Ajtai's Completeness Theorem for Nonstandard Finite Structures

Michal Garlík *
Faculty of Mathematics and Physics
Charles University in Prague

Abstract

Ajtai's generalization of Gödel's completeness theorem is a tool that can be used to construct an extension of a given pseudo-finite structure into a model of a given theory. The existence of such model extensions is closely related to questions in complexity theory. In this paper we give a new proof of Ajtai's theorem using basic techniques of model theory.

1 Introduction

It is well known that various statements of complexity theory can be equivalently expressed in terms of mathematical logic, and model theory in particular. Some of these model-theoretic statements have a similar form asserting the existence of certain extensions of first-order structures. Let us mention informally three specific examples, all discussed already in detail in [3] (we refer the reader there for details of these equivalences).

Call a structure with a finite signature pseudo-finite if it is coded in a non-standard model of true arithmetic and is countably infinite. The statement that parity is not in $\mathbf{AC}^0$ is equivalent to the statement that there are pseudo-finite structures containing a unary predicate whose size is odd in the original non-standard model coding the structure but the same structure can be encoded in another non-standard model which thinks that the predicate is of even size. The statement that the pigeonhole principle has no polynomial size propositional proofs in constant depth Frege systems is equivalent to the statement that every pseudo-finite structure has an expansion by a function violating the pigeonhole principle while satisfying induction for all definable sets. Finally, the statements that the class NP is not closed under complementation is equivalent to the existence of non-3-colorable pseudo-finite graph such that any pseudo-finite

*Supported by grant GAUK 5732/2012 and in part by grant IAA100190902 of GA AV ČR. A part of this research has been done while the author was a visiting fellow at the Isaac Newton Institute in Cambridge (programme Semantics and Syntax) in Spring 2012.

structure on its vertices expanding the graph can be extended to a pseudo-finite structure containg a 3-coloring of the graph.

Note that Ajtai's original proofs of super-polynomial lower bounds for constant depth circuits for parity (Ajtai [1], indepedently also Furst, Saxe, Sipser [6]) and for constant depth Frege proofs of the pigeonhole principle (Ajtai [2]) proceeded by establishing first the equivalent model-theoretic statements. It is thus of great interest to understand when such extensions can be constructed. Ajtai [3] and [4] formulated a theorem that can be understood as a completeness theorem for the existence of similar extensions-expansions (see Section 4 for the statement). In this paper we give a new (and simpler) proof of this theorem.

2 Preliminaries

Definition 2.1. Let $L_0(exp)$ denote the first-order language of arithmetic with symbols $\leq, +, \cdot, 0, 1, 2^x$, where 2^x is a unary function symbol. A bounded quantifier is a quantifier of the form $\exists x \leq t$ or $\forall x \leq t$, where t is an $L_0(exp)$-term that does not include x. A $\Delta_0(exp)$-formula is a formula in the language $L_0(exp)$, in which all quantifiers are bounded. $I\Delta_0(exp)$ will denote the first-order theory in the language $L_0(exp)$ with the following axioms: the axioms of Robinson's arithmetic Q, $2^0 = 1$, $2^{(x+1)} = 2^x + 2^x$ and induction for all $\Delta_0(exp)$-formulas. We define $x \in y$ by the formula

$$\exists u \leq y \; \exists w < 2^x \; y = u \cdot 2^{x+1} + 2^x + w.$$

Let $B \subseteq M \models I\Delta_0(exp)$ and $b \in M$. We will say that b *codes* B in M if for each $x \in M$,

$$x \in B \Leftrightarrow M \models x \in b.$$

Note that $\Delta_0(exp)$-comprehension holds in $I\Delta_0(exp)$, that is, for each $\Delta_0(exp)$-formula $\varphi(x, \bar{z})$, $I\Delta_0(exp)$ proves

$$\forall x \exists y < 2^x \forall u < x (u \in y \leftrightarrow \varphi(u, \bar{z})).$$

Hence a subset of M which is not cofinal in M is $\Delta_0(exp)$-definable in M if and only if it is coded by an element in M. See [7] for details on the theory $I\Delta_0(exp)$.

Definition 2.2. Assume that M is a model of $I\Delta_0(exp)$. Let $L_0'(exp)$ be the same language as $L_0(exp)$ except that the functions of $L_0(exp)$ are treated as relations $\odot(x, y, z), \oplus(x, y, z), e(x, y)$. Let $a \in M$. Then $M \restriction a$ will denote the substructure for the language $L_0'(exp)$ which has universe

$$\{m \in M \mid M \models m \leq a\}.$$

Definition 2.3. Assume $\mathcal{L}$ is a first-order language containing a constant symbol a. Let φ be an $\mathcal{L}$-formula. Then $\varphi^{\leq a}$ is the formula we get by replacing every occurrence of $\forall x, \exists x$ in φ, where x is a variable, by $\forall x \leq a, \exists x \leq a$, respectively. If J is a set of formulas, $J^{\leq a}$ denotes the set $\{\varphi^{\leq a} \mid \varphi \in J\}$.

