Notre Dame Journal of Formal Logic
Volume 49, Number 1, 2008

Decidability of $\exists^*\forall\forall$-sentences in HF

D. Bellè and F. Parlamento

Abstract Let **HF** be the collection of the hereditarily finite well-founded sets and let the primitive language of set theory be the first-order language which contains binary symbols for equality and membership only. As announced in a previous paper by the authors, "Truth in **V** for $\exists^*\forall\forall$-sentences is decidable," truth in **HF** for $\exists^*\forall\forall$-sentences of the primitive language is decidable. The paper provides the proof of that claim.

1 Introduction

Let **V** be the cumulative set theoretic hierarchy generated from the empty set by taking powers at successor stages and unions at limit stages and, following [2], let the primitive language of set theory be the first-order language which contains binary symbols for equality and membership only. As shown in [1], the satisfiability in **V** of $\forall\forall$-formulas of the primitive language is reducible to the problem of determining, given a set $\mathcal{G}$ of graphs on $\{1, \ldots, n, n+1, n+2\}$ having a common restriction to $\{1, \ldots, n\}$, whether or not there is an extensional well-founded binary structure with n distinguished elements, which, taken together with two other distinct elements of the structure, generate graphs that (up to isomorphism, of course) all belong to $\mathcal{G}$. Binary structures fulfilling the last requirement will be called $\mathcal{G}$-structures. A difficulty with the latter problem is that the existence of a well-founded extensional $\mathcal{G}$-structure does not necessarily entail the existence of a finite well-founded extensional $\mathcal{G}$-structure. As shown in [1], that difficulty can be overcome by relaxing the requirement of extensionality into a requirement of *quasi extensionality* and proving that there is a well-founded extensional $\mathcal{G}$-structure if and only if there is a well-founded quasi-extensional $\mathcal{G}$-structure whose cardinality is primitively recursively bounded with respect to n. Decidability follows since there are only finitely many binary structures of bounded cardinality and for each one of them we can effectively detect whether it is a well-founded quasi-extensional $\mathcal{G}$-structure or not. Whenever

Received March 19, 2007; accepted July 6, 2007; printed December 3, 2007
2000 Mathematics Subject Classification: Primary, 03B25; Secondary, 03E30, 03C62
Keywords: quantifiers, decidability, hereditarily finite sets
 10.1215/00294527-2007-003

a well-founded quasi-extensional $\mathcal{G}$-structure, say $\mathcal{M}$, is found, one knows that there is a well-founded extensional $\mathcal{G}$-structure, but there seems to be no way, based solely on an inspection of $\mathcal{M}$, to determine whether one can succeed also in the more demanding task of building a finite well-founded extensional $\mathcal{G}$-structure.

In the present paper we overcome that problem by showing that if there is a finite extensional $\mathcal{G}$-structure, then there is a quasi-extensional $\mathcal{G}$-structure which can be modified so as to obtain a finite well-founded extensional $\mathcal{G}$-structure, whose cardinality is itself primitively recursively bounded with respect to n. Thus decidability of the existence of a finite well-founded extensional $\mathcal{G}$-structure can be achieved by inspecting the finite set of all the finitely many binary structures whose cardinality is bounded in that way, to determine whether it contains one which is a well-founded extensional $\mathcal{G}$-structure or not. The decidability of the satisfiability in **HF** of the $\forall\forall$-formulas of the primitive language follows since, by essentially the same argument given in [1] concerning **V**, that problem can be reduced to the problem of establishing for $\mathcal{G}$ as above, whether there is a finite well-founded extensional $\mathcal{G}$-structure or not.

2 Basic Definitions and Reduction

The following are the relevant definitions and properties from [1]. They all refer to structures of the form $\mathcal{M} = (M, c_1, \dots, c_n, E)$, with $M \neq \varnothing$, where $c_1, \dots, c_n$ are pairwise distinct elements of M and E is a binary relation which is well-founded on M.

