

EQUATIONAL BOOLEAN RELATION THEORY

by

Harvey M. Friedman

Ohio State University

friedman@math.ohio-state.edu

<http://www.math.ohio-state.edu/~friedman/>

9/03/02

NOTE: THIS IS ONLY THE FIRST THREE SECTIONS, WHICH CONTAINS THE PROOF FROM LARGE CARDINALS.

Abstract. Equational Boolean Relation Theory concerns the Boolean equations between sets and their forward images under multivariate functions. We study a particular instance of equational BRT involving two multivariate functions on the natural numbers and three infinite sets of natural numbers. We prove this instance from certain large cardinal axioms going far beyond the usual axioms of mathematics as formalized by ZFC. We show that this particular instance cannot be proved in ZFC, even with the addition of slightly weaker large cardinal axioms, assuming the latter are consistent.

1. EQUATIONAL BOOLEAN RELATION THEORY.

Equational Boolean Relation Theory (equational BRT) concerns the Boolean equations between sets and their images under multivariate functions. We formally present equational BRT in this section.

To be fully rigorous, we need to distinguish, say, a function of two variables from A into A and a function of one variable from A^2 into A . For this reason, we use the following definition of multivariate function.

A multivariate function is a pair $f = (g, k)$, where $k \geq 1$ (the arity of f) and $\text{dom}(g)$ is a set of ordered k -tuples. We put no other restrictions on g .

We define $\text{dom}(f)$ to be $\text{dom}(g)$, and write $f(x_1, \dots, x_k) = g(\langle x_1, \dots, x_k \rangle)$, where $\langle x_1, \dots, x_k \rangle$ is the ordered k -tuple with coordinates shown. In practice, we need not be so careful about multivariate functions.

Equational BRT is based on the following crucial notion of forward image. Let f be a multivariate function and A be a set. We define

$$fA = \{f(x_1, \dots, x_k) : k \text{ is the arity of } f \text{ and } x_1, \dots, x_k \in A\}.$$

We could write $f[A^k]$ for this forward image construction, but it is particularly convenient to suppress the arity and write fA . In this way, f defines a special kind of operator from sets to sets.

A BRT setting is a pair (V, K) , where V is a set of multivariate functions and K is a set of sets. Typically, V and K are naturally related so that one is interested in the forward images of elements of V on elements of K , although in equational BRT, no restrictions are placed on the choice of V, K .

We use N for the set of all nonnegative integers. We say that f is a multivariate function from A into B if and only if f is a multivariate function with $\text{dom}(f) = A^k$ and $\text{rng}(f) \subseteq B$, where the arity of f is k .

We use $MF(A, B)$ for the set of all multivariate functions from A into B , and $MF(A)$ for the set of all multivariate functions from A into A .

We use $S(A)$ for the set of all subsets of A , and $INF(A)$ for the set of all infinite subsets of A .

We say that $f \in MF(N)$ is strictly dominating if and only if

$$\text{for all } x \in \text{dom}(f), f(x) > \max(x).$$

Here $\max(x)$ is the maximum coordinate of x . We use $SD(N)$ for the set of all strictly dominating elements of $MF(N)$.

Here are two examples of statements in equational BRT in the BRT setting $(SD(N), INF(N))$.

1. For all $f \in SD(N)$ there exists $A \in INF(N)$ such that $fA = N \setminus A$.
2. For all $f, g \in SD(N)$ there exists $A, B, C \in INF(N)$ such that $C \subseteq fA = C \subseteq gB = fA \cap gB = \emptyset$.

Statement 1 is called the Complementation Theorem, and we give a proof of it at the end of this section. We leave the proof of statement 2 to the reader.

Note that the first example involves only one function and one set, and is therefore a particularly simple instance of equational BRT (see [Fr01]).

Note that the second example involves two functions and three sets, and is therefore more involved. The particular instance which is the subject of this paper (Proposition A) involves two functions and three sets.

We now give a formal presentation of equational BRT. In equational BRT, we use set variables A_1, A_2, \dots , and function variables f_1, f_2, \dots .

The BRT atoms consist of $\emptyset, U, A_i, f_i A_j$, where $i, j \geq 1$. Here U is for "universal".

BRT terms are defined inductively by

- i) every BRT atom is a BRT term;
- ii) if s, t are BRT terms then so are $s \sqcup t, s \sqcap t, s'$.

The BRT equations are of the form $s = t$, where s, t are BRT terms.

An equational BRT statement is a statement of the form:

for all $f_1, \dots, f_n \in V$, there exists $A_1, \dots, A_m \in K$,
such that a given BRT equation holds among
the sets and their images under the functions.

More formally, an equational BRT statement is a statement of the form:

for all $f_1, \dots, f_n \in V$, there exists $A_1, \dots, A_m \in K$,
such that a given BRT equation holds, where we require
that in the given BRT equation, all BRT atoms
that appear are among the $m(n+1)$ BRT atoms

$$A_1, \dots, A_m$$

$$f_1 A_1, \dots, f_1 A_m$$

$$\dots$$

$$f_n A_1, \dots, f_n A_m.$$

These statements are what we call the statements in equational BRT of type (n,m) ; i.e., with n functions and m sets. In equational BRT of type (n,m) , there are $m+nm = m(n+1)$ BRT atoms, and consequently $2^{m(n+1)}$ BRT terms up to Boolean equivalence. Since every BRT equation can be put into the form $t = \emptyset$, we see that there are $2^{m(n+1)}$ statements in equational BRT of type (n,m) up to Boolean equivalence.

An equational BRT statement becomes an actual statement when the BRT setting (V,K) is specified. We follow the convention that the interpretation of U is the union of the elements of K , and take s' to abbreviate $U \setminus s$.

It is very awkward to look at actual BRT equations. Normally, a complicated BRT equation is broken up into a finite conjunction of simple BRT equations, where these simple Boolean equations are typically written as yet simpler inclusions.

More systematically, a basic inclusion is an inclusion of the form

$$y_1 \sqcap \dots \sqcap y_p \sqcap z_1 \sqcap \dots \sqcap z_q$$

where $p, q \geq 0$, and $y_1, \dots, y_p, z_1, \dots, z_q$ are distinct BRT atoms.

If $p = 0$ and $q > 0$ then we write this basic inclusion as

$$z_1 \sqcap \dots \sqcap z_q = U.$$

If $q = 0$ and $p > 0$ then we write this basic inclusion as

$$y_1 \sqcap \dots \sqcap y_p = \emptyset.$$

If $p = q = 0$ then we write this basic inclusion as

$$U = \emptyset.$$

In fact, by simple Boolean algebra manipulations (or disjunctive normal form in propositional calculus), we see that the BRT equations can be put in the form of a conjunction of basic inclusions. Also, every conjunction of basic inclusions is equivalent to a BRT equation.

In this paper, we focus on a particular statement in equational BRT of type $(2,3)$ that is independent of ZFC.

Let $f \in MF(N)$. We say that f is of expansive linear growth if and only if there exist $c, d > 1$ such that for all but finitely many $x \in \text{dom}(f)$,

$$c|x| \leq f(x) \leq d|x|$$

where $|x|$ is the maximum coordinate of the tuple x .

Let $ELG(N)$ be the set of all $f \in MF(N)$ of expansive linear growth. We focus on the following particular statement in equational BRT of type $(2,3)$ on the BRT setting $(ELG(N), INF(N))$.

We use $X \dot{\perp} Y$ for $X \perp Y$ together with the commitment that X, Y are disjoint. For example,

$$X \dot{\perp} Y \dot{\perp} Z \dot{\perp} W$$

means

$$X \dot{\perp} Y \dot{\perp} Z \dot{\perp} W \dot{\perp} X \dot{\perp} Y = \emptyset \dot{\perp} Z \dot{\perp} W = \emptyset.$$

PROPOSITION A. For all $f, g \in ELG(N)$ there exist $A, B, C \in INF(N)$ such that

$$\begin{aligned} A \dot{\perp} fA \dot{\perp} C \dot{\perp} gB \\ A \dot{\perp} fB \dot{\perp} C \dot{\perp} gC. \end{aligned}$$

In section 3, we use large cardinals in an essential way in order to prove Proposition A. The large cardinals involved are (strongly) Mahlo cardinals of finite order. These are defined inductively on the natural number n as follows.

A cardinal κ is 0-Mahlo if and only if κ is strongly inaccessible.

