - |H| + (|H| - |H|^{1/k^*}) = |s| - |H|^{1/k^*} \leq |s| - |s|^{1/5k^*}$.

We remark that if $g \in \mathcal{S}$ then $g = h \cup f$, where $h \in 2^{s\setminus H}$ and $f \in \mathcal{S}_h$, and this representation is unique (since $\mathcal{S}_h$ is H-complete), and so we can define, for $i \in E$ and $g \in \mathcal{S}$,

$$\sigma_{g,i} = \bigcup_{h^{(i)}\in 2^{u_i}} \left(B^s_{h^{(i)}} \cap \tau^\dagger_{f,i,h^{(i)}}\right),$$

where $\tau^\dagger_{f,i,h^{(i)}}$ is the lifting of $\tau_{f,i,h^{(i)}}$ (given by 21) to 2^s. Thus $\sigma_{g,i}$ is a basic subset of 2^s, since u_i is genuinely finite.

For all $i \in E$ we clearly get, using 20:

23.
$$\alpha_i = \bigcup_{h\in 2^{s\setminus H}} \bigcup_{h^{(i)}\in 2^{u_i}} \left(B^s_{h\cup h^{(i)}} \cap \alpha_{h\cup h^{(i)}}\right)$$

and

24.
$$\bigcup_{g\in\mathcal{S}} (B^s_g \cap \sigma_{g,i}) = \bigcup_{h\in 2^{s\setminus H}} \bigcup_{h^{(i)}\in 2^{u_i}} \left(B^s_{h\cup h^{(i)}} \cap \left(\bigcup_{f\in\mathcal{S}_h} (B^s_f \cap \tau^\dagger_{f,i,h^{(i)}})\right)\right).$$

Thus

25.

$$\left|\alpha_i \triangle \bigcup_{g\in\mathcal{S}} (B^s_g \cap \sigma_{g,i})\right|$$

$$= \left|\bigcup_{h\in 2^{s\setminus H}} \bigcup_{h^{(i)}\in 2^{u_i}} \left(B^s_{h\cup h^{(i)}} \cap \left(\alpha_{h\cup h^{(i)}} \triangle \bigcup_{f\in\mathcal{S}_h} (B^s_f \cap \tau^\dagger_{f,i,h^{(i)}})\right)\right)\right|.$$

Now, for all $h \in 2^{s\setminus H}$ and $h^{(i)} \in 2^{u_i}$,

$$\left|B^s_{h\cup h^{(i)}} \cap \left(\alpha_{h\cup h^{(i)}} \triangle \bigcup_{f\in\mathcal{S}_h} (B^s_f \cap \tau^\dagger_{f,i,h^{(i)}})\right)\right|$$

$$= \left|\alpha^*_{h\cup h^{(i)}} \triangle \bigcup_{f\in\mathcal{S}_h} (B^H_f \cap \tau_{f,i,h^{(i)}})\right| \le 2^{|H|-|H|^{1/k^*}}$$

(by 21), and so

26. For all $i \in E$,

$$\left|\alpha_i \triangle \bigcup_{g\in\mathcal{S}} (B^s_g \cap \sigma_{g,i})\right| \le 2^{|s|-|H|} \cdot 2^\ell \cdot 2^{|H|-|H|^{1/k^*}} \le 2^{|s|-|s|^{1/5k^*}},$$

where the first inequality follows from 25 and 18, and the second one from 17.

Now, let us put $\sigma_{g,i} = \varnothing$ for all $g \in \mathcal{S}$ if $i \notin E$. Thus for all $i \notin E$,

$$\left|\alpha_i \triangle \bigcup_{g\in\mathcal{S}} (B^s_g \cap \sigma_{g,i})\right| = |\alpha_i| \le \left(1 - \frac{1}{2^{n+1}}\right)^{\sqrt{|s|}} \cdot 2^{|s|}$$

(using 12 and the definition of E), and so

27. For all $i \notin E$,

$$\left|\alpha_i \triangle \bigcup_{g\in\mathcal{S}} (B^s_g \cap \sigma_{g,i})\right| \le 2^{|s|-|s|^{1/5k^*}}.$$

The induction is now complete (see 22, 26 and 27), so that we have proved the case $\alpha_i \in \tilde{A}^s_1$ of the theorem.