Definition 2.1

1. a is *discernible* from b in M with respect to E, or E*-discernible* from b in M, if there is c in M such that $(c, a) \in E \equiv (c, b) \notin E$; such a c is said to be an E*-differentiating* element of a and b or an E*-witness* of the difference between a and b.
2. E is *extensional* on a in M if a is E-discernible in M from all the elements in $M \setminus \{a\}$. $\mathcal{M}$ is extensional if E is extensional in M on all the elements of M.
3. For $a \in M \setminus \{c_1, \dots, c_n\}$, the *type* of a in $\mathcal{M}$, denoted by $\tau^{\mathcal{M}}(a)$, is the pair (J, I) where $J = \{j : (c_j, a) \in E\}$ and $I = \{i : (a, c_i) \in E\}$.
4. An *n-type* is a pair of the form (J, I) such that $J, I \subseteq \{1, \dots, n\}$. An n-type A is said to be *realized* in $\mathcal{M}$ if, for some $a \in M \setminus \{c_1, \dots, c_n\}$, $\tau^{\mathcal{M}}(a) = A$.
5. For $|M| \geq n + 2$, $\mathcal{G}(\mathcal{M})$ is the set of all graphs on $\{1, \dots, n, n + 1, n + 2\}$ which are isomorphic to the restriction $E|\{c_1, \dots, c_n, a, b\}$ of E under the map which sends $1, \dots, n, n + 1, n + 2$ into $c_1, \dots, c_n, a, b$, respectively, for some a and b distinct elements of $M \setminus \{c_1, \dots, c_n\}$.
6. For a set $\mathcal{G}$ of $n + 2$-graphs, if $\mathcal{G}(\mathcal{M}) \subseteq \mathcal{G}$ we say that $\mathcal{M}$ is a $\mathcal{G}$*-structure*.
7. The graph in $\mathcal{G}(\mathcal{M})$, determined by the pair (a, b) of distinct elements of M, can be recovered from $\tau^{\mathcal{M}}(a)$, $\tau^{\mathcal{M}}(b)$ with the addition of the pair $(n + 1, n + 2)$ or $(n + 2, n + 1)$ if $(a, b) \in E$ or $(b, a) \in E$, respectively.

Since E is assumed to be well-founded on M, the graphs in $\mathcal{G}(\mathcal{M})$ are acyclic. In any case they all have a common restriction to $\{1, \dots, n\}$, which is isomorphic to $E|\{c_1, \dots, c_n\}$. In the sequel we will omit reference to $\mathcal{M}$ whenever the latter is clear from the context. For example, we will write $\tau(a)$ instead of $\tau^{\mathcal{M}}(a)$ whenever it is clear that a belongs to the domain of $\mathcal{M}$. Furthermore, the graphs on $\{1, \ldots, n, n+1, n+2\}$ are going to be called $n+2$-graphs and whenever a set of $n+2$-graphs $\mathcal{G}$ is considered, it will be tacitly assumed that all the graphs in $\mathcal{G}$ have the same restriction to $\{1, \ldots, n\}$.

Any acyclic graph on $\{1, \ldots, n, n+1, n+2\}$, with a given restriction to $\{1, \ldots, n\}$, can be described as $(A, B, \circ)$, where A and B are n-types (those of $n+1$ and $n+2$ in the given graph) and $\circ = \rightarrow$ if $(n+1, n+2)$ belongs to the graph, $\circ = \leftarrow$ if $(n+2, n+1)$ belongs to the graph, and $\circ =:$ if neither belongs to the graph.

Definition 2.2 Given a set $\mathcal{G}$ of $n+2$-graphs, we say that an n-type A *belongs* to $\mathcal{G}$, or A is in $\mathcal{G}$, if $(A, B, \circ)$ or $(B, A, \circ)$ belongs to $\mathcal{G}$ for some n-type B and $\circ \in \{:, \leftarrow, \rightarrow\}$.

Throughout the sequel $\mathcal{G}$ is assumed to be a set of $n+2$-graphs, and n-types are simply called types.

Definition 2.3 For A and B types which belong to $\mathcal{G}$ and $\circ \in \{\rightarrow, \leftarrow, :\}$ we say that

1. A is a *predecessor* type of B in $\mathcal{G}$, if $(A, B, \circ) \in \mathcal{G}$ implies that $\circ$ is $\rightarrow$;
2. A is *tied* with B in $\mathcal{G}$ if $(A, B, \circ) \in \mathcal{G}$ implies that $\circ$ is either $\rightarrow$ or $\leftarrow$;
3. B is a *differentiating* type of A in $\mathcal{G}$, if $(B, A, \rightarrow) \in \mathcal{G}$ and either $(B, A, :) \in \mathcal{G}$ or $(B, A, \leftarrow) \in \mathcal{G}$;
4. B is a *free differentiating* type of A in $\mathcal{G}$ if B is a differentiating type of A in $\mathcal{G}$ and A and B are not tied in $\mathcal{G}$.

Definition 2.4

1. A *differentiating cycle* in $\mathcal{G}$ is a sequence of types $B_0, \ldots, B_{k-1}$ which belong to $\mathcal{G}$ such that, for $i < k-1$, B_i is a differentiating type for B_{i+1}, B_{k-1} is a differentiating type for B_0, and, for $i, j < k$, B_i is not a predecessor type for B_j.
2. A *tied cycle* in $\mathcal{G}$ is a differentiating cycle in $\mathcal{G}$ of the form (B_0, B_1) such that B_0 and B_1 are tied in $\mathcal{G}$.
3. A *free cycle* in $\mathcal{G}$ is a differentiating cycle in $\mathcal{G}$ of pairwise distinct types $B_0, \ldots, B_{k-1}$ such that for $i < k-1$ B_i is a free differentiating type of B_{i+1} and B_{k-1} is a free differentiating type of B_0.