Definition 2.4. Assume $\mathcal{L}$ is a first-order language and A is an $\mathcal{L}$-structure. $\mathcal{L}(A)$ will denote the language we get from $\mathcal{L}$ by adding new constant symbols $\hat{a}$ for each $a \in A$ to $\mathcal{L}$. $\mathrm{Th}_{\mathcal{L}}(A)$, *the theory of* A, denotes the set of all $\mathcal{L}$-sentences true in A. Let A_A be the structure we get by expansion of A to $\mathcal{L}(A)$ such that for each $a \in A$ the constant symbol $\hat{a}$ is interpreted as a. The *atomic diagram of* A, which will be denoted by $\mathtt{diag}(A)$, is the set of all atomic and negated atomic sentences in the language $\mathcal{L}(A)$ that are true in A_A.

3 Proofs Definable in a Structure

Let **H** be any logical calculus for predicate logic, e.g. Hilbert-style calculus as defined in Chapter IV of [9]. Proofs in **H** can be thought of as finite trees whose nodes are labelled by formulas. The label of a node and the labels of its immediate successors form the conclusion and premises of either the rule modus ponens or the generalization rule. We are going to generalize the notion of an **H**-proof by allowing possibly infinite proof trees definable in a structure.

Suppose that $\mathcal{L}$ is a first-order language containing a finite number of relation and function symbols and A is a set, $|A| \geq 2$. $\mathtt{symb}(\mathcal{L})$ denotes the set of symbols of $\mathcal{L}$, that is relation and function symbols, symbols for variables, boolean operations, the existential and universal quantifiers, left and right parentheses and comma. We will want to represent the symbols of $\mathcal{L}(A)$ by the elements of a cartesian product A^i where i is a positive integer. So assume that for some positive integer i, $\mathtt{symb}(\mathcal{L})$ forms a subset of $A^i \setminus \{\langle a, a, \ldots, a\rangle \in A^i \mid a \in A\}$ and each symbol $\hat{a}$ is identified with the constant i-tuple $\langle a, a, \ldots, a\rangle$. Of course if A is finite there are only finitely many variables represented in this way in A^i. It would be easier to assume that A is infinite but later constructions do not need to assume that and we want to maintain maximal generality in this respect. Therefore for every $j > i$ we also consider an extended representation of the symbols of $\mathcal{L}(A)$ that will be denoted by $\mathtt{symb}^{(j,A)}(\mathcal{L}(A))$, such that the symbols of $\mathcal{L}(A)$ in A^i are naturally embedded in A^j in the following way. An element $\langle a_1, \ldots, a_i, a_{i+1}, \ldots, a_j\rangle$ is a non-variable symbol of $\mathtt{symb}^{(j,A)}(\mathcal{L}(A))$ iff $\langle a_1, \ldots, a_i\rangle$ is the corresponding non-variable symbol in A^i and $a_i = a_{i+1} = \ldots = a_j$. An element $\langle a_1, \ldots, a_i, a_{i+1}, \ldots, a_j\rangle$ is a variable symbol of $\mathtt{symb}^{(j,A)}(\mathcal{L}(A))$ iff $\langle a_1, \ldots, a_i\rangle$ is a variable symbol in A^i. Thus we have $|A|^{j-i}$ times more variables in $\mathtt{symb}^{(j,A)}(\mathcal{L}(A))$ than in A^i.

Definition 3.1. Let $\langle P, \leq\rangle$ be a partially ordered set and $a, b \in P$. We say that b is a *successor* of a if $a < b$ and there is no element $c \in P$ with $a < c < b$. We say that b is a *predecessor* of a if a is a successor of b.

Definition 3.2. A *tree* is a partially ordered set $\langle T, \leq_T\rangle$ satisfying the following conditions:

(1) There exists an element $0_T \in T$, which is called the *root of* T, such that for all $a \in T$ we have $0_T \leq a$.

(2) Suppose $a, b, c, d \in T$, $a < b < d$ and $a < c < d$. Then $b \leq c$ or $c \leq b$.

Definition 3.3. Suppose that $\mathcal{K}, \mathcal{L}$ are first-order languages, each containing a finite number of relation and function symbols, $\mathcal{K} \subseteq \mathcal{L}$, $\mathcal{K}$ contains a binary relation symbol $\leq$ and a constant symbol a. Assume that A is a $\mathcal{K}$-structure whose universe is linearly ordered by $\leq$ and a is the largest element with respect to $\leq$. Suppose that G is a theory in $\mathcal{L}(A)$. Let q, k, l be positive integers, $T \subseteq A^q$, $\leq_T \subseteq A^{2q}$ and $\Theta \subseteq A^{q+kl}$.