In order to prove the theorem in general, we remark that if it holds for a sequence $\langle \alpha_i : i < A\rangle$, then it also holds for its complement $\langle 2^s \setminus \alpha_i : i < A\rangle$, since the class of basic subsets is closed under complementation. Thus it suffices to prove that if the theorem holds for the sequence $\langle \alpha_{i,j} : i, j < A\rangle$ then it also holds for the sequence $\langle \bigcup_{j<A} \alpha_{i,j} : i < A\rangle$.

Let us therefore choose $k \in \omega$ and an s-complete set $\mathcal{S}$ with $\|\mathcal{S}\| \le |s| - |s|^{1/k}$ such that for all $i, j < A$,

$$\left|\alpha_{i,j} \triangle \bigcup_{f\in\mathcal{S}} (B^s_f \cap \sigma_{f,i,j})\right| \le 2^{|s|-|s|^{1/k}},$$

where the $\sigma_{f,i,j}$ are basic subsets of 2^s. (We comment that the sequence $\langle \alpha_{i,j} : i,j < A\rangle$ has length at most $A^2 \le |s|^{2m}$.) Let $\beta_{f,i} = \bigcap_{j<A} \sigma_{f,i,j}$ for $f \in \mathcal{S}$ and $i < A$, so that $\beta_{f,i} \in \tilde{A}^s_1$. Thus for all $i < A$,

$$\left(\bigcap_{j<A} \alpha_{i,j}\right) \triangle \bigcup_{f\in\mathcal{S}} (B^s_f \cap \beta_{f,i}) \subseteq \bigcup_{j<A} \left(\alpha_{i,j} \triangle \bigcup_{f\in\mathcal{S}} (B^s_f \cap \sigma_{f,i,j})\right),$$

and so

28. For all $i < A$,

$$\left|\left(\bigcap_{j<A} \alpha_{i,j}\right) \triangle \bigcup_{f\in\mathcal{S}} (B^s_f \cap \beta_{f,i})\right| \le A \cdot 2^{|s|-|s|^{1/k}}.$$

Clearly, for all $i < A$ and $f \in \mathcal{S}$ the projection $\beta^*_{f,i}$ of $\beta_{f,i}$ into $s \setminus \mathrm{dom}(f)$ belongs to $\tilde{A}_1^{s\setminus \mathrm{dom}(f)}$. The already proven case of the theorem implies that for all $f \in \mathcal{S}$ there exist $k' \in \omega$ and an $(s \setminus \mathrm{dom}(f))$-complete set $\mathcal{S}_f$, with $\|\mathcal{S}_f\| \le |s \setminus \mathrm{dom}(f)| - |s \setminus \mathrm{dom}(f)|^{1/k'} \le |s| - \|\mathcal{S}\| - (|s| - \|\mathcal{S}\|)^{1/k'}$, such that

29. For all $i < A$ and $f \in \mathcal{S}$,

$$\begin{aligned}\left|\beta^*_{f,i} \triangle \bigcup_{g\in\mathcal{S}_f} (B_g^{s\setminus\mathrm{dom}(f)} \cap \tau_{g,i})\right| &\le 2^{|s\setminus\mathrm{dom}(f)|-|s\setminus\mathrm{dom}(f)|^{1/k'}} \\ &\le 2^{|s|-\|\mathcal{S}\|-(|s|-\|\mathcal{S}\|)^{1/k'}},\end{aligned}$$

where the $\tau_{g,i}$ are basic subsets of $2^{s\setminus\mathrm{dom}(f)}$. Like above, we can suppose that k' does not depend on f, and that for all $f, g \in \mathcal{S}$, $\|\mathcal{S}_f\| = \|\mathcal{S}_g\|$.