Note 2.5 There is a slight change here with respect to the notions used in [1] in that there B_{i+1} is required to be a differentiating type of B_i (and B_{k-1} of B_0). Such a switch is inessential as far as the proof of Proposition 4.1 in [1] goes, but it somewhat simplifies the notations to be used in the foregoing proof.

2.1 Reduction By adapting arguments given in [1] one easily obtains the following reduction of our decision problem.

Proposition 2.6 *The decision problem for truth in the collection* **HF** *of the hereditarily finite well-founded sets of $\exists^*\forall\forall$-sentences is reducible to the problem of determining, for any set $\mathcal{G}$ of $n+2$-graphs, whether or not there is a finite extensional well-founded $\mathcal{G}$-structure.*

We will show that, contrary to what happens in the case of **V**, in the case of **HF** decidability can be attained by placing a bound on the cardinality, hence on the number, of the finite extensional well-founded $\mathcal{G}$-structures that need to be tried.

2.2 Basic structures A basic structure introduced in [1] is the binary structure k_3^--*curl* with $k > 1$ whose domain, letting c_{ij} denote the pair of natural numbers (i, j), is

$$C_{k_3} = \{c_{ij} : 0 \leq i < k, 0 \leq j < 3\} \cup \{(0, 3)\}$$

and whose binary relation is

$$E_{k_3}^- = \{(c_{ij}, c_{i+1,j'}) : 0 \leq i < k-1, j \leq j' < 3 \mid i = 0 \vee j \neq 0 \vee j' \neq 2\} \\ \cup \{(c_{k-1,j}, c_{0j'}) : j < j' < 3 | j \neq 0 \vee j' \neq 3\}.$$

For the foregoing proof we will use the following straightforward generalization of that notion.

Definition 2.7 For $3 \leq m$, the k_m^--*curl* is the binary structure whose domain is

$$C_{k_m} = \{c_{ij} : 0 \leq i < k, 0 \leq j < m\} \cup \{(0, m)\}$$

and whose binary relation is

$$E_{k_m}^- = \{(c_{ij}, c_{i+1,j'}) : 0 \leq i < k-1, j \leq j' < m | i = 0 \vee j \neq 0 \vee j' \neq m-1\} \\ \cup \{(c_{k-1,j}, c_{0j'}) : j < j' < m \mid j \neq 0 \vee j' \neq m\}.$$

2.3 Free-enoughness

Definition 2.8 Let $\mathcal{M} = (M, c_1, \dots, c_n, E)$ be a well-founded $\mathcal{G}$-structure and $<$ be a well-ordering of M which extends E on M. We say that a cycle $(B_0, \dots, B_{k-1})$ (strictly) covers an element a of M if (strictly) above a, with respect to $<$, there are elements of type B_i for each $0 \leq i \leq k-1$.

An element a of M is said to be *free enough* in $\mathcal{M}$ with respect to $<$ and $\mathcal{G}$ (free enough for short) if one, at least, of the following three conditions is satisfied.

Condition 1 In $\mathcal{G}$ there is a tied cycle (B_0, B_1), with $B_0 = \tau(a)$, such that, letting $s = \text{maxmin}_<^{\mathcal{M}}(B_0, B_1)$, $a > s$, (B_0, B_1) strictly covers s, and if $B_1 = (J_1, I_1)$ and $i \in I_1$, then $a < c_i$.

Condition 2 In $\mathcal{G}$ there is a free cycle $(B_0, B_1, \dots, B_{k-1})$ with $B_0 = \tau(a)$ such that, letting $s = \text{maxmin}_<^{\mathcal{M}}(B_0, \dots, B_{k-1})$, $a > s$ and $B_0, \dots, B_{k-1}$ strictly covers s.

Condition 3 In M there are elements $a_1, \dots, a_h, b_0$ of types $A_1, \dots, A_h, B_0$, respectively, such that

(a) $a > a_1 > a_2 > \cdots > a_h > b_0$;
(b) if $h > 0$, then A_1 is a free differentiating type of $\tau(a)$ in $\mathcal{G}$; for $0 < i < h$, A_{i+1} is a free differentiating type of A_i in $\mathcal{G}$, and B_0 is a free differentiating type of A_h in $\mathcal{G}$;
(c) if $h = 0$, then B_0 is a free differentiating type of $\tau(a)$ in $\mathcal{G}$;
(d) b_0 satisfies Condition 1 or Condition 2 above.

Note 2.9 The requirement that $B_1 = (J_1, I_1)$ and $i \in I_1$, then $a < c_i$, in Condition 1 above, retained from [1], is not really needed for the subsequent proof.