A cardinal κ is $(n+1)$ -Mahlo if and only if it is n -Mahlo and every closed and unbounded subset of κ has an element that is n -Mahlo.

Let $MAH = ZFC + \{\text{there exists an } n\text{-Mahlo cardinal}\}_n$. Let $MAH^+ = ZFC + \text{"for all } n \text{ there exists an } n\text{-Mahlo cardinal"}$.

In section 3 we prove Proposition A in MAH^+ . In sections 4-?, we show that Proposition A is not provable in MAH , assuming

MAH is consistent. In fact, we show that Proposition A is not provable in any consistent subsystem of MAH.

It is clear that Proposition A is (equivalent in Boolean algebra to) a statement in equational BRT of type (2,3) on $(\text{ELG}(\mathbb{N}), \text{INF}(\mathbb{N}))$.

The number of statements in equational BRT of type (2,3) is $2^{2^{3(2+1)}} = 2^{512}$, up to Boolean equivalence.

CONJECTURE. Every statement in equational BRT of type (2,3) on $(\text{ELG}(\mathbb{N}), \text{INF}(\mathbb{N}))$ is provable or refutable in MAH+.

We know that this conjecture is false if we replace MAH+ by MAH, assuming MAH is consistent, since Proposition A is a statement in equational BRT of type (2,3) on $(\text{ELG}(\mathbb{N}), \text{INF}(\mathbb{N}))$.

It is clear that Proposition A has a particularly simple structure compared to a typical statement in equational BRT of type (2,3). In fact, the two clauses in Proposition A have the form

$$\begin{aligned} X \square . fY \square Z \square . gW \\ S \square . fT \square U \square . gV \end{aligned}$$

where X, Y, Z, W, S, T, U, V are among the three letters A, B, C . This amounts to a particular set of instances of equational BRT of type (2,3) on $(\text{ELG}(\mathbb{N}), \text{INF}(\mathbb{N}))$ of cardinality $3^8 = 6561$.

We have been able to show that all of these 6561 statements are provable or refutable in MAH+. The proof will appear elsewhere (see [Fr??]).

We now prove the Complementation Theorem as promised.

COMPLEMENTATION. For all $f \square \text{SD}(\mathbb{N})$ there exists $A \square \text{INF}(\mathbb{N})$ such that $fA = \mathbb{N} \setminus A$. For all $f \square \text{SD}(\mathbb{N})$ there exists a unique $A \square \mathbb{N}$ such that $fA = \mathbb{N} \setminus A$.

Proof: Let $f \square \text{SD}(\mathbb{N})$ have arity k . For existence, we construct A inductively. We define sets $A_n \square [0, n)$, $n \geq 0$, and take $A = \bigcup \{A_n : n \geq 0\}$. Define $A_0 = \emptyset$. Suppose A_n has been defined. Define $A_{n+1} = A_n$ if $n \square fA_n$; $A_n \cup \{n\}$ if $n \square fA_n$.

We first claim that for all $n \square A$, we have $n \square A_{n+1}$. To see this, let $n \square A_m$. Clearly $m > n$. If $m = n+1$ then $n \square A_{n+1}$. So

assume $m > n+1$. If $n \in A_{n+1}$ then by induction, $n \in A_m$. Hence $n \in A_{n+1}$.

We secondly claim that $fA = \bigcap \{fA_n : n \geq 0\}$. To see this, let $n \in fA$. Let $n = f(m_1, \dots, m_k)$, $m_1, \dots, m_k \in A$. Since f is strictly dominating, $m_1, \dots, m_k < n$. Hence by the first claim, $m_1, \dots, m_k \in A_n$, and so $n \in fA_n$.

Now suppose $n \in A$. By the first claim, $n \in A_{n+1}$, and so $n \in fA_n$. By the second claim, $n \in fA$. Now suppose $n \in A$. Then $n \in A_{n+1}$, and so $n \in fA_n$. Therefore $n \in fA$.

We have shown that for all n , $n \in A \iff n \in fA$. Therefore $fA = N \setminus A$.

For uniqueness, let $A, B \in N$, $fA = N \setminus A = fB$. Let n be least such that $n \in A \iff n \in B$. Then $n \in fA \iff n \in fB$. Since f is strictly dominating, this violates the choice of n . QED

The Complementation Theorem is an instance of equational BRT of type (1,1) on $(SD(N), INF(N))$. There are 16 such instances. It is not difficult to determine the truth value of each of these instances, the only nontrivial case being the Complementation Theorem. See [Fr01] for such determinations on several BRT settings.

2. SOME SET THEORETIC PRELIMINARIES.

Let $[A]^n$ be the set of all n element subsets of A . Let A be a set of ordinals. We say that $f: [A]^n \rightarrow \text{On}$ is regressive if and only if for all $x \in [A]^n$ with $\min(x) > 0$, $f(x) < \min(x)$.

We will not attempt to minimize the level of Mahloness needed for the results of this section. This simplifies the arguments.

LEMMA 2.1. Let $n \geq 0$, κ be n -Mahlo, $A \in \kappa$ unbounded, and $f: [A]^{n+2} \rightarrow \kappa$ be regressive. For all $\alpha < \kappa$, there exists $E \in A$ of order type α such that for all $x, y \in [E]^n$, $\min(x) = \min(y) \implies f(x) = f(y)$.

Proof: See [HKS87], p. 147. The result originally appeared in [Sc74] using different notation. QED

We will use a function F with domain \mathbb{Q} such that for all $\alpha \geq \beta$, $F(\alpha)$ is a one-one mapping from the set of all finite sequences from \mathbb{Q} , into $\mathbb{Q} \setminus \{0\}$.

LEMMA 2.2. Let $n, m \geq 1$, \mathbb{Q} be $2n$ -Mahlo, $A \subseteq \mathbb{Q}$ unbounded, and $f: [A]^n \times \mathbb{Q}^m \rightarrow \mathbb{Q}$. Assume that for all $x \in [A]^n$ and $z \in \mathbb{Q}^m$, $f(x, z) < \min(x)$. There exists $E \subseteq A \setminus \mathbb{Q}$ of order type \mathbb{Q} such that for all $x, y \in [E]^n$ and $z \in \mathbb{Q}^m$, if $\max(z) < \min(x) = \min(y)$ then $f(x, z) = f(y, z)$.

Proof: Let n, m, \mathbb{Q}, A, f be as given. Define $g: [A]^{2n-1} \rightarrow \mathbb{Q}$ as follows. Let $x = \{x_1 < \dots < x_{2n-1}\} \in A$ be given.

case 1. $x_1 \geq \mathbb{Q}$ and there exists $z \in \mathbb{Q}^m$ such that $\max(z) < x_1$ and $f(\{x_1, \dots, x_n\}, z) \neq f(\{x_1, x_{n+1}, \dots, x_{2n-1}\}, z)$. Choose z to be lexicographically least. Define $g(x) = F(x_1)(z, f(\{x_1, \dots, x_n\}, z))$.

case 2. Otherwise. Define $g(x) = 0$.

Apply Lemma 2.1 to g . Let $E' \subseteq A$ be of order type $\mathbb{Q} + \mathbb{Q}$ such that for all $x, y \in [E']^n$, $\min(x) = \min(y) \implies g(x) = g(y)$. Let E be the result of chopping off the first \mathbb{Q} elements of E' .

Suppose case 1 applies to $x \in [A]^{2n-1}$. Then g is nonzero at any $y \in [A]^{2n-1}$ such that $\min(x) = \min(y)$. Hence case 1 applies to all $y \in [A]^{2n-1}$, $\min(x) = \min(y)$. In particular, let $y = \{x_1 < x_{n+1} < \dots < x_{2n-1} < y_1 < \dots < y_{n-1}\} \in A$. Then $g(x) = g(y)$, and so $F(x_1)(z, f(\{x_1, \dots, x_n\})) = F(x_1)(z', f(\{x_1, x_{n+1}, \dots, x_{2n-1}\}))$, where z, z' are as in case 1 for $g(x), g(y)$, respectively. Hence $z = z'$ and $f(\{x_1, \dots, x_n\}) = f(\{x_1, x_{n+1}, \dots, x_{2n-1}\})$. This is a contradiction.