We say that $P = \langle T, \leq_T, \Theta \rangle$ is an $\mathbf{H}^{(A)}$*-proof from* G *with formula length* l if the following conditions are satisfied:

(1) The relations $T, \leq_T, \Theta$ are definable in A.

(2) $\langle T, \leq_T \rangle$ is a tree.

(3) $\mathtt{symb}(\mathcal{L}(A)) \subseteq A^r$ for some positive integer r, and $r \leq k$.

(4) The relation Θ is a function from T to A^{kl}, i.e. we can write

$$\bar{\Theta}(a_1, \ldots, a_q) = \langle a_{q+1}, \ldots, a_{q+kl} \rangle \quad \text{iff} \quad \Theta(a_1, \ldots, a_q, a_{q+1}, \ldots, a_{q+kl}).$$

(5) If $\langle a_1, a_2, \ldots a_{q+kl} \rangle \in A^{q+kl}$ and $\Theta(a_1, a_2, \ldots, a_{q+kl})$ then for every integer $i = 0, 1, \ldots, l-1$ we have

$$\langle a_{q+ki+1}, a_{q+ki+2} \ldots, a_{q+ki+k} \rangle \in \mathtt{symb}^{(k,A)}(\mathcal{L}(A))$$

and the sequence $\{\langle a_{q+ki+1}, a_{q+ki+2} \ldots, a_{q+ki+k} \rangle\}_{i=0}^{l-1}$ is an $\mathcal{L}(A)$-formula (padded on the left to length l using the symbol "," of $\mathcal{L}$ to accommodate all $\mathcal{L}(A)$-formulas of length at most l).

(6) If $\bar{c} \in T$ and the set S of its successors is nonempty then one of the two following conditions holds:

(i) $|S| \leq 2$ and the formulas assigned by the function $\bar{\Theta}$ to $\bar{c}$ and its successors are formed according to an inference rule of $\mathbf{H}$, i.e. by modus ponens or generalization.

(ii) There exist $\langle a_2, a_3, \ldots, a_q \rangle \in A^{q-1}$ and an $\mathcal{L}(A)$-formula $\varphi(x)$ with one free variable such that $S = \{\langle a_1, a_2, \ldots, a_q \rangle \mid a_1 \in A\}$, for every $a_1 \in A$ we have $\bar{\Theta}(a_1, a_2, \ldots, a_q) = \varphi(a_1)$ and $\bar{\Theta}(\bar{c}) = \forall x \leq a\ \varphi(x)$. In this case we will say that $\forall x \leq a\ \varphi(x)$ was derived from $\{\varphi(a_1) \mid a_1 \in A\}$ by the *A-rule*.

(7) If $\bar{c} \in T$ is a maximal element with respect to $\leq_T$, then $\bar{\Theta}(\bar{c})$ is an instance of an axiom scheme of $\mathbf{H}$ or a sentence from G.

Remark 3.4. Without further restrictions on the tree considered in this definition it may happen that the tree contains a non-maximal node without any successors, preventing the proof from being sound. In our application these problems will be resolved by assuming that the structure A has certain finiteness properties.

4 Ajtai's Completeness Theorem

Definition 4.1. Assume that $\mathcal{K}, \mathcal{L}$ are first-order languages, $\mathcal{K} \subseteq \mathcal{L}$, $\mathcal{K}$ contains a binary relation symbol $\leq$ and a constant symbol a. Suppose that A is a $\mathcal{K}$-structure such that $\leq$ is a linear order on A and a its largest element with respect to $\leq$. We say that an $\mathcal{L}$-structure B is *expanded end-extension* of A if it meets the following four requirements:

(1) B is linearly ordered by $\leq$.

(2) $\mathtt{universe}(A) \subseteq \mathtt{universe}(B)$ and for every $b \in B$, $B \models b \leq a$ iff $b \in A$.

(3) For all $k < \omega$, for all $b_1, \ldots, b_k \in A$ and for every k-ary relation symbol R in $\mathcal{K}$ we have $A \models R(b_1, \ldots, b_k)$ iff $B \models R(b_1, \ldots, b_k)$.

(4) For all $k < \omega$, for all $b_0, b_1, \ldots, b_k \in A$ and for every k-ary function symbol f in $\mathcal{K}$ we have $A \models f(b_1, \ldots, b_k) = b_0$ iff $B \models f(b_1, \ldots, b_k) = b_0$.

Assume further that G is a theory in $\mathcal{L}$. We say that G *has a model over* A if there exists a model B of G such that B is expanded end-extension of A.

The following theorem is essentially Ajtai's theorem from [4] formulated in our terminology.