3 Proof of Decidability

Proposition 3.1 *If $\mathcal{G}$ is a set of $n + 2$-graphs all having the same restriction to $\{1, \ldots, n\}$ and there is a finite extensional well-founded $\mathcal{G}$-structure, then there is an extensional well-founded $\mathcal{G}$-structure whose cardinality is primitively recursively bounded with respect to n.*

Proof Let $\mathcal{M} = (M, c_1, \ldots, c_n, E)$ be a finite extensional well-founded $\mathcal{G}$-structure and let $<$ be a total ordering of M which extends E. Let t be the number of types which are realized in $\mathcal{M}$. Trivially, t is exponentially bounded with respect to n. By Proposition 4.1 in [1], the set N of elements of M which are not free enough in $\mathcal{M}$ with respect to $\mathcal{G}$ is bounded by $\lambda(t)$, where λ is a primitive recursive function. For A a type realized in $\mathcal{M}$, let $\min^{\mathcal{M}}_{<}(A)$ ($\max^{\mathcal{M}}_{<}(A)$) be the minimum (maximum) with respect to $<$ of the elements of M of type A. If $A_1, \ldots, A_t$ are the types realized in $\mathcal{M}$, let $s_1 = \min^{\mathcal{M}}_{<}(A_1), \ldots, s_t = \min^{\mathcal{M}}_{<}(A_t)$ and $m_1 = \max^{\mathcal{M}}_{<}(A_1), \ldots, m_t = \max^{\mathcal{M}}_{<}(A_t)$. Let N_0 be obtained by adding to $N \cup \{c_1, \ldots, c_n, s_1, \ldots, s_t, m_1, \ldots, m_t\}$ the maxima of the E-predecessors of the c_is and of the s_is. Notice that since M is finite all such maxima actually exist. Finally, add a minimal differentiating set Δ in $\mathcal{M}$, for the set N_0, and let M_0 be the subset of M thus obtained. Obviously, $|M_0|$ is primitively recursively (*pr. ric.*) bounded with respect to n. Let $\mathcal{M}_0$ be the restriction of $\mathcal{M}$ to its subdomain M_0. If $\mathcal{M}_0$ is extensional, our claim is proved. Otherwise, we proceed as follows. By the construction, if two elements a and b of M_0 are not E-discernible in $\mathcal{M}_0$, then at least one among a and b belongs to Δ, so that it is free-enough in $\mathcal{M}$ with respect to $\mathcal{G}$. Let $\text{maxmin}^{\mathcal{M}}_{<}(B_0, \ldots, B_{k-1})$ denote the maximum with respect to $<$ of the set $\{\min^{\mathcal{M}}_{<}(B_0), \ldots, \min^{\mathcal{M}}_{<}(B_{k-1})\}$. Given $s \in \{s_1, \ldots, s_t\}$, if there is a differentiating cycle γ in $\mathcal{G}$ such that $s = \text{maxmin}^{\mathcal{M}}_{<}\gamma$ and γ strictly covers s in $\mathcal{M}_0$, let $\alpha_1, \ldots, \alpha_u$ and $\beta_1, \ldots, \beta_v$ be the tied and free cycles, respectively, of $\mathcal{G}$, whose $\text{maxmin}^{\mathcal{M}}_{<}$ is s and which strictly cover s. Furthermore, let the initial type of all such cycles be $\tau(s)$. From the fact that they strictly cover the same element s, it easily follows that their concatenation $\alpha_1 \ldots \alpha_u \beta_1 \ldots \beta_v$ is a differentiating cycle, namely, that if the types B and B' belong to some of the cycles $\alpha_1, \ldots, \beta_v$, then B is not a predecessor type of B'. Let $(A_0, \ldots, A_{k-1})$ be $\alpha_1, \ldots, \alpha_u, \beta_1, \ldots, \beta_v$ and $m = 1 + 2 \cdot p$, where p is the number of pairs of E-indiscernible elements of M_0. Let $\mathcal{M}_0\{s/k^-_m(A_0, \ldots, A_{k-1})\}$ be the result of replacing s in $\mathcal{M}_0$ by the k^-_m-*curl* and extending the binary relation E into the binary relation E_s in the following way. If c_{ij} is an element of the k^-_m-*curl* which replaces s and $A_i = (J_i, I_i)$, then the set of E_s-predecessors (E_s-successors) among $c_1, \ldots, c_n$ of c_{ij} is $\{c_j : j \in J_i\}$ ($\{c_j : j \in I_i\}$). In other words, the same type A_i is assigned to all the elements of the form c_{ij}. The E_s-predecessors of c_{00} and c_{0m} are the E-predecessors of s, and the E_s-successors of c_{01} are the E-successors of s. Furthermore, all the connections between elements forced by the tiedness relation between types are added in agreement with the total ordering $<_s$, which is obtained from $<$ by replacing s with all the elements in C_{k_m} in their lexicographical ordering. Finally, if $v > 0$ then the pairs in the set $\{(c_{k-1,0}, c_{2p,m-1}) : 0 < p < u\}$ are added to E_s. As in the proof of Lemma 3.1 of [1], one verifies that E_s is contained in $<_s$ so that it is well-founded. Furthermore, if a and b are indiscernible in $\mathcal{M}_0\{s/k^-_m(A_0, \ldots, A_{k-1})\}$ then at least one among a and b is free-enough in $\mathcal{M}$. For two distinct elements of the k^-_m-*curl* are easily seen to be E_s-discernible, so that if a and b is a pair of E_s-indiscernible elements, then one, at least, among a and b, say a, belongs to $M_0 \setminus \{s\}$. If also $b \in M_0 \setminus \{s\}$, then a and b were already E-indiscernible in M_0, so that one at least among a and b is free enough. On the other hand, if $b \in C_{k_m}$, then either $b = c_{00}$ or $b = c_{0m}$, as we are going to show. If $\upsilon > 0$, then a is E_s-discernible from all the elements in the k_m^--*curl* different from c_{00}. In fact for any such element, say c, of type A_{i+1} (A_0), in the k_m^--*curl*, there are elements of type A_i (A_{k-1}) which are E_s-related to c and others which are not E_s-related to c. Furthermore, no element in the k_m^--*curl* has c_{01} as its unique E_s-predecessor in the k_m^--*curl*. On the other hand, if A_i is tied with $\tau(a)$ and $s < a$, then all of the elements of type A_i in the k_m^--*curl* are E_s-related to a; otherwise, none of them is E_s-related to a, with the only possible exception of c_{01}. That ensures, as it is easy to verify, that in the k_m^--*curl* there is an E_s-witness of the difference between a and c. If $\upsilon = 0$, then the same argument applies except for $c = c_{0m}$, since all the elements of type A_{k-1} in the k_m^--*curl* are E-related to c_{0m}. Since the E_s-predecessors of a in $M_0 \setminus \{s\}$ are the same as the E-predecessors of a in $M_0 \setminus \{s\}$, and the E_s-predecessors of c_{00} and of c_{0m} in $M_0 \setminus \{s\}$ are the same as the E-predecessors of s in $M_0 \setminus \{s\}$, it is clear that if a and c_{00} or a and c_{0m} are E_s-indiscernible then a and s are E-indiscernible. That entails that in any case a is free enough, since s, being the minimum of the elements of its own type, cannot be free-enough.