We have shown that case 1 does not apply to any $x \in [A]^{2n-1}$. Since $E \subseteq A \setminus \mathbb{Q}$ is of order type \mathbb{Q} , we are done. QED

LEMMA 2.3. Let $n, m \geq 1$, \mathbb{Q} be $2n$ -Mahlo, $A \subseteq \mathbb{Q}$ unbounded, and for all $i \geq 0$, $f_i: [A]^n \times \mathbb{Q}^m \rightarrow \mathbb{Q}$. Assume that for all $i \geq 0$, $x \in [A]^n$ and $z \in \mathbb{Q}^m$, $f_i(x, z) < \min(x)$. There exists $E \subseteq A \setminus \mathbb{Q}$ of order type \mathbb{Q} such that for all $x, y \in [E]^n$ and $z \in \mathbb{Q}^m$, if $\max(z) < \min(x) = \min(y)$ then $f_i(x, z) = f_i(y, z)$.

Proof: Let n, m, \mathbb{Q}, A, f_i be as given. Let $f: [A]^n \times \mathbb{Q}^{m+1} \rightarrow \mathbb{Q}$ be defined as follows. Let $x \in [A]^n$, $y \in \mathbb{Q}^m$. Define $f(x, y, i) = f_i(x, y)$ if $i \in \mathbb{Q}$; 0 otherwise. Apply Lemma 2.2 to f . QED

LEMMA 2.4. Let $n \geq 1$, \square be $2n$ -Mahlo, $A \square \square$ unbounded, and for all $i \geq 0$, $f_i: [A]^n \square \square$. There exists $E \square A \setminus \square$ of order type \square such that for all $x, y \square [A]^n$, if $x \square \min(E \setminus f(x)) + 1 = y \square \min(E \setminus f(x)) + 1$ then $f_i(x) = f_i(y)$.

Proof: Let n, \square, A, f_i be as given. We define $g_i: [A]^n \cdot \square^n \square \square$ as follows. Let $x \square [A]^n$, $z \square \square^n$. Write $x = \{x_1 < \dots < x_n\}$, $z = (z_1, \dots, z_n)$. Let j be greatest such that $z_1 < \dots < z_j < x_1$. Define $g(x, z) = 1 + f_i(\{z_1, \dots, z_j, x_1, \dots, x_{n-i}\})$ if $f_i(\{z_1, \dots, z_j, x_1, \dots, x_{n-i}\}) < x_1$; 0 otherwise. Let $E \square A \setminus \square$ be of order type \square , where for all $x, y \square E[n]$, $z \square \square^n$, if $\max(z) < \min(x) = \min(y)$, we have $g_i(x) = g_i(y)$.

Let $x, y \square [A]^n$, $x \square \min(E \setminus f_i(x)) + 1 = y \square \min(E \setminus f_i(x)) + 1$. Let $x = \{x_1 < \dots < x_n\}$, $y = \{y_1 < \dots < y_n\}$. Let $x_1 < \dots < x_j$ be the elements of $x \square \min(E \setminus f_i(x)) + 1$. If $f_i(x) \geq x_{j+1}$ then $\min(E \setminus f_i(x)) \geq x_{j+1}$, and so $x_{j+1} \square x \square \min(E \setminus f_i(x)) + 1$, which is impossible. Hence $i = n$ or $f_i(x) < x_{j+1}$.

It suffices to show that $f_i(x) = f_i(y)$. Suppose $j = n$. Then $x = x \square \min(E \setminus f_i(x)) + 1 = y \square \min(E \setminus f_i(x)) + 1$ has cardinality n , and therefore $y \square \min(E \setminus f_i(x)) + 1 = y$. Hence $x = y$, and we are done. So we assume $f_i(x) < x_{j+1}$.

Let $x_n, y_n < u_1 < \dots < u_j$, where the u 's lie in E . Note that $g(\{x_{j+1}, \dots, x_n, u_1, \dots, u_j\}, x_1, \dots, x_j, 0, \dots, 0) = 1 + f_i(x)$. Also $g(\{y_{j+1}, \dots, y_n, u_1, \dots, u_j\}, x_1, \dots, x_j, 0, \dots, 0) = 1 + f_i(y)$ if $f_i(y) < y_{j+1}$; 0 otherwise. Since $g(\{x_{j+1}, \dots, x_n, u_1, \dots, u_j\}, x_1, \dots, x_j, 0, \dots, 0) = g(\{y_{j+1}, \dots, y_n, u_1, \dots, u_j\}, x_1, \dots, x_j, 0, \dots, 0)$, we have $g(\{y_{j+1}, \dots, y_n, u_1, \dots, u_j\}, x_1, \dots, x_j, 0, \dots, 0) = 1 + f_i(x)$. Hence $1 + f_i(x) = 1 + f_i(y)$, and so $f_i(x) = f_i(y)$. QED

We now move over to ordered n -tuples. Let x, y be n -tuples of ordinals. We write $\min(x)$ for the minimum coordinate of x . We write $\text{rng}(x)$ for the set of all coordinates of x .

LEMMA 2.5. Let $n \geq 1$, \square be $2n$ -Mahlo, $A \square \square$ unbounded, and for all $i \geq 0$, $f_i: A^n \square \square$. There exists $E \square A \setminus \square$ of order type \square such that for all $x, y \square E^n$ and $i \square \square$, if x, y have the same order type, $\text{rng}(x) \square \min(E \setminus f_i(x)) + 1 = \text{rng}(y) \square \min(E \setminus f_i(x)) + 1$, then $f_i(x) = f_i(y)$.

Proof: Let n, \square, A, f_i be as given. Each f_i gives rise to finitely many functions $f_{i1}, \dots, f_{ip}: [A]^n \square \square$, one for each order type of n -tuples. This gives a denumerable sequence of

functions for which we can apply Lemma 2.4, with one caveat. The arities of these functions are $\leq n$, rather than n . However, this is not a problem since we can pad with higher dummy arguments. QED

LEMMA 2.6. Let $n \geq 1$, E be a set of ordinals of order type α , $\beta \leq E$, and x_1, x_2, \dots be an infinite sequence of distinct elements of E^n . There is an infinite subsequence of the x 's such that any two terms have their coordinates $\leq \beta$ in precisely the same positions.

Proof: Choose an infinite subsequence whose first coordinates are either constant or greater than β . Choose an infinite subsequence of this infinite subsequence whose second coordinates are either constant or greater than β . Continue in this way n times. QED

LEMMA 2.7. Let $n \geq 0$, α be $2n$ -Mahlo, $f_1, f_2, \dots: \alpha^n \rightarrow \alpha$ be indexed by positive integers, and $g: \alpha^n \rightarrow \alpha$. There exists $E \subseteq \alpha$ of order type α such that

- i) for all $i \geq 1$, $f_i E$ is either finite or is of order type α with the same sup as E ;
- ii) gE is finite.

Proof: Let n, α, g , and the f 's be as given. Let A be the unbounded set of all $\beta < \alpha < \alpha$ such that every $f_i[\alpha^n] \subseteq \beta$. Let $E \subseteq A \setminus \alpha$ be as given by Lemma 2.5, where g and the f_i are restricted to A^n . Write $E = \{E_1 < E_2 < \dots\}$. Clearly g is constant on n -tuples from E of the same order type, and therefore ii) holds. It is clear that the sup of each $f_i E$ is at most the sup of E .

Suppose $f_i E$ is infinite. It suffices to show that for all j , $f_i E \cap E_j$ is finite. Let $x_1, x_2, \dots \in E^n$ have the same order type $\leq E_j$, where $f_i(x_1), f_i(x_2), \dots$ are distinct ordinals $< E_j$. Apply Lemma 2.6 to obtain an infinite subsequence y_1, y_2, \dots of the x 's, where any two y 's have their coordinates $\leq E_j$ in precisely the same positions, all of the same order type, and all equivalent below E_j . By the choice of E , f_i is constant on this infinite subsequence. This is a contradiction. QED

3. PROOF OF PROPOSITION A.

In this section we prove Proposition A in MAH+.

It is convenient to prove a stronger statement.

PROPOSITION B. Let $f, g \in \text{ELG}(N)$ and $n \geq 1$. There exist infinite sets $A_1 \cap \dots \cap A_n \cap N$ such that

- i) for all $1 \leq i < n$, $fA_i \cap A_{i+1} = \emptyset$, gA_{i+1} ;
- ii) $A_1 \cap fA_n = \emptyset$.

To see that B implies A, use $n = 3$ and $A = A_1$, $B = A_2$, $C = A_3$. Then $A \cap B \cap C \cap N$. By ii), A, fA are disjoint, and A, fB are disjoint. By i), C, gC are disjoint, and hence C, gB are disjoint.