Theorem 4.2. (Ajtai [4]). Suppose the following situation:

($\star$) $M \models I\Delta_0(exp)$ and a is a nonstandard element of M such that the set $\{b \in M \mid M \models b \leq a\}$ is countable. Assume that A is an expansion of $M{\restriction}a$ to a first-order language $\mathcal{K}$ containing a finite number of relation and function symbols such that every function and relation of A is coded by an element in M. Let a be also a constant symbol of $\mathcal{K}$ naming the element a.

Suppose further that $\mathcal{L} \supseteq \mathcal{K}$ is a first-order language containing a finite number of relation and function symbols and G is a theory in $\mathcal{L}$ such that the following conditions are satisfied:

(1) $G \vdash$ "$\leq$ is a linear order",

(2) There is a set $\widehat{G}$ coded by an element in M such that $\widehat{G} \cap \mathbb{N}$ is the set of Gödel numbers of the sentences from G.

(3) $G \vdash \forall \bar{u}\ [\exists x \leq a\ \varphi(x, \bar{u}) \rightarrow \exists x \leq a\ [\varphi(x, \bar{u}) \wedge \forall y < x\ \neg\varphi(y, \bar{u})]]$ for every $\mathcal{L}$-formula $\varphi(x, \bar{u})$.

Then the following two statements are equivalent:

(4) There exists a positive integer l and an $\mathbf{H}^{(A)}$-proof of a contradiction from $\mathtt{diag}(A) \cup G$ with formula length l.

(5) G does not have a model over A.

Let us remark that when G contains only sentences with quantifiers bounded by a one can use the well-known translation of first-order proofs into propositional proofs (see e.g. [10]) and state condition (4) equivalently using the provability in constant-depth Frege systems. In this way one gets the equivalence statement from the example with the pigeonhole principle mentioned in the introduction.

5 A New Proof of Ajtai's Completeness Theorem

Ajtai's original proof of the implication (5) $\Rightarrow$ (4) involves a lengthy and explicit construction of a model of G. We simplify this part significantly by utilizing the ideas behind the proof of the theorem due to Barwise and Schlipf [5] , and (independently) Ressayre [12], that states that countable recursively saturated structures are resplendent (cf. [8], Theorem 15.7, for a presentation). The proof of the implication (4) $\Rightarrow$ (5) is essentially that of Ajtai.

Lemma 5.1. *Suppose the situation* $(\star)$ *from Theorem 4.2. Assume that* $p(x)$ *is a type in the language* $\mathcal{K}$ *in* A *over* $a_0, \ldots, a_{n-1} \in A$, $n \in \omega$, *and suppose that there is* $d \in M$ *such that*

$$\{m \in M \mid M \models m \in d\} \cap \mathbb{N} = \{\ulcorner \varphi(x, x_0, \ldots, x_{n-1}) \urcorner \mid \varphi(x, a_0, \ldots, a_{n-1}) \in p(x)\}.$$

Then $p(x)$ *is realized in* A.

Proof. There exists a $\Delta_0(exp)$-formula $\mathrm{Tr}(t, u, v, w)$ such that for any $\mathcal{K}$-formula $\psi(\bar{z})$ and any tuple $\bar{c}$ of elements of A of the same length as $\bar{z}$ the following holds:

$$M \models \mathrm{Tr}(a, \langle \bar{e} \rangle, \ulcorner \psi(\bar{z}) \urcorner, \langle \bar{c} \rangle) \quad \text{iff} \quad A \models \varphi(\bar{c}),$$

where $\bar{e}$ are the elements of M coding the functions and relations of A. Since from the point of view of M all the quantifiers in ψ are bounded by a, as well as are the values of all the terms in $\psi(\bar{c})$, Tr can be constructed as a truth definition for bounded formulas with all the quantifiers in it bounded by exponential terms. See e.g. [11] for details of the truth definition.

Now let $\theta(s)$ be the following formula:

$$\exists r \leq a \; \forall y \leq s \, (y \in d \rightarrow \mathrm{Tr}(a, \langle \bar{e} \rangle, y, \langle r, a_0, \ldots, a_{n-1} \rangle)) \, .$$

It is a $\Delta_0(exp)$-formula with parameters $a, d, \bar{e}, a_0, \ldots a_{n-1}$ and since $p(x)$ is a type, $M \models \theta(i)$ for every $i \in \mathbb{N}$. Therefore, by overspill, there is a nonstandard $i \in M$ such that $M \models \theta(i)$. It follows that there exists an element in A that satisfies all the formulas from $p(x)$ in A, i.e. $p(x)$ is realized. $\square$

Lemma 5.2. *Suppose the situation* $(\star)$ *from Theorem 4.2. Suppose further that* $\mathcal{L} \supseteq \mathcal{K}$ *is a first-order language containing a finite number of relation and function symbols and* G *is a theory in* $\mathcal{L}$ *such that the following conditions are satisfied:*

(1) $G \vdash$ "$\leq$ *is a linear order*",

(2) *There is a set* $\widehat{G}$ *coded by an element in* M *such that* $\widehat{G} \cap \mathbb{N}$ *is the set of Gödel numbers of the sentences from* G.