The operation which leads from $\mathcal{M}_0$ to $\mathcal{M}_0\{s/k_m^-(A_0, \ldots, A_{k-1})\}$ can be iterated, after a renaming of the elements which have been added, until all the $\text{maxmin}_<^{\mathcal{M}}$ of some free or tied cycle in $\mathcal{G}$, which strictly covers its $\text{maxmin}_<^{\mathcal{M}}$, are replaced. Let $\mathcal{M}'_0 = (M'_0, E')$ be the well-founded structure and $<'$ be the total ordering which extends E', which are obtained in that way. Since each k_m^--*curl* has cardinality pr. ric. bounded with respect to t, and at most t of them are added in the transition from $\mathcal{M}_0$ to $\mathcal{M}'_0$, $|M'_0|$ is also pr. ric. bounded with respect to t, hence with respect to n. Furthermore, if a and b in M'_0 are E'-indiscernible, then either a or b belongs to M_0 and is free enough in $\mathcal{M}$.

We are going to show that through the addition of less than t new elements $\mathcal{M}'_0$ can be modified into a well-founded $\mathcal{G}$-structure which has fewer pairs of indiscernible elements than $\mathcal{M}'_0$. It will then suffice to repeat such transformation a pr. ric. bounded (with respect to n) number of times in order to obtain an extensional well-founded $\mathcal{G}$-structure of bounded cardinality.

Assume $a \in M_0$ is free enough and is E'-indiscernible from b in $\mathcal{M}'_0$. We have already noted that b is not an internal point of any of the k_m^--*curl*s that have been added to obtain $\mathcal{M}'_0$; thus we have only to take care of the case in which $b \in M_0 \cup \{c_{00}, c_{0m}\}$ where c_{00}, c_{0m} denote the first and last point (with respect to $<'$) of some of the added k_m^--*curl*s.