For the proof of Proposition B, we fix $n \geq 1$ and $f, g \in \text{ELG}(N)$ with arities p, q respectively.

It is easy to see that we can fix an integer $b > 1$ such that for all $x \in N^p$ and $y \in N^q$, if $|x|, |y| > b$ then

$$\begin{aligned} (1 + 1/b)|x| &< f(x) < b|x| \\ (1 + 1/b)|y| &< g(y) < b|y|. \end{aligned}$$

We also fix a suitably Mahlo cardinal κ . We make no attempt at optimization here. Let $a_1 = 1$ and $a_{i+1} = pa_i + q + 2$. Fix $e = a_n$. Fix κ to be a $2e$ -Mahlo cardinal.

We begin with the discrete linearly ordered semigroup with extra structure, $M = (N, <, 0, 1, +, f, g)$.

The plan will be to first construct a structure of the form $M^* = (N^*, <^*, 0^*, 1^*, +^*, f^*, g^*, c_0^*, \dots)$, where the c 's are indexed by N . This structure is non well founded and generated by the constants $0^*, 1^*$, and the c^* 's. The indiscernibility of the c^* 's will be with regard to atomic formulas only. The first nonstandard point in M^* is c_0 .

While it is obvious that we cannot embed M^* back into M , we use the fact that we can embed any partial substructure of M^* that is "boundedly generated" back into M .

Of course, M^* is not well founded, but we prove the well foundedness of the crucial irreflexive transitive relation

$$sx <^* y$$

on N^* , where $s > 1$ is a rational number.

Using the atomic indiscernibility of the c^* 's, we canonically extend M^* to a structure $M^{**} = (N^{**}, <^{**}, 0^{**}, 1^{**}, +^{**}, f^{**}, g^{**}, c_0^{**}, \dots, c_{\aleph}^{**}, \dots)$, $\aleph < \aleph$. Many properties of M^* are preserved when passing to M^{**} . The embedding property asserts that any partial substructure of M^{**} boundedly generated by $0^{**}, 1^{**}$, and a set of c^{**} 's of order type \aleph is embeddable back into M^* and M .

Recall that the proof of the Complementation Theorem requires that the function is strictly dominating with respect to the well founded relation $<$ on N . Here we verify that g^{**} is strictly dominating on the nonstandard part of M^{**} with respect to the above crucial partial ordering. This enables us to apply an analog of the Complementation Theorem to g^{**} on the nonstandard part of M^{**} in order to obtain a unique set $W \subseteq \text{nst}(M^{**})$ such that for all $x \in \text{nst}(M^*)$, $x \in W \iff x \in g^{**}W$.

We then build a Skolem hull construction of length \aleph consisting entirely of elements of W . The construction starts with the set of all c^{**} 's. Witnesses are thrown in from W that verify that values of f^{**} at elements thrown in at previous stages do not lie in W (provided they in fact do not lie in W). Only the first n stages of the construction will be used.

There exists r such that every element of the n -th stage of the Skolem hull construction has a suitable name involving r of the c^{**} 's. We then apply Lemma 2.7 to \aleph , with $n = e$, in order to obtain a suitably indiscernible subset of the c^* 's of order type \aleph .

We redo the Skolem hull construction starting with this type \aleph set of the c^{**} 's. Because of the indiscernibility, we see that at the n -th stage we have a subset of N^{**} of order type \aleph . The n -th stage together with its image under the functions of M^{**} also forms a suitable partial substructure of M^{**} , so that it is embeddable back into M . The image of this embedding on the n stages of the Skolem hull construction will comprise the $A_1 \cup \dots \cup A_n$ satisfying the conclusion of Proposition B. This completes the description of the plan for the proof.

We now begin the detailed proof of Proposition B. We begin with the structure $M = (N, <, 0, 1, +, f, g)$ in the language L consisting of the binary relation $<$, constants $0, 1$, the

binary function $+$, the p -ary function f , the q -ary function g , and equality.

Let $V(L) = \{v_i : i \geq 0\}$ be the set of variables of L . Let $TM(L)$ be the set of terms of L , and $AF(L)$ be the set of atomic formulas of L . For $t \in TM(L)$, we define $lth(t)$ as the number of occurrences of functions, constants, and variables, in t . For $\phi \in AF(L)$, we also define $lth(\phi)$ as the total number of occurrences of functions, constants, and variables, in ϕ .

An M -assignment is a partial function $h:V(L) \rightarrow N$. We write $Val(M,t,h)$ for the value of the term t in M at the assignment h . This is defined if and only if h is adequate for t ; i.e., h is defined at all variables in t .

We also write $Sat(M,\phi,h)$ for atomic formulas ϕ . This is true if and only if h is adequate for ϕ and M satisfies ϕ at the assignment h . Here h is adequate for ϕ if and only if h is defined at all variables in ϕ .

We say that h is increasing if and only if for all $i < j$, if $v_i, v_j \in \text{dom}(h)$ then $h(v_i) < h(v_j)$.

LEMMA 3.1. There exist infinite sets $N \supseteq E_0 \supseteq E_1 \supseteq \dots$ indexed by N , such that for all $i \geq 0$, $\phi \in AF(L)$, $lth(\phi) \leq i$, and increasing h_1, h_2 adequate for ϕ with $\text{rng}(h_1), \text{rng}(h_2) \subseteq E_i$, we have $Sat(M,\phi,h_1) \iff Sat(M,\phi,h_2)$.

Proof: A straightforward application of the usual infinite Ramsey theorem. QED

We fix the E 's in Lemma 3.1. In an abuse of notation, we write $Sat(M,\phi,E)$ if and only if $\phi \in AF(L)$ and for all increasing h adequate for ϕ with range included in E_i , we have $Sat(M,\phi,h)$, where $lth(\phi) = i$. Note that by Lemma 3.1, this is equivalent to $\phi \in AF(L)$ and for some increasing h adequate for ϕ with range included in E_i , we have $Sat(M,\phi,h)$, where $lth(\phi) = i$. We can also use any i with $i \geq lth(\phi)$ and get an equivalent condition.

We now introduce constants c_i , $i \in \mathbb{N}$. Let C be the set of all such constants. Let L^* be L expanded by these constants. Structures in L^* will be written $M^* = (N^*, <^*, 0^*, 1^*, +^*, f^*, g^*, c_0^*, \dots)$.

We let $CT(L^*)$ be the set of closed terms of L^* , and $AS(L^*)$ be the set of atomic sentences of L^* .

For each $\phi \in AS(L^*)$, we write $X(\phi)$ for the following element of $AF(L)$. Let c_{i_1}, \dots, c_{i_r} be the elements of C that appear in ϕ , where $i_1 < \dots < i_r$. Let $X(\phi)$ be the result of replacing these c 's by the variables v_1, \dots, v_r , respectively.

Let T be the following theory in L^* . T consists of all $\phi \in AS(L^*)$ such that $Sat(M, X(\phi), E)$.

LEMMA 3.2. T is consistent. For all $s, t \in CT(L^*)$, exactly one of $s = t$, $s < t$, $t < s$ belongs to T .

Proof: It suffices to show that every finite subset of T is consistent. Let ϕ_1, \dots, ϕ_k be sentences in T . Then for all i , $Sat(M, X(\phi_i), E)$. Obviously if $\phi, \phi' \in AF(L)$ and ϕ' results from ϕ by an increasing change of variables, then $Sat(M, \phi, E) \Rightarrow Sat(M, \phi', E)$. Hence we see that $Sat(M, X(\phi_1 \wedge \dots \wedge \phi_k), E)$, and so $\phi_1 \wedge \dots \wedge \phi_k \in T$. Let $lth(\phi_1 \wedge \dots \wedge \phi_k) = j$, and let c_{i_1}, \dots, c_{i_r} be the elements of C appearing in $\phi_1 \wedge \dots \wedge \phi_k$, where $i_1 < \dots < i_r$. Take $M' = (N, <, 0, 1, +, f, g, c_0', \dots)$, where $c_{i_1}', \dots, c_{i_r}'$ are the first r elements of E_j , and the remaining c 's are 0. Then M' satisfies ϕ_1, \dots, ϕ_k .