Then the following two statements are equivalent:

(3) $\mathrm{Th}_{\mathcal{K}}(A)^{\leq a} \cup G$ *is consistent,*

(4) G *has a model over* A.

Proof. The implication (4)⇒(3) is obvious; let us prove (3)⇒(4). We will construct a complete theory J in the language

$$\mathcal{L}(A, C) = \mathcal{L} \cup \{b \mid b \in A\} \cup \{c_i \mid i < \omega\},$$

where we denote the constant symbol representing an element b by b itself and where $C = \{c_i \mid i < \omega\}$ are new distinct constant symbols, such that

(i) $G \subseteq J$,

(ii) for every $\mathcal{K}(A)$-sentence σ, $J \vdash \sigma^{\leq a} \Rightarrow A \models \sigma$,

(iii) if $\varphi(x)$ is an $\mathcal{L}(A, C)$-formula with only x free and $J \vdash \exists x \varphi(x)$, then either $J \vdash \varphi(c_i)$ for some $i < \omega$ or $J \vdash \varphi(b)$ for some $b \in A$,

(iv) for all $i < \omega$, $J \vdash a \leq c_i$.

It is clear that the canonical structure for the theory J is the desired model of G over A.

We will construct theories J_i ($i < \omega$) in the language $\mathcal{L}(A, C)$ such that the following two statements will hold for all $j < \omega$:

(v) If σ is a $\mathcal{K}(A)$-sentence and $J_j \vdash \sigma^{\leq a}$, then $A \models \sigma$.

(vi) There exists $l_j < \omega$ such that all the constants from C occurring in the formulas of J_j are exactly $c_0, c_1, \ldots, c_{l_j - 1}$.

Since $\mathrm{Th}_{\mathcal{K}}(A)^{\leq a} \cup G$ is consistent, (v) is true for $j = 0$ and $J_0 := G$. There are no constants from C in J_0, hence (vi) is true as well, with $l_0 = 0$.

Let $\{\varphi_i(x) \mid i < \omega\}$ be an enumeration of all $\mathcal{L}(A, C)$-formulas with only one free variable x such that every such formula occurs in it infinitely many times. (Here we use the assumption that A is countable.) Assume that J_i has been constructed so that (v) and (vi) hold for i. Let $k > i$ be the smallest integer such that the constants from C occurring in $\varphi_k(x)$ are among $c_0, c_1, \ldots, c_{l_i - 1}$. We shall construct J_{i+1} by adding to J_i one of the following formulas

- $\forall x \neg \varphi_k(x) \wedge a = c_{l_i}$,
- $\varphi_k(c_{l_i}) \wedge a < c_{l_i}$,
- $\varphi_k(b)$ for some $b \in A$

so that (v) and (vi) hold for $i + 1$.

Before we show that one of these choices can be made, note that if $\varphi_k(x)$ is $a < x$, J_{i+1} has to include the new constant c_{l_i} in its language. As $a < x$ will be dealt with infinitely many times during the construction of all J_j's ($j < \omega$),

every constant from C will eventually appear in the language of J_j for some $j < \omega$. Therefore every $\mathcal{L}(A, C)$-formula will be treated at some step of the construction. And it is clear that once all J_j's are constructed satisfying (v) and (vi), the theory $J = \bigcup_{j<\omega} J_j$ has the required properties (i)-(iv).

It remains to show that J_{i+1} can be constructed by adding one of the above formulas to J_i so that (v) is true for $i+1$. Let $a_0, \ldots, a_{n-1}$ be the elements of A occurring in $J_i \cup \{\varphi_k(x)\}$ and suppose, for a contradiction, that none of the above choices can be made. Then there are $\mathcal{K} \cup \{a_0, \ldots, a_{n-1}\}$-sentences σ, γ, η_r for all $r < n$, and for all $b \in A \setminus \{a_0, \ldots, a_{n-1}\}$ there is a $\mathcal{K} \cup \{a_0, \ldots, a_{n-1}\}$-formula $\xi_b(x)$ such that

$$\begin{aligned} J_i + \forall x \neg\varphi_k(x) \wedge a = c_{l_i} &\vdash \sigma^{\leq a} \\ J_i + \varphi_k(c_{l_i}) \wedge a < c_{l_i} &\vdash \gamma^{\leq a} \\ J_i + \varphi_k(a_r) &\vdash \eta_r^{\leq a} \text{ for all } r < n \\ J_i + \varphi_k(b) &\vdash \xi_b^{\leq a}(b) \text{ for all } b \in A \setminus \{a_0, \ldots, a_{n-1}\} \end{aligned}$$