Case 1 a is free-enough by Condition 2. Let $s = \text{maxmin}_<^{\mathcal{M}}(B_0, \ldots, B_{l-1})$ where $(B_0, \ldots, B_{l-1})$ is the free cycle of $\mathcal{G}$ which witnesses the free-enoughness of a. At a certain stage in the construction, which leads from $\mathcal{M}_0$ to $\mathcal{M}'_0$, s is replaced by a $k_m^-(A_0, \ldots, A_{k-1})$-*curl*, for appropriate m and sequence of types $A_0 \ldots, A_{k-1}$, which contains the subsequence $\beta = B_{i_0}, \ldots, B_{l-1}, B_0, \ldots, B_{i_0-1}$, where $B_{i_0} = \tau(s)$. Assume $\tau(a) = A_i$ with A_i in β. If $i = 0$, we add to E' the pair $(c_{k-1,1}, a)$; if $i = 1$, we add to E' (c_{02}, a); finally, if $1 < i = j + 1$, we add to E' (c_{j1}, a). Since the type of $c_{k-1,1}$ (c_{02} or c_{j1}) is a free differentiating type of $\tau(a)$, the resulting structure is still a $\mathcal{G}$-structure, and furthermore, since no element has $c_{k-1,1}$

(c_{02} or c_{j1}), with $0 < j$, as its unique E'-predecessor in the $k_m^-(A_0, \ldots, A_{k-1})$-*curl*, it is extensional on a.

Case 2 a is free-enough by Condition 3. Let $a_1, \ldots, a_h, b_0 \in M$ be such that $b_0 < a_h < \cdots < a_1 < a$; $\tau(a_1)$ is a free differentiating type of $\tau(a)$; $\tau(a_{i+1})$ is a free differentiating type of $\tau(a_i)$; $\tau(b_0)$ is a free differentiating type of $\tau(a_h)$ and b_0 is free enough by Condition 1 or by Condition 2. Say b_0 is free enough by Condition 2 and let $(B_0, \ldots, B_{l-1})$ be the free cycle in $\mathcal{G}$ which witnesses the free-enoughness of b_0 and $s = \mathrm{maxmin}_<^{\mathcal{M}}(B_0, \ldots, B_{l-1})$. As in the previous case, in building $\mathcal{M}_0'$, s is replaced by a $k_m^-(A_0, \ldots, A_{k-1})$-*curl*, for appropriate m and sequence of types $A_0, \ldots, A_{k-1}$, which contains the subsequence $\beta = B_{i_0}, \ldots, B_{l-1}, B_0, \ldots, B_{i_0-1}$, where $B_{i_0} = \tau(s)$. Let $\tau(b_0) = A_i$, where A_i belongs to the subsequence β. If $0 < h$, then we add h new elements $a_1', \ldots, a_h'$ to the structure. Then we add the pairs needed to give the types $\tau(a_1), \ldots, \tau(a_h)$ to $a_1', \ldots, a_h'$, respectively, as well as the pairs in the following sets:

$$\{(a_1', c) : c \neq a, (a_1, c) \in E'\} \cup \{(a_1', a) : (a_1, a) \notin E'\},$$

$$\{(a_{i+1}', c) : c \neq a_i, (a_{i+1}, c) \in E'\} \cup \{(a_{i+1}', a_i) : (a_{i+1}, a_i) \notin E'\},$$

$$\{(a_{i+1}, a_i') : (a_{i+1}, a_i) \notin E'\} \cup \{(a_{i+1}', a_i') : (a_{i+1}, a_i) \in E'\},$$

for $1 \leq i < h$. Furthermore, if $i \neq 0$ we add to E' the pairs (c_{i1}, a_h), (c_{i2}, a_h'), whereas if $i = 0$ we add the pairs (c_{02}, a_h) and (c_{03}, a_h'). Since, clearly, the types $\tau(a), \tau(a_1), \ldots, \tau(a_h), \tau(b_0)$ can be assumed to be distinct, the number of added elements is less than τ. As is easy to check, either a_1 or a_1' witnesses the difference between a and any other element in the structure and either a_{i+1} or a_{i+1}' witnesses the difference between both a_i and a_i' and any other element. Furthermore, for $i \neq 0$, since no element except a_h (a_h') has c_{i1} (c_{i2}) as its unique E'-predecessor in the $k_m^-(A_0, \ldots, A_{k-1})$-*curl*, the structure so obtained is extensional on a_h and a_h', a conclusion that holds, for a similar reason, also in the case $i = 0$. Thus that structure is extensional on $\{a, a_1, a_1', \ldots a_h, a_h'\}$. In particular, a and b are discernible and no new pair of indiscernible elements is introduced. The ordering $<'$ of M is extended by letting a_i' be the immediate $<'$ successor of a_i.

The cases in which $h = 0$ or b_0 is free enough by Condition 1 are similar.

Case 3 a is free enough by Condition 1 but not by Condition 2 or Condition 3, so that Case 1 and Case 2 above do not apply. Let $s = \mathrm{maxmin}_<^{\mathcal{M}}(B_0, B_1)$, where $B_0 = \tau(a)$ and (B_0, B_1) is the tied cycle which witnesses the free-enoughness of a. Since (M, E) is extensional, in M there is an element, say d, which E-witness the difference between a and b. Since a and b are E'-indiscernible in $\mathcal{M}_0'$, $d \notin M_0$, so that d is free-enough. Let γ be the cycle which witnesses the free-enoughness of d and $s' = \mathrm{maxmin}_<^{\mathcal{M}}(\gamma)$. s' is one of the elements which in the transition from $\mathcal{M}_0$ to $\mathcal{M}_0'$ is replaced, say by a $k_{m'}^-(A_0', \ldots, A_{k'-1}')$-*curl* for appropriate m' and sequence of types $A_0', \ldots, A_{k'-1}'$ which contains a subsequence γ' corresponding to γ. Let $\tau(d) = A_i'$ with A_i' in γ'.