For the second claim, let $s, t \in CT(L^*)$. Let $i = lth(s = t)$ and h be an M -assignment into E_i that is adequate for $s = t$. Then $Sat(M, s = t, h)$ or $Sat(M, s < t, h)$ or $Sat(M, t < s, h)$. Hence $Sat(M, s = t, E)$ or $Sat(M, s < t, E)$ or $Sat(M, t < s, E)$. Therefore at least one of $s = t$, $s < t$, $t < s$ lies in T . Since at most one of $Sat(M, s = t, E)$, $Sat(M, s < t, E)$, $Sat(M, t < s, E)$ can hold, clearly at most one of $s = t$, $s < t$, $t < s$ lies in T . QED

We now fix $M^* = (N^*, 0^*, 1^*, <^*, f^*, g^*, c_0^*, \dots)$ to be any model of T which is generated from its constants. Such an M^* exists by the compactness theorem and the fact that T consists entirely of atomic sentences.

LEMMA 3.3. Let $\phi \in AS(L^*)$. $Sat(M^*, \phi)$ if and only if $\phi \in T$.

Proof: Suppose $\phi \in T$. First assume ϕ is of the form $s < t$. By Lemma 3.2, $t > s \notin T$ or $s = t \notin T$. Hence $Sat(M^*, \phi)$ is false. Now assume ϕ is of the form $s = t$. By Lemma 3.2, $s < t \notin T$ or $t < s \notin T$. Hence $Sat(M^*, \phi)$ is false. QED

For $r \geq 1$, we write $M^*[r]$ for the set of all values in M^* of $t \in CT(L^*)$ of length $\leq r$.

We say that H is an r -embedding from M^* into M if and only if

- i) $H:M^*[r] \rightarrow N$;
- ii) $H(0^*) = 0, H(1^*) = 1$;
- iii) for all $x, y \in M^*[r], x <^* y \Rightarrow H(x) < H(y)$;
- iv) for all $x, y, z \in M^*[r], x +^* y = z \Rightarrow H(x) + H(y) = H(z)$;
- v) for all $x_1, \dots, x_p, y \in M^*[r], f^*(x_1, \dots, x_p) = y \Rightarrow f(H(x_1), \dots, H(x_p)) = H(y)$;
- vi) for all $x_1, \dots, x_p, y \in M^*[r], g^*(x_1, \dots, x_p) = y \Rightarrow g(H(x_1), \dots, H(x_p)) = H(y)$.

LEMMA 3.4. Let $r \geq 1$. There is an r -embedding from M^* into M . Every universal sentence of L that holds in M holds in M^* . For any atomic sentence of L^* , if we replace equal c^* 's by equal c 's in a manner that is order preserving on indices, then the truth value in M^* is preserved. The c^* 's are increasing and unbounded in N^* .

Proof: Let H be the increasing bijection from C onto $E_{r(p+q+2)}$. Let h be the increasing bijection from $V(L)$ onto $E_{r(p+q+2)}$. Let h^* be the increasing bijection from C onto $V(L)$.

We extend H to $M^*[r]$ as follows. Let $x = \text{Val}(M^*, t)$, where $t \in CT(L^*), \text{lth}(t) \leq r$. Define $H(x) = \text{Val}(M, h^*(t), h)$.

To see this is well defined, let $x = \text{Val}(M^*, t')$, where $t' \in CT(L^*), \text{lth}(t') \leq r$. We must verify that $\text{Val}(M, h^*(t), h) = \text{Val}(M, h^*(t'), h)$. Since $\text{lth}(t = t') \leq r(p+q+2)$, this equation is equivalent to $\text{Val}(M, h^*(t = t'), E)$, and also to $h^*(t = t') \in T$. By Lemma 3.3, this is equivalent to $\text{Sat}(M^*, t = t')$, which we already have.

For ii), $H(0^*) = \text{Val}(M, h^*(0), h) = 0$. $H(1^*) = \text{Val}(M, h^*(1), h) = 1$.

For iii), we must verify that $\text{Val}(M^*, t) <^* \text{Val}(M^*, t') \Rightarrow \text{Val}(M, h^*(t), h) < \text{Val}(M, h^*(t'), h)$. The left side is equivalent to $\text{Sat}(M^*, t < t')$. The right side is equivalent to $\text{Sat}(M, h^*(t < t'), h)$, and to $\text{Sat}(M, h^*(t < t'), E)$, and to $h^*(t < t') \in T$. Apply Lemma 3.3.

For iv), we must verify that $\text{Val}(M^*, t) +^* \text{Val}(M^*, t') = \text{Val}(M^*, t''') \Rightarrow \text{Val}(M, h^*(t), h) + \text{Val}(M, h^*(t'), h) =$

$\text{Val}(M, h^*(t''), h)$. The left side is equivalent to $\text{Sat}(M^*, t + t' = t'')$. The right side is equivalent to $\text{Sat}(M, h^*(t + t' = t''), h)$, and to $(\text{Sat}, M, h^*(t + t' = t''), E)$, and to $h^*(t + t' = t'')$ \square T. Apply Lemma 3.3.

For v), we must verify that $f^*(\text{Val}(M^*, t_1), \dots, \text{Val}(M^*, t_p)) = \text{Val}(M^*, t) \square f(\text{Val}(M, h^*(t_1)), \dots, \text{Val}(M, h^*(t_p)))$. The left side is equivalent to $\text{Sat}(M^*, f(t_1, \dots, t_p) = t)$. The right side is equivalent to $\text{Sat}(M, h^*(f(t_1, \dots, t_p) = t), E)$, and to $f(t_1, \dots, t_p) = t \square$ T. Apply Lemma 3.3.

For vi), we must verify that $g^*(\text{Val}(M^*, t_1), \dots, \text{Val}(M^*, t_q)) = \text{Val}(M^*, t) \square g(\text{Val}(M, h^*(t_1)), \dots, \text{Val}(M, h^*(t_q)))$. See v).

The second claim follows immediately from the first claim.

Let $\square \square \text{AS}(L^*)$, and \square be obtained by replacing equal c^* 's by equal c^* 's in a manner that is order preserving on indices. We must show that $\text{Sat}(M^*, \square) \square \text{Sat}(M^*, \square)$. Let h^* be an increasing C-assignment which is defined at both \square and \square . Then $\text{Sat}(M, h^*(\square), E) \square \text{Sat}(M, h^*(\square), E)$. Hence $h^*(\square) \square$ T \square $h^*(\square) \square$ T. Apply Lemma 3.3.

For the final claim, let $i < j$. Obviously there is a C-assignment H such that $\text{Sat}(M, H(c_i < c_j), E)$, and so $\text{Sat}(M^*, c_i^* < c_j^*)$.

To see that the c^* 's are unbounded in N^* , let $t \square \text{CT}(L^*)$ and let c_i be the element of C appearing in t with largest subscript. We claim that $t < c_{i+1}$ lies in T . To see this, let h^* be any C-assignment defined at $t < c_{i+1}$. We must verify that $\text{Val}(M, h^*(t < c_{i+1}), E)$. It suffices to find some increasing M-assignment into E_j under which M satisfies $h^*(t < c_{i+1})$, where j is sufficiently large. We can use any increasing M-assignment defined at $h^*(t < c_{i+1})$, where the value at the variable $h^*(c_{i+1})$ is raised to be sufficiently high. QED

We now define the structure $M^{**} = (N^{**}, <^{**}, 0^{**}, 1^{**}, f^{**}, g^{**}, c_0^{**}, \dots, c_\square^{**}, \dots)$, $\square < \square$. Let L^{**} be the language L^* extended by the constants c_\square , $\square < \square$. L^* already has the constants c_i , $i \square \square$.

Let $\text{CT}(L^{**})$ be the set of all closed terms of L^{**} . Let $\text{AS}(L^{**})$ be the set of all atomic sentences of L^{**} . Let $C^{**} = \{c_\square^{**} : \square < \square\}$. C^{**} is the set of transfinite constants.

A reduction is a partial function $J: C^{**} \rightarrow C$. A reduction is said to be increasing if and only if for all $i < j$, if $J(c_i^{**}) = c_i$ and $J(c_j^{**}) = c_j$, then $i < j$. J extends to a partial map from $CT(L^{**})$ into $CT(L^*)$, and to a partial map $AS(L^{**})$ into $AS(L^*)$ in the obvious way. Here J is defined at a closed term or atomic sentence if and only if J is defined at every constant appearing in the closed term or atomic sentence.

We define \equiv on $CT(L^{**})$ as follows. $s \equiv t$ if and only if for all increasing reductions J defined at s, t , we have $\text{Sat}(M^*, J(s = t))$. By Lemma 3.4, the choice of increasing reduction J is irrelevant as long as J is defined at both s, t . This defines an equivalence relation on $CT(L^{**})$. The equivalence classes are written $[t]$, $t \in CT(L^{**})$.

