MAXIMAL NONFINITELY GENERATED SUBALGEBRAS

Harvey M. Friedman*
friedman@math.ohio-state.edu
http://www.math.ohio-state.edu/~friedman/
Department of Mathematics
Ohio State University

September 24, 2000
October 19, 2001

Abstract. We show that "every countable algebra with a nonfinitely generated subalgebra has a maximal nonfinitely generated subalgebra" is provably equivalent to $□^1_1$-CA_0 over RCA_0.

1. INTRODUCTION

For our purposes, a countable algebra □ is a system whose domain is a subset of □ (possibly empty), with at most countably many constant and function symbols of various arities.

A subalgebra of a countable algebra □ is a subset of its domain that contains the constants and is closed under the functions. The empty subalgebra is allowed. (We could have defined subalgebras to be algebras, but it is more convenient for us to identify subalgebras with their domains).

A finitely generated subalgebra is a subalgebra □ such that for some finite □ □ □, □ consists of all values of terms involving constants and functions from □ and arguments from □. □ is called a set of generators for □. A subalgebra is said to be nonfinitely generated if and only if it is not finitely generated. Note that the empty set is automatically finitely generated.

A maximal nonfinitely generated subalgebra is a nonfinitely generated subalgebra □ such that every nonfinitely generated subalgebra is a subset of □.

THEOREM 1.1. Every countable algebra with a nonfinitely generated subalgebra has a maximal nonfinitely generated subalgebra.

Proof: Let □ be a countable algebra with a nonfinitely generated subalgebra □. We define a transfinite sequence $□_□$,

$\square < \omega_1$, of nonfinitely generated subalgebras of □ as follows. $\square_0 = \square$. Suppose $\square_\square$ has been defined. Define $\square_{\square+1}$ to be a nonfinitely generated subalgebra of □ properly extending $\square_\square$ if such exists; $\square_\square$ otherwise. Suppose $\square_\square$, $\square < \square$, has been defined. For limit ordinals □, set $\square_\square$ to be the union of the $\square_\square$, $\square < \square$. By cardinality considerations, let $\square < \omega_1$ be such that $\square_\square = \square_{\square+1}$. Then $\square_\square$ is as required. QED

We wish to analyze Theorem 1.1 from the viewpoint of reverse mathematics. The formalization of Theorem 1.1 within the language of the base theory RCA_0 is straightforward.

Note that above proof is very set theoretic, and even uses the axiom of choice both in the choice of the $\square_{\square+1}$ and in the use of the regularity of ω_1.

We now give a second, more concrete proof.

Proof: We define a sequence $\square_n$, $n < \omega$, of nonfinitely generated subalgebras of □ as follows. Let $\square_0$ be any nonfinitely generated subalgebra of □. Suppose $\square_n$ has been defined. Define $\square_{n+1}$ to be a nonfinitely generated subalgebra of □ properly containing $\square_n \cup \{n\}$ if such exists; $\square_n$ otherwise. Let □ be the union of the $\square_n$. Obviously □ is a nonfinitely generated subalgebra of □. To see that □ is maximal, let □□be a nonfinitely generated subalgebra of □ containing □, and let n be the least element of □□\□. Then by construction, n was thrown in at stage n+1, and so $n \in \square$, which is a contradiction. QED

LEMMA 1.2. Theorem 1.1 is provable in $\Pi^1_1\text{-}CA_0$.

Proof: The second proof above is clearly within strong $\Pi^1_1\text{-}DC_0$, which is equivalent to $\Pi^1_1\text{-}CA_0$ according to [Si99], p. 301. QED

This suggests that Theorem 1.1 is provably equivalent to $\Pi^1_1\text{-}CA_0$ over RCA_0, which we confirm in section 3.

2. WELL FOUNDED PARTS.

Here we obtain some results in reverse mathematics that we needed for the next section. These results are of independent interest.

All definitions in this section are made within RCA$_0$ in the standard way as described in Si99.

A linear ordering on □ is an R □ □^{2} such that for all n,m,r □ □,
i) (n,m) □ R □ (m,r) □ R) □ (n,r) □ R;
ii) exactly one of (n,m) □ R, (m,n) □ R, n = m holds.

Note that ii) is trichotomy, and implies irreflexivity.

We normally write R as <□ and use infix notation. We also use □□ for the reflexive closure of <□.

A tail of a linear ordering on □ is an □ □ □ such that (n □ □ □ n <□ m) □ m □ □.

There are three obvious notions of well foundedness for linear orderings on □. Well foundedness asserts that every nonempty subset has a least element. Tail well foundedness asserts that every nonempty tail has a least element. Sequential well foundedness asserts that there are no infinite descending sequences.

THEOREM 2.1. The following is provable in RCA$_0$. Well foundedness and sequential well foundedness are equivalent. Well foundedness implies tail well foundedness.

Proof: The second claim is obvious. For the first claim, let <□ be a linear ordering on □. Assume <□ is well founded. Let f:□ □ □ be strictly descending. Define g:□ □ □ by g(0) = f(0), g(n+1) = f((□m)(f(m) > g(n))). Since g is strictly increasing, its range of values can be defined in both □$^0_1$ and □$^0_1$ form. Therefore rng(g) exists, and has no least element. Therefore <□ is sequentially well founded.

On the other hand, assume <□ is sequentially well founded. Let □ be a nonempty set with no least element. Let r □ □. Define h:□ □ □ by h(0) = r, h(n+1) = (□m)(m □ □ □ m <□ h(n)). Then h is a strictly descending sequence. Therefore <□ is well founded.

Note that in both directions, we use primitive recursion, which is available in RCA$_0$. Strictly speaking, we need to define intermediate functions using the □ operator, which is also available in RCA$_0$. QED

The (non) well founded part of a linear ordering of □ is the set of all elements of □ such that the linear ordering up to that element is (not) well founded.

The (non) tail well founded part of a linear ordering of □ is the set of all elements of □ such that the linear ordering up to that element is (not) tail well founded.

As we shall see, these parts cannot be proved to exist within RCA_0, or even ACA_0.

All of the definitions in the preceding three paragraphs are made within RCA_0.

There are some relationships that are provable in RCA_0.

THEOREM 2.2. The following is provable in RCA_0. Let <□ be a linear ordering of □. If the well founded part of <□ exists then the tail well founded part of <□ exists and they are equal.

Proof: i) is obvious. Suppose □ is the well founded part of <□. If n □ □ then obviously <□ is tail well founded up to n. If n □ □ then <□ is not tail well founded up to n since {p <□ n: p is not in the well founded part of <□} is a nonempty tail in <□ below n with no <□ least element. Therefore □ is the tail well founded part of <□. QED

LEMMA 2.3. The following are equivalent over RCA_0.
i) For all one-one f:□ □ □\{0}, rng(f) exists;
ii) ACA_0.

Proof: [Si99], p. 105, proves this without the deletion of 0. Just compose with +1. QED

Let □^□ be the set of all finite sequences from □ (including the empty sequence). For x □ □^□, we write lth(x) for the number of terms of x. We index the terms of each x □ □^□ from 1 to lth(x). For x,y □ □^□ we write x □ y to indicate that x is an initial segment of y, and x □ y to indicate that x is a proper initial