Case 3.1 $b <' a$. If $(d, b) \in E$ and $(d, a) \notin E$, c_{i1}, if $i \neq 0$, or c_{i2}, if $i = 0$, is not E'-related to a, since $\tau(c_{i1}) = \tau(d)$, if $i \neq 0$, or $\tau(c_{02}) = \tau(d)$, if $i = 0$, and $\tau(d)$ is not tied with $\tau(a)$. Therefore, c_{i1}, if $i \neq 0$, or c_{02}, if $i = 0$, is not E'-related to b either. Thus it suffices to add the pair (c_{i1}, b) to E', if $i \neq 0$, or (c_{02}, b), if $i = 0$, to obtain a $\mathcal{G}$-structure in which c_{i1} or c_{02} witnesses the difference between a and b. If, on the other hand, $(d, a) \in E$ and $(d, b) \notin E$, we distinguish two subcases.

Case 3.1.1 $\tau(d)$ is a free differentiating type of $\tau(a)$. An argument similar to the previous one shows that it suffices to add the pair (c_{i1}, a), if $i \neq 0$, or (c_{02}, b), if $i = 0$, to E'.

Case 3.1.2 $\tau(d)$ is tied with $\tau(a)$. We show that it suffices to add d to M' and extend E' by adding all the pairs in $E \cap (M'_0 \cup \{d\})^2$ which contain d, as well as those which such an enrichment forces to be present by the tiedness relation between types. Let E'' be the relation thus obtained. Obviously, the resulting structure is a $\mathcal{G}$-structure and d E''-witnesses the difference between a and b. It remains to be shown that no pair of E''-indiscernible elements is added, namely, that E'' is extensional on d in $M' \cup \{d\}$. From the assumption that $\tau(d)$ is tied with $\tau(a)$ it follows that all the elements of type $\tau(d) = A'_i$ in the $k^-_{m'}(A'_0, \ldots, A'_{k'-1})$-*curl* are E'-related to a, so that, by the E'-indiscernibility of a and b, they are E'-related to b as well. But that can happen only if $\tau(d)$ is tied with $\tau(b)$. Since $(d, b) \notin E$, it follows that $(b, d) \in E''$. Let $s'' = \text{maxmin}(\tau(d), \tau(a))$. $(\tau(d), \tau(a))$ strictly covers s''. For obviously $s'' \leq a$. Furthermore, $s'' \neq a$. Otherwise, a would be the minimum of the elements of its own type and then the maximum of its E-predecessors, which is in the structure from the very beginning, would witness the difference between a and b, against the assumption. Furthermore, the maximum of the elements of type $\tau(d)$, which is also in the structure from the beginning, is greater than a, since, otherwise, it would witness the difference between a and b. Therefore, in the transition from $\mathcal{M}_0$ to $\mathcal{M}'_0$, s'' is one of the elements which are replaced. Say s'' is replaced by a $k^-_{m''}(A''_0, \ldots, A''_{k''-1})$-*curl* for appropriate m'' and types $A''_0, \ldots, A''_{k''-1}$, among which there are $\tau(d)$ and $\tau(a)$. Assume by way of contradiction that d' is E''-indiscernible from d. All the elements of type $\tau(a)$ in the $k^-_{m''}(A''_0, \ldots, A''_{k''-1})$-*curl*, which replaces s'', by the tiedness of $\tau(a)$ and $\tau(d)$, are E''-related to d; hence they are also E''-related to d'. But that can happen only if $\tau(a)$ is tied with $\tau(d')$. As a consequence either d' is E'-related to a or a is E'-related to d'. In the former case d' would witness the difference between b and a, against their E'-indiscernibility. In the latter case, a would witness the difference between d' and d, against the assumption that d' and d are E''-indiscernible.

Case 3.2 $a < b$. b cannot be one of the constants $c_1, \ldots, c_n$ since otherwise the maximum of the predecessors of c_i, which is in the structure, would witness that b is different from a. Then essentially the same argument of Case 3.2 applies by letting $s'' = \text{maxmin}(\tau(d), \tau(b))$.