We define N^{**} to be the set of all such equivalence classes. We define $0^{**} = [0]$. We define $1^{**} = [1]$.

We define $[s] <^{**} [t]$ if and only if $\text{Sat}(M^*, J(s < t))$, where J is any (some) reduction defined at s, t .

We define $[s] +^{**} [t] = [s + t]$. We define $f^{**}([t_1], \dots, [t_p]) = [f(t_1, \dots, t_p)]$. We define $g^{**}([t_1], \dots, [t_q]) = [g(t_1, \dots, t_q)]$.

We have to show that the previous two paragraphs constitute well defined definitions.

Suppose $s \equiv s'$, $t \equiv t'$, and for all increasing reductions J defined at s, t , $\text{Sat}(M^*, J(s < t))$. Then for all increasing reductions J defined at s, t, s', t' , $\text{Sat}(M^*, J(s' < t'))$. Hence for some increasing reductions J defined at s', t' , $\text{Sat}(M^*, J(s' < t'))$. So for all increasing reductions J defined at s', t' , $\text{Sat}(M^*, J(s' < t'))$.

Suppose $s \equiv s'$, $t \equiv t'$. We want to show $s + t \equiv s' + t'$. Obviously for all increasing reductions J defined at s, t, s', t' , $\text{Sat}(M^*, J(s + t = s' + t'))$. The remaining cases are handled analogously.

We write $M^{**} = (N^{**}, <^{**}, 0^{**}, 1^{**}, +^{**}, f^{**}, g^{**}, c_0^{**}, \dots, c_{\omega}^{**}, \dots)$, $\omega < \omega$.

The terms $t \in CT(L^{**})$ play a dual role. We used them to define N^{**} as the set of all $[t]$, $t \in CT(L^{**})$, under the equivalence relation \equiv .

However, now that we have defined the structure M^{**} , we can use the terms $t \in CT(L^{**})$ for $Val(M^{**}, t)$.

We leave it to the reader to check that for all $t \in CT(L^{**})$, $Val(M^{**}, t) = [t]$. In particular, every element of M^{**} is generated by its constants.

Let $S \subseteq \mathbb{N}$. We say that $t \in CT(L^{**})$ is an S -term if and only if all transfinite constants in t have subscript lying in S .

LEMMA 3.5. Let $S \subseteq \mathbb{N}$ have order type α . Then the substructure of M^{**} generated by $\{c_\beta^{**} : \beta \in S\}$ is isomorphic to M^* by an isomorphism that maps $\{c_\beta^{**} : \beta \in S\}$ onto $\{c_i^* : i \in \mathbb{N}\}$.

Proof: Let $S = \{\beta_0 < \beta_1 < \dots\}$ be as given. The subset of N^{**} generated in M^{**} by $\{c_\beta^{**} : \beta \in S\}$ is the same as the set of all $[t]$, where $t \in CT(L^{**})$ is an S -term. This can be seen by induction. Let J be the increasing reduction from $\{c_\beta^{**} : \beta \in S\}$ onto $\{c_i^* : i \in \mathbb{N}\}$. The isomorphism maps each of these $[t]$ to $Val(M^*, J(t))$.

To see that this is well defined, let $[t] = [t']$, where $t, t' \in CT(L^{**})$ are S -terms. Then $Val(M^*, J(t = t'))$, and so $Val(M^*, J(t)) = Val(M^*, J(t'))$.

We leave it to the reader to check that this defines the required isomorphism. QED

For $S \subseteq \mathbb{N}$ and $r \geq 1$, we write $M^{**}[S, r]$ for the set of all values in M^{**} of S -terms $t \in CT(L^{**})$ of length $\leq r$.

We say that H is an S, r -embedding from M^{**} into M if and only if

- i) $H: M^{**}[S, r] \rightarrow N$;
- ii) $H(0^{**}) = 0$, $H(1^{**}) = 1$;
- iii) for all $x, y \in M^{**}[S, r]$, $x <^{**} y \rightarrow H(x) < H(y)$;
- iv) for all $x, y, z \in M^{**}[S, r]$, $x +^{**} y = z \rightarrow H(x) + H(y) = H(z)$;
- v) for all $x_1, \dots, x_p, y \in M^{**}[S, r]$, $f^{**}(x_1, \dots, x_p) = y \rightarrow f(H(x_1), \dots, H(x_p)) = H(y)$;

vi) for all $x_1, \dots, x_p, y \in M^{**}[S, r]$, $g^{**}(x_1, \dots, x_p) = y \in g(H(x_1), \dots, H(x_p)) = H(y)$.

LEMMA 3.6. Let $S \subseteq \mathbb{N}$ be of order type ω and $r \geq 1$. There is an S, r -embedding from M^{**} into M . Every universal sentence of L that holds in M holds in M^{**} . For any atomic sentence of L^{**} , if we replace equal transfinite constants by equal transfinite constants in a manner that is order preserving on indices, then the truth value in M^{**} is preserved. The c^{**} 's are increasing and unbounded in N^{**} .

Proof: By Lemma 3.5, let K be an isomorphism from $M^{**}[M^{**}[S]]$ onto M^* mapping $\{c_i^{**}: i \in S\}$ onto $\{c_i^*: i \in \mathbb{N}\}$. By Lemma 3.4, there is an r -embedding from M^* into M . By composing these two mappings, we obtain the desired S, r -embedding from M^{**} into M . The second claim follows immediately. The third claim follows immediately from Lemmas 3.4 and 3.5. The final claim also follows immediately from Lemmas 3.4 and 3.5. QED

We refer to the second claim of Lemma 3.6 as universal sentence preservation. We refer to the third claim of Lemma 3.6 as atomic indiscernibility.

For integers $m \geq 0$, we write m^\wedge for the term $1 + \dots + 1$ with m 1's, where 0^\wedge is 0.

We say that $x \in N^{**}$ is standard if and only if it is the value in M^{**} of some m^\wedge , $m \geq 0$. We say that $x \in N^{**}$ is nonstandard if and only if x is not standard. We write $st(M^{**})$ for the standard elements of N^{**} , and $nst(M^{**})$ for the nonstandard elements of N^{**} .

LEMMA 3.7. Let $x_1, \dots, x_p, y_1, \dots, y_q \in N^{**}$, where $\max(x_1, \dots, x_p), \max(y_1, \dots, y_q) \in nst(M^{**})$. Then

$$\begin{aligned} (1 + 1/b) \max(x_1, \dots, x_p) &<^{**} f^{**}(x_1, \dots, x_p) <^{**} b \max(x_1, \dots, x_p) \\ (1 + 1/b) \max(y_1, \dots, y_q) &<^{**} g^{**}(y_1, \dots, y_q) <^{**} b \max(y_1, \dots, y_q). \end{aligned}$$

Proof: It is clear how to formulate these inequalities without using division, and only addition. Hence they hold by universal sentence preservation. QED

Let $t \in CT(L^{**})$. We write $\#(t)$ for the transfinite constant of greatest index that appears in t . If none appears, take $\#(t) = 0$.

LEMMA 3.8. Let $t \in CT(L^{**})$. If $\#(t) = 0$ then $\text{Val}(M^{**}, t)$ is standard. Suppose $\#(t) = c_\square$. There exists a positive integer d such that $c_\square^{**} \sqsubseteq^* \text{Val}(M^{**}, t) <^{**} dc_\square^{**} <^* c_{\square+1}^{**}$. For all positive integers d and $\square < \square$, $dc_\square^{**} <^{**} c_{\square+1}^{**}$.

Proof: First suppose $\#(t) = 0$. Let $\text{Val}(M^{**}, t) = m$. By universal sentence preservation, $\text{Val}(M^{**}, t) = m^\wedge$. Suppose $\#(t) = c_\square$. It is easy to prove by induction on t that $c_\square^{**} \sqsubseteq^{**} \text{Val}(M^{**}, t)$ using the lower bounds in Lemma 3.7. It is also easy to prove by induction on t that there exists a positive integer d such that $\text{Val}(M^{**}, t) <^{**} dc_\square^{**}$, using the upper bounds in Lemma 3.7.