but $A \not\models \sigma$, $A \not\models \gamma$, $A \not\models \eta_r$ for all $r < n$, and $A \not\models \xi_b(b)$ for all elements b in $A \setminus \{a_0, \ldots, a_{n-1}\}$. Using the fact that c_{l_i} does not occur in $J_i + \varphi_k(x)$ it follows that

$$\begin{aligned} J_i + \neg\sigma^{\leq a} &\vdash \exists x \varphi_k(x) \\ J_i &\vdash \forall x(\varphi_k(x) \wedge \neg\gamma^{\leq a} \to x \leq a) \\ J_i &\vdash \forall x(\varphi_k(x) \wedge \bigwedge_{r<n} \neg\eta_r^{\leq a} \to \bigwedge_{r<n} x \neq a_r). \end{aligned}$$

Thus if $\theta(x)$ is a $\mathcal{K} \cup \{a_0, \ldots, a_{n-1}\}$-formula and

$$J_i \vdash \forall x(\varphi_k(x) \wedge x \leq a \wedge \bigwedge_{r<n} x \neq a_r \to \theta^{\leq a}(x))$$

then

$$J_i \vdash \neg\sigma^{\leq a} \wedge \neg\gamma^{\leq a} \wedge \bigwedge_{r<n} \neg\eta_r^{\leq a} \to (\exists x \leq a)\theta^{\leq a}(x).$$

By the induction hypothesis it follows that $A \models \exists x \theta(x)$. This consideration shows that the set $p(x)$ consisting of all $\mathcal{K} \cup \{a_0, \ldots, a_{n-1}\}$-formulas of the form $\theta(x) \wedge \theta(x) \wedge \ldots \wedge \theta(x)$ (s conjunctions) such that there is a proof from J_i of length s of the sentence

$$\forall x(\varphi_k(x) \wedge x \leq a \wedge \bigwedge_{r<n} x \neq a_r \to \theta^{\leq a}(x))$$

is a type in A. Moreover, there exists a $\Delta_0(exp)$-formula $\pi(y)$ such that

$$\{m \in M \mid M \models \pi(m)\} \cap \mathbb{N} = \{\ulcorner \delta \urcorner \mid \delta \in p(x)\}.$$

(Here we use the condition (2).) Hence there is d in M such that

$$\{m \in M \mid M \models m \in d\} \cap \mathbb{N} = \{\ulcorner \delta \urcorner \mid \delta \in p(x)\},$$

by $\Delta_0(exp)$-comprehension. By Lemma 5.1, $p(x)$ is realized by some element $b \in A \setminus \{a_0, \ldots, a_{n-1}\}$ (because a formula equivalent to $\bigwedge_{r<n} x \neq a_r$ is in $p(x)$). But for this b we have $J_i + \varphi_k(b) \vdash \xi_b^{\leq a}(b)$. Since b does not occur in J_i it follows that $J_i \vdash \forall x(\varphi_k(x) \to \xi_b^{\leq a}(x))$ so we have that $\xi_b(x) \wedge \xi_b(x) \wedge \ldots \wedge \xi_b(x)$ is in $p(x)$ for some suitable number of conjuncts. Thus $A \models \xi_b(b)$, a contradiction with our assumption on $\xi_b(x)$. Thus J_{i+1} can be found satisfying (v) for $i+1$ and by its construction it obviously satisfies (vi).

□

Definition 5.3. Suppose that $\mathcal{H}$ is a first-order language, B is an $\mathcal{H}$-structure, k is a positive integer, $X \subseteq (\mathtt{universe}(B))^k$ is a definable set in B and $\leq$ is a definable linear order on X. We say that X is *quasi-finite in B with respect to* $\leq$ if the following requirements are met:

(1) X has a smallest and a largest element,

(2) each definable nonempty subset of X has a smallest element,

(3) each element of X, except for the smallest one, has a predecessor.

Lemma 5.4. *Assume that $\mathcal{H}$ is a first-order language, B is an $\mathcal{H}$-structure, X is a definable set in B which is quasi-finite in B with respect to a definable linear order $\leq$ on X. Suppose that i is a positive integer and $\langle P, \leq_P \rangle$ is a nonempty partial order definable in B so that $P \subseteq X^i$. Then P has a minimal element.*

Proof. Let $Y = X^i$ and $\leq_Y$ be the lexicographic order on Y induced by $\leq$. It is easily checked that $\leq_Y$ is definable in B and that Y is quasi-finite in B with respect to $\leq_Y$. Next we verify that each definable nonempty subset U of Y has a largest element in $\leq_Y$. Indeed, it is either the largest element 1_Y of Y if $1_Y \in U$, or it is the predecessor of the least element of the set $\{x \in Y \mid \neg\exists y\,(y \in U \wedge x \leq_Y y)\}$.