The process by which the E'-indiscernibility between a and b, with a free-enough, has been eliminated can be iterated, thanks to the large enough number, namely, $m = 1+2 \cdot p$, of elements c_{ij} having the same type, say A_i, which are present in each $k^-_m(A_0, \ldots, A_{k-1})$-*curl* introduced in the transition from $\mathcal{M}_0$ to $\mathcal{M}'_0$. For example, having dealt with a as above, suppose (a', b') is another pair of E'-indiscernible elements and that a' is free-enough by Condition 2. Furthermore, assume that such a free-enoughness is witnessed by the same cycle β which witnesses the free-enougness of a. If $\tau(a) = A_{i'}$ and $\tau(a') \neq \tau(a)$ we can proceed exactly as in Case 2 above. On the other hand, if $\tau(a') = \tau(a) = A_i$ then, if $i \neq 0$, instead of the pairs (c_{i1}, a_h) and (c_{i2}, a'_h) we add pairs having c_{i3} and c_{i4} as their first components. If, on the other hand, $i = 0$, then, instead of the pairs (c_{02}, a_h) and (c_{03}, a'_h), we add pairs having c_{04} and c_{05} as their first components.

Clearly, the number of times the process we have described must be repeated, before no pair of indiscernible elements is left, is pr. ric. bounded with respect to n. As a consequence the cardinality of the extensional $\mathcal{G}$-structure thus obtained is also pr. ric. bounded with respect to n. □

3.1 Completeness As shown in [1] from the proof of decidability of $\exists^*\forall\forall$-sentences in **V** one can infer the completeness of ZF with respect to such sentences. Due to the existence of $\exists\exists\forall\forall$-sentences which are true in **V** but not in **HF** ([4]), ZF−Inf, where Inf denotes the Infinity Axiom, which states the existence of the set of the natural numbers, fails to be complete with respect to such 4-quantifier sentences. Completeness with respect to $\exists^*\forall\forall$-sentences is restored if we add the negation ¬Inf of the Infinity Axiom to ZF−Inf. In fact, given an $\exists^*\forall\forall$-sentence $\exists x_1 \dots \exists x_n \forall x \forall y F$, if it is true in **HF**, then there is a finite structure (actuallly a hereditarily finite one) which ZF−Inf can detect to have the property required to ensure the satisfiability of $\forall\forall F$ in **HF**, by hereditarly finite sets $a_1, \dots, a_n$. Since $a_1, \dots, a_n$ satisfy $\forall x \forall y F$ in **HF** if and only if they satisfy it in **V**, ZF−Inf can conclude that $\exists x_1 \dots \exists x_n \forall x \forall y F$. On the other hand, if ZF−Inf verifies that there is no finite structure, among the finitely many that need to be inspected, that has the property required to ensure the satisfiability of $\forall\forall F$ in **HF**, then it can conclude that if $\exists x_1 \dots x_n \forall x \forall y F$ then some of the $x_1, \dots, x_n$ is not hereditarily finite. Therefore, the transitive closure of $\{x_1, \dots, x_n\}$ contains a set which is not equinumerous to any natural number. By a well-known argument going back to [5] (see [3], Ch. III), the existence of such a set entails Inf in ZF−Inf. Therefore, in ZF−Inf + ¬Inf we obtain a contradiction, so that ZF−Inf + ¬Inf derives $\neg\exists x_1 \dots \exists x_n \forall x \forall y F$. Thus ZF and ZF−Inf + ¬Inf are both complete with respect to $\exists^*\forall\forall$-sentences. [2] conjectures that ZF is complete with respect to all 4-quantifier sentences. In light of the above results, it seems of interest to consider that conjecture also in the case of the theory ZF−Inf + ¬Inf.

References

[1] Bellé, D., and F. Parlamento, "Truth in **V** for $\exists^*\forall\forall$-sentences is decidable," *The Journal of Symbolic Logic*, vol. 71 (2006), pp. 1200–1222. Zbl 1109.03057. MR 2275856. 55, 56, 57, 58, 59, 63

[2] Friedman, H. M., "Three-quantifier sentences," *Fundamenta Mathematicae*, vol. 177 (2003), pp. 213–40. Zbl 1020.03044. MR 1992241. 55, 63

[3] Lévy, A., *Basic Set Theory*, Springer-Verlag, Berlin, 1979. Zbl 0404.04001. MR 533962. 63

[4] Parlamento, F., and A. Policriti, "Note on: 'The logically simplest form of the infinity axiom' " (Proceedings of the American Mathematical Society, vol. 103 (1988), pp. 274–76), *Proceedings of the American Mathematical Society*, vol. 108 (1990), pp. 285–86. Zbl 0694.03031. MR 993751. 63

[5] Tarski, A., "Sur les ensembles finis," *Fundamenta Mathematicae*, vol. 6 (1924), pp. 45–95. Zbl 50.0135.02. 63

Acknowledgments

This work has been supported by funds PRIN2004-MIUR. The authors are grateful to the referee for helpful comments and suggestions.

Department of Mathematics and Computer Science
University of Udine
via Delle Scienze 206
33100 Udine
ITALY
dorella.belle@dimi.uniud.it
franco.parlamento@dimi.uniud.it