It remains to prove that for all positive integers d and $\square < \square$, $dc_\square^{**} <^{**} c_{\square+1}^{**}$. Suppose $dc_\square^{**} \geq^{**} c_{\square+1}^{**}$. By atomic indiscernibility, for all $\square > \square$, $dc_\square^{**} \geq^{**} c_\square^{**}$. This contradicts the unboundedness of the c^{**} 's in N^{**} . Liberal doses of universal sentence preservation throughout the arguments are used. QED

We will use interval notation for the linear ordering $<^{**}$.

LEMMA 3.9. $\text{st}(M^{**}) = \{x : x <^{**} c_0^{**}\} = [0, c_0^{**})$.

Proof: Suppose $c_0^{**} \sqsubseteq^{**} m^\wedge$. By universal sentence preservation, let $c_0^{**} = r^\wedge$, $r \sqsubseteq m$. By atomic indiscernibility, $c_1^{**} = r^\wedge$, violating $c_0^{**} <^* c_1^{**}$. This verifies the forward inclusion. For the reverse inclusion, let $x <^{**} c_0^{**}$. Write $x = \text{Val}(M^{**}, t)$. By Lemma 3.8, $\#(t) = 0$. By Lemma 3.8, x is standard. QED

Let s be a rational number > 1 and $x \sqsubseteq N^*$. We define $sx <^{**} y$ as follows. Let $s = d/e$, where d, e are positive integers. Then $sx <^{**} y$ if and only if $dx <^{**} ey$.

We write $<_s^{**}$ for the relation on N^{**} given by $x <_s^{**} y \iff sx <^{**} y$.

LEMMA 3.10. Let s be a rational number > 1 . There exists $k \geq 1$ such that for all $x_1 <_s^{**} x_2 <_s^{**} \dots <_s^{**} x_k$, we have $2x_1 <^{**} x_k$.

Proof: Using universal sentence preservation, we see that $x_1 <_{s'}^{**} x_k$, where $s' = s^{k-1}$. If k is large enough then $s' \geq 2$. QED

LEMMA 3.11. Let s be a rational number > 1 . The relation $<_s^{**}$ on N^{**} is transitive, irreflexive, and well founded.

Proof: Transitivity and irreflexivity follow from universal sentence preservation. By well foundedness, we mean that every nonempty subset S of N^{**} has a $<_s^{**}$ minimal element; i.e., an $x \in S$ such that for no $y \in S$ is $y <_s^{**} x$.

By Lemma 3.10, if $<_2^{**}$ is well founded then $<_s^{**}$ is well founded. We now show that $<_2^{**}$ is well founded.

Let Y be a nonempty subset of N^{**} . Choose t so that $\#(t)$ is least with $\text{Val}(M^{**}, t) \in Y$. If $\#(t) = 0$ then Y has a standard element. Let x be the least standard element of Y . Then x is a $<_2^{**}$ minimal element of S .

Let $\#(t) = c_0$ and assume Y has no $<_2^{**}$ minimal element. Choose an infinite sequence $t = t_1, t_2, \dots$ such that in M^{**} , each $t_j > 2t_{j+1}$. By Lemma 3.8, $\text{Val}(M^{**}, t) <^{**} c_{0+1}^{**}$, and so by Lemma 3.8, each $\#(t_j) \in c_0$. By the choice of c_0 , each $\#(t_j) = c_0$. By Lemma 3.8, each $t_j \geq c_0$ in M^{**} . Hence each in M^{**} , each $t_{j+2} > 2^i c_0$. By Lemma 3.8, let d be a positive integer such that $t < dc_0$ holds in M^{**} . Then for all j , $dc_0 > 2^j c_0$ in M^{**} . This is a contradiction. QED

It is convenient to let $s = 1 + 1/b$ for using Lemma 3.7. We now apply the well foundedness of $<_s^{**}$ in an essential way.

LEMMA 3.12. There is a unique set $W \in \text{nst}(M^{**})$ such that for all $x \in \text{nst}(M^{**})$, $x \in W \iff x \in g^{**}W$. For all $\alpha < \omega$, $c_\alpha^{**} \in \text{rng}(f^{**}), \text{rng}(g^{**})$. In particular, each $c_\alpha^{**} \in W$.

Proof: Since $<_s^{**}$ is well founded on N^{**} , we can perform transfinite recursion on $<_s^{**}$. So we can define $x \in W$ if and only if $x \in \text{nst}(M^{**})$ and $(\exists y \in W^\alpha) (\max(y) <_s^{**} x \in g^{**}(y) \neq x)$.

Let $x \in \text{nst}(M^{**})$. We claim that $x \in W \iff x \in g^{**}W$. Let $x \in W$, $x \in g^{**}W$. Let $x = g^{**}(y)$, $y \in W^\alpha$. Since $W \in \text{nst}(M^{**})$, by Lemma 3.7, we have $\max(y) \in \text{nst}(M^{**})$. Hence by Lemma 3.7, we have $\max(y) <_s^{**} g^{**}(y)$. Hence $y \in W^\alpha$, $\max(y) <_s^{**} x$, $g^{**}(y) = x$, which is a contradiction.

We also claim that $x \in g^{**}W \iff x \in W$. Let $x \in W$. Then $x \in \text{nst}(M^{**})$ or $(\exists y \in W^\alpha) (\max(y) <_s^{**} x \in g^{**}(y) = x)$. Hence $x \in g^{**}W$.

To see that W is unique, let $W' \subseteq \text{nst}(M^{**})$, where for all $x \in \text{nst}(M^{**})$, $x \in W' \iff x \in g^{**}W'$, and $W \neq W'$. Let x be $<_s^{**}$ minimal such that $x \in W \not\subseteq x \in W'$. Then $x \in \text{nst}(M^{**})$, and $x \in g^{**}W \not\subseteq x \in g^{**}W'$. Also, for all $y <_s^{**} x$, $y \in W \iff y \in W'$. By Lemma 3.7, $x \in g^{**}W \not\subseteq x \in g^{**}W'$. This is a contradiction.

For the second claim, write $c_0^{**} = f^{**}(x_1, \dots, x_p)$. By Lemma 3.7, $\max(x_1, \dots, x_p) \in \text{nst}(M^{**})$, and so by Lemma 3.7, $\max(x_1, \dots, x_p) <^{**} c_0^{**}$. By Lemma 3.8, $\text{bmax}(x_1, \dots, x_p) <^{**} c_0^{**}$. By Lemma 3.8, $f^{**}(x_1, \dots, x_p) <^{**} \text{bmax}(x_1, \dots, x_p) <^{**} c_0^{**}$, which is a contradiction. The same argument works for g^{**} . The third claim follows from $c_0^{**} \in \text{rng}(g^{**})$. QED

We fix the unique W from Lemma 3.12. We will use q functions $F_1, \dots, F_q: N^{**} \subseteq W$ such that for all $x \in g^{**}W$,

$$x = g^{**}(F_1(x), \dots, F_q(x))$$

and for all $x \in g^{**}W$,

$$F_1(x) = \dots = F_q(x) = c_0^{**}.$$

We now come to the Skolem hull construction.

We let $E \subseteq \emptyset$. Define $E[1] = \{c_0^{**}: \emptyset \subseteq E\}$. Suppose $E[1] \subseteq \dots \subseteq E[k] \subseteq W$ have been defined. Define $E[k+1] = E[k] \cup (f^{**}E[k] \cup W) \cup F_1 f^{**}E[k] \cup \dots \cup F_q f^{**}E[k]$.

LEMMA 3.13. Let $E \subseteq \emptyset$. Then $E[1] \subseteq \dots \subseteq E[k] \subseteq W$, and for all $i \geq 1$, $f^{**}E[i] \subseteq E[i+1] \subseteq g^{**}E[i+1]$, and $E[1] \cap f^{**}E[i] = \emptyset$.

Proof: Let $i \geq 1$ and $x \in f^{**}E[i]$. Since $E[i] \subseteq \text{nst}(M^{**})$, we have $x \in \text{nst}(M^{**})$ by Lemma 3.7. Hence if $x \in W$ then $x \in E[i+1]$. Suppose $x \notin W$. Then $x \in g^{**}W$, and so $x = g^{**}(F_1(x), \dots, F_q(x))$. Now each $F_i(x) \in E[i+1]$ since $x \in f^{**}E[i]$. Hence $x \in g^{**}E[i+1]$.

$E[i+1] \cap g^{**}E[i+1] = \emptyset$ follows from $W \cap g^{**}W = \emptyset$. $E[1] \cap f^{**}E[i]$ follows from the second claim of Lemma 3.12. QED

Note that Proposition B is essentially the same as Lemma 3.12 (restricted to $1 \leq i < n$), but Proposition B lives in M and Lemma 3.12 lives in M^{**} . The remainder of the proof of

Proposition B surrounds the choice of a suitable E such that $E[n]$ can be suitably embedded back into M .