Consider the set $V = \{x \in P \mid \forall y \in P\,(y \leq_P x \to x \leq_Y y)\}$. V is nonempty because it contains the $\leq_Y$-smallest element of P. Let v be the $\leq_Y$-largest element of V. Either v is a minimal element of $\langle P, \leq_P \rangle$ or the set $W = \{x \in P \mid x <_P v\}$ is nonempty. We will show that the latter case leads to a contradiction. Consider the $\leq_Y$-smallest element w of W. Since $v \in V$ and $w <_P v$ we have $v <_Y w$. Because of the maximality of v in V we get $w \notin V$ and so there must exist $u \in P$ with $u \leq_P w$ and $u <_Y w$. By transitivity of $\leq_P$ we get $u <_P v$ and so $u \in W$ in contradiction to the minimality of w. □

Proof of Ajtai's Completeness Theorem.
First we show the implication (5)⇒(4). If G does not have a model over A, then by Lemma 5.2 there exists a proof of a contradiction from $\mathrm{Th}_{\mathcal{K}}(A)^{\leq a} \cup G$. Since the proof is finite, there exists an $\mathbf{H}^{(A)}$-proof P_0 of a contradiction from

$\mathrm{Th}_{\mathcal{K}}(A)^{\leq a} \cup G$ with formula length l for some positive integer l. Thus it remains to find an $\mathbf{H}^{(A)}$-proof from $\mathtt{diag}(A)$ of each of the finitely many sentences of $\mathrm{Th}_{\mathcal{K}}(A)^{\leq a}$ that occur as axioms in P_0 and attach these proofs to P_0. It suffices to show the following claim.

Claim: For every $\mathcal{K}$-formula $\alpha(\bar{x})$, where $\bar{x} = \langle x_1, \ldots, x_n \rangle$ for some positive integer n, there exist $\mathcal{K}(A)$-formulas $\tau^{\alpha}(\bar{x}, \bar{u})$, $\lambda^{\alpha}(\bar{x}, \bar{v})$, $\phi^{\alpha}(\bar{x}, \bar{w})$ (where $\bar{u}, \bar{v}, \bar{w}$ are some tuples of free variables) such that for every $\bar{a} = \langle a_1, \ldots, a_n \rangle \in A^n$, if $A \models \alpha(\bar{a})$ then the triple of relations defined in A by formulas $\tau^{\alpha}(\bar{a}, \bar{u}), \lambda^{\alpha}(\bar{a}, \bar{v}), \phi^{\alpha}(\bar{a}, \bar{w})$ is an $\mathbf{H}^{(A)}$-proof of $\alpha^{\leq a}(\bar{a})$ from $\mathtt{diag}(A)$.

To prove the claim, we may assume that in α negation only occurs in front of atomic formulas. We proceed by induction on the logical complexity of α. The claim is obvious if α is an atomic or negated atomic formula. For α of the form $\alpha_1 \wedge \alpha_2$ we just join the $\mathbf{H}^{(A)}$-proofs of $\alpha_1^{\leq a}$, $\alpha_2^{\leq a}$ and of an appropriate axiom by applying modus ponens twice. Similarly for α of the form $\alpha_1 \vee \alpha_2$. If $\alpha(\bar{x})$ is $\forall x_0 \, \beta(x_0, \bar{x})$ we use the induction hypotheses for β to uniformly (in $\bar{a}$'s satisfying $A \models \alpha(\bar{a})$) define a family of $|A|$ disjoint $\mathbf{H}^{(A)}$-proofs of $\beta^{\leq a}(b, \bar{a})$ ($b \in A$) and join these proofs by an application of the A-rule. Finally, let α be of the form $\exists x_0 \, \beta(x_0, \bar{x})$. From the assumptions ($\star$) it easily follows that the least number principle for $\mathcal{K}$-formulas holds in A. So we apply it to the formula $\beta(x_0, \bar{x})$ with parameters $\bar{x}$ and use the induction hypotheses to uniformly (in $\bar{a}$'s satisfying $A \models \alpha(\bar{a})$) define the $\mathbf{H}^{(A)}$-proof of $\beta^{\leq a}(b, \bar{a})$ with b the least possible such that $A \models \beta(b, \bar{a})$. Then we join this proof by modus ponens with an instance of $\exists$-introduction axiom. This completes the proof of the claim and of the implication (5)$\Rightarrow$(4).