Let $\mathcal{S}^* = \{f \cup g : f \in \mathcal{S},\ g \in \mathcal{S}_f\}$, and for all $f \in \mathcal{S}$, $g \in \mathcal{S}_f$ and $i < A$, let $\sigma_{f\cup g,i} = \tau^\dagger_{g,i}$, where $\tau^\dagger_{g,i}$ is the lifting of $\tau_{g,i}$ to 2^s. We remark that

30.
$$\|\mathcal{S}^*\| \le |s| - (|s| - \|\mathcal{S}\|)^{1/k'} \le |s| - |s|^{1/k'}.$$

Using 29 we have that for all $i < A$,

$$\begin{aligned}\left|\bigcup_{f\in\mathcal{S}} \left((B^s_f \cap \beta_{f,i}) \triangle \left(B^s_f \cap \bigcup_{g\in\mathcal{S}_f} (B^s_g \cap \tau^\dagger_{g,i})\right)\right)\right| &\le |\mathcal{S}| \cdot 2^{s-\|\mathcal{S}\|-(|s|-\|\mathcal{S}\|)^{1/k'}} \\ &= 2^{|s|-(|s|-\|\mathcal{S}\|)^{1/k'}} \\ &\le 2^{|s|-|s|^{1/kk'}}.\end{aligned}$$

(The fact that $|\mathcal{S}| = 2^{\|\mathcal{S}\|}$ follows easily from the definition of an s-complete set.)

But

$$\bigcup_{f\in\mathcal{S}}\left(B^s_f\cap\bigcup_{g\in\mathcal{S}_f}(B^s_g\cap\tau^\dagger_{g,i})\right)=\bigcup_{h\in\mathcal{S}^*}(B^s_h\cap\sigma_{h,i}),$$

and so

$$\left|\bigcup_{f\in\mathcal{S}}(B^s_f\cap\beta_{f,i})\,\triangle\bigcup_{h\in\mathcal{S}^*}(B^s_h\cap\sigma_{h,i})\right|\le 2^{|s|-|s|^{1/kk'}}.$$

This, along with 28 and 30, implies that if we set $k^*=kk'+1$ then for all $i<A$,

$$\left|\bigcap_{j<A}\alpha_{i,j}\,\triangle\bigcup_{h\in\mathcal{S}^*}(B^s_h\cap\sigma_{h,i})\right|\le 2^{|s|-|s|^{1/k^*}}$$

and $\|\mathcal{S}^*\|\le|s|-|s|^{1/k^*}$, which is what we wanted to prove. □

31. The results of 7 and 8 can be used in the study of sets of the form Δ_0^B (see 1). For example, it's an open question whether the class of Δ_0 sets (without an oracle) is closed under "counting modulo 2", that is: does $B\in\Delta_0$ (where $B\subseteq\omega$) imply that $B^{\text{even}}\in\Delta_0$, where $B^{\text{even}}=\{n\in\omega:|m\le n:n\in B|\}$ is even? On the other hand, using the remark mentioned after the proof of 8 and an enumeration of the formulas in $\bigcup_{n\in\omega}E_n^R$, it is easy to construct a set $B\subseteq\omega$ such that $B^{\text{even}}\notin\Delta_0^B$ (see Paris-Wilkie below).

Closing, I'd like to mention an amusing result that can be proven using the same method. I leave the details as an exercise.

32. *Proposition.* (Ajtai)

Suppose that M is denumerable. Let $a\in M$ be non-standard, and $\tilde{a}$ be the substructure of M with domain $\{x\in M:x<a\}$ (recall that the language of M is relational). Then there exist $A,B\subseteq\{x\in M:x<a\}$, coded inside M, such that $(\tilde{a},A)\cong(\tilde{a},B)$ but, according to M, $|A|$ is even while $|B|$ is odd!

33. *Bibliography.*

M. Ajtai, Σ^1_1*-formulae on finite structures*, Annals of Pure and Applied Logic, Vol. 24(1), 1983.

J. Paris and A. J. Wilkie, *Counting problems in bounded arithmetic*, Proceedings of the Seventh Latin American Logic Congress, Caracas, Venezuela, 1983.