LEMMA 3.14. There exist functions G_1, G_2, \dots , indexed by the positive integers, where the G_i are multivariate functions from \square into W of various arities, such that the following holds. For all $i \geq 1$ and $E \square \square$, $E[i] = G_i E$. In fact, we can take the arities to be a_1, a_2, \dots , where $a_1 = 1$ and $a_{i+1} = pa_i + q + 2$.

Proof: We construct the G 's by induction. Take $G_1(\square) = c_{\square}^{**}$. Suppose G_i has been defined, $i \geq 1$, with arity r . Recall that $E[i+1] = E[i] \square (f^{**}E[i] \square W) \square F_1 f^{**}E[i] \square \dots \square F_q f^{**}E[i]$. G_{i+1} works with p elements of $E[i]$ together with an integer in $[1, q+2]$, the latter indicating what operation to perform on these p elements of $E[i]$. I.e., G_{i+1} applies to pr elements of W and an element of $[1, q+2]$. We can clearly arrange for G_{i+1} to apply to $pr+q+2$ elements of E . We are not trying to do any optimization here. QED

We will only be using the function G_n from Lemma 3.14. Recall that \square is 2e-Mahlo, where $e = a_n$ is the arity of G_n .

We now define "term decomposition" functions $H_i: W \square \square$, indexed by the natural numbers. Let $x \square W$. To define the $H_i(x)$, first choose $t \square CT(L^{**})$ such that $\text{Val}(M^{**}, t) = x$. Let $c_{\square 1}, c_{\square 2}, \dots, c_{\square s}$ be a listing of all transfinite constants appearing in t from left to right (with repetitions). In general, there will be repetitions.

For $x \square W$, set $H_0(x) = \text{lth}(t)$. For $1 \square i \square s$, set $H_i(x) = \square_i$. For $i > s$, set $H(x_0) = 0$.

Finally, define functions $J_i: \square^e \square \square$, $i \geq 0$, by $J_i(\square_1, \dots, \square_r) = H_i(G_n(\square_1, \dots, \square_r))$.

LEMMA 3.15. Let $E \square \square$. Every element of $E[n]$ is the value in M^{**} of a term $t \square CT(L^{**})$ whose length lies in $J_0 E$ and whose transfinite constants have subscripts lying in $\square \{J_i E: 1 \square i \square \text{lth}(t)\}$.

Proof: Let $x \square E[n]$. By Lemma 3.13, $x \square G_n E$. Let t be the term used to represent x in the definition of the $H_i(x)$. Write $x = G_n(\square_1, \dots, \square_e)$, $\square_1, \dots, \square_e \square E$. Then $J_0(\square_1, \dots, \square_e) = H_0(x) = \text{lth}(t)$, and $J_1(\square_1, \dots, \square_e), J_2(\square_1, \dots, \square_e), \dots, J_{\text{lth}(t)}(\square_1, \dots, \square_e)$

enumerates at least the subscripts of transfinite constants in t . QED

LEMMA 3.16. There exists $E \sqsubseteq S \sqsubseteq \Omega$, E, S of order type Ω , and a positive integer d , such that $E[n] \sqsubseteq M^{**}[S, d]$.

Proof: By Lemma 2.7, let $E \sqsubseteq \Omega$ be of order type Ω such that for all $i \geq 1$, $J_i E$ is either finite or has order type Ω with the same sup as E , and $J_0 E$ is finite. Let d be the maximum element of $J_0 E$. By Lemma 3.15, every element of $E[n]$ is the value in M^{**} of a closed term t of length at most d , whose transfinite constants have subscripts lying in $\{\{J_i E: 1 \leq i \leq \text{lth}(t)\}\}$. Therefore every element of $E[n]$ is the value in M^{**} of a closed term of length at most d whose transfinite constants have subscripts lying in $\{J_i E: 1 \leq i \leq d\}$. Set $S = \{J_i E: 1 \leq i \leq d\} \sqsubseteq E$. QED

We fix E, S, d as given by Lemma 3.16.

THEOREM 3.17. Assume MAH+. Proposition B holds.

Proof: By Lemma 3.13, for all $1 \leq i < n$, $f^{**}E[i] \sqsubseteq E[i+1] \sqsubseteq g^{**}E[i+1]$, and $E[1] \sqsubseteq f^{**}E[n] = \emptyset$. By Lemma 3.6, there is an $S, d(p+q+2)$ -embedding H from M^{**} into M . Note that $f^{**}[E[n]] \sqsubseteq g^{**}[E[n]] \sqsubseteq M^{**}[S, d(p+q)] \sqsubseteq \text{dom}(H)$.

For $1 \leq i \leq n$, let $A_i = HE[i]$. It is clear that $A_1 \sqsubseteq \dots \sqsubseteq A_n \sqsubseteq N$.

We first claim that for all $1 \leq i < n$, $fA_i \sqsubseteq A_{i+1} \sqsubseteq gA_{i+1}$.

Let $1 \leq i < n$, and $x \in fA_i$. Write $x = f(Hy_1, \dots, Hx_p)$, $y_1, \dots, y_p \in E[i]$. Now $f^{**}(y_1, \dots, y_p) \in \text{dom}(H)$, and so $Hf^{**}(y_1, \dots, y_p) = f(Hy_1, \dots, Hy_p) = x$.

Now $f^{**}(y_1, \dots, y_p) \in E[i+1] \sqsubseteq g^{**}E[i+1]$. First suppose $f^{**}(y_1, \dots, y_p) \in E[i+1]$. Then $Hf^{**}(y_1, \dots, y_p) = x \in A_{i+1}$.

Secondly suppose $f^{**}(y_1, \dots, y_p) \in g^{**}E[i+1]$, and write $f^{**}(y_1, \dots, y_p) = g^{**}(z_1, \dots, z_q)$, where $z_1, \dots, z_q \in E[i+1]$. Then $g^{**}(z_1, \dots, z_q) \in \text{dom}(H)$, and so $Hg^{**}(z_1, \dots, z_q) = g(Hz_1, \dots, Hz_q)$. Hence $Hf^{**}(y_1, \dots, y_p) = Hg^{**}(z_1, \dots, z_q) = g(Hz_1, \dots, Hz_q) = f(Hy_1, \dots, Hy_p) = x$. Hence $x \in gA_{i+1}$.

We secondly claim that for all $1 \leq i < n$, $A_{i+1} \sqsubseteq gA_{i+1} = \emptyset$. We must verify that $HE[i+1] \sqsubseteq gHE[i+1] = \emptyset$. Let $x, y_1, \dots, y_q \in$

$E[i+1]$, $H(x) = g(Hy_1, \dots, Hy_q)$. Since $g^{**}(y_1, \dots, y_q) \in \text{dom}(H)$, we have $H(x) = Hg^{**}(y_1, \dots, y_q)$, and so $x = g^{**}(y_1, \dots, y_q)$. This contradicts $E[i+1] \cap gE[i+1] = \emptyset$.

We finally claim that $A_1 \cap fA_n = \emptyset$. Let $x \in A_1$, $y_1, \dots, y_p \in A_n$, $x = f(y_1, \dots, y_p)$. Let $x' \in E[1]$, $y_1', \dots, y_p' \in E[n]$, where $x = H(x')$, and $y_1, \dots, y_p = H(y_1'), \dots, H(y_p')$ respectively. Note that $f^{**}(y_1', \dots, y_p') \in \text{dom}(H)$. Hence $f(Hy_1', \dots, Hy_p') = Hf^{**}(y_1', \dots, y_p') = x = H(x')$. Therefore $x' = f^{**}(y_1', \dots, y_p')$, contradicting claim 2 of Lemma 3.12. QED

REFERENCES

[Fr01] H. Friedman, Lecture notes on baby Boolean relation theory, <http://www.math.ohio-state.edu/~friedman/>

[Fr??] H. Friedman, 6561 cases of Boolean relation theory, in preparation.

[HKS] A. Hajnal, A. Kanamori, S. Shelah, Regressive partition relations for infinite cardinals, TAMS 299 (1987), 145-154.

[Sc74] J. Schmerl, A partition property characterizing cardinals hyperinaccessible of finite type, TAMS 188 (1974), 281-291.

*This research was partially supported by NSF Grant DMS-9970459.