Now we show the implication (4) $\Rightarrow$ (5). Suppose there exists an $\mathbf{H}^{(A)}$-proof P of a contradiction from $\mathtt{diag}(A) \cup G$ with formula length l, but contrary to (5), there exists a model N of G over A. $\mathtt{universe}(A)$ is defined in N by the formula $x \leq a$. All the functions and relations of A are definable in N by restricting the functions and relations of the same name in N to elements $\leq a$. Therefore the components $T, \leq_T, \Theta$ of P are defined in N as well. It follows from the way A originated from $M \models I\Delta_0(exp)$ and from the condition (3) of the theorem that $\mathtt{universe}(A)$ is quasi-finite in N with respect to $\leq$. We know that $T \subseteq (\mathtt{universe}(A))^q$ for some positive integer q. Therefore Lemma 5.4 implies that each nonempty subset of T which is definable in N has a maximal and a minimal element with respect to $\leq_T$.

The lengths of the formulas of the proof P are bounded by l, the symbols of $\mathcal{L}(A)$ used in these formulas are those of $\mathtt{symb}^{(k,A)}(\mathcal{L}(A))$ for some positive integer k and the language $\mathcal{L}$ contains only finitely many function and relation symbols. Therefore there exists a function $\Gamma : A^{kl} \mapsto \{0, 1\}$ definable in N that assigns truth value in N to each $\mathcal{L}(A)$ formula $\{\langle a_{i+1}, \ldots, a_{i+k} \rangle\}_{i=0}^{l-1} \in (A^k)^l$.

Now let F be the set of those elements t of T that satisfy $\Gamma(\bar{\Theta}(t)) = 0$. For the root 0_T of T we have that $\bar{\Theta}(0_T)$ is a contradiction, so F is nonempty. Since F is a nonempty definable subset of T there exists an element $m \in F$ which is maximal in F with respect to $\leq_T$. If t is a maximal element of $\langle T, \leq_T \rangle$ then $\bar{\Theta}(t)$ is an instance of an axiom scheme of $\mathbf{H}$ or a sentence from $\mathtt{diag}(A) \cup G$,

so $\bar{\Theta}(t)$ holds in N. Therefore m cannot be a maximal element of $\langle T, \leq_T \rangle$. Let $Q = \{t \in T \mid m <_T t\}$. Since Q is a nonempty definable subset of T it has a minimal element with respect to $\leq_T$. Let $S \subseteq Q$ be the set of minimal elements of Q with respect to $\leq_T$. It is the set of all $\leq_T$-successors of m and by the definition of $\mathbf{H}^{(A)}$-proof the formulas assigned by $\bar{\Theta}$ to m and its successors must satisfy one of the inference rules. The inference rules have the property that for every element $t \in T$ the formula $\bar{\Theta}(t)$ is true in N if for every successor t' of t the formula $\bar{\Theta}(t')$ is true in N. (The case of the A-rule relies here on the fact that N is a model over A). This contradicts to $\Gamma(\Theta(s)) = 1$ for all $s \in S$. □

References

[1] M. Ajtai, Σ^1_1-*formulae on finite structures*, Annals of Pure and Applied Logic 24 (1983) 1-48

[2] M. Ajtai, *The Complexity of the Pigeonhole Principle*, Proceedings of the IEEE 29th Annual Symposium on Foundation of Computer Science (1988) 346-355

[3] M. Ajtai, *Generalizations of the Compactness Theorem and Gödel's Completeness Theorem for Nonstandard Finite Structures*, Proceedings of the 4th international conference on Theory and applications of models of computation (2007) 13-33.

[4] M. Ajtai, *A Generalization of Gödel's Completeness Theorem for Nonstandard Finite Structures*, manuscript (2011)

[5] J. Barwise, J. Schlipf, *An Introduction to Recursively Saturated and Resplendent Models* J. Symbolic Logic, 41 (1976) 531-536

[6] M. Furst, J. Saxe, M. Sipser, *Parity, Circuits, and the Polynomial-Time Hierarchy*, Mathematical Systems Theory 17 (1984) 13-27

[7] P. Hájek, P. Pudlák, *Metamathematics of first order arithmetic*, Springer, 1993

[8] R. Kaye, *Models of Peano Arithmetic*, Oxford Logic Guides 15, Oxford University Press, 1991

[9] S. C. Kleene, *Introduction to metamathematics*, D. Van Nostrand Co., Inc., New York, N. Y., 1952.

[10] J. Krajíček, *Bounded Arithmetic, Propositional Logic, and Complexity Theory*, Cambridge University Press, 1995

[11] J. Paris and C. Dimitracopoulos, *Truth definitions for* Δ_0 *formulae*, Logic and Algorithmic, L'Enseignement Mathematique Monographie no 30, Geneva, (1982) 317-330.

[12] J. P. Ressayre, *Models with Compactness Properties Relative to an Admissible Language*, Annals of Pure and Applied Logic 11 (1977) 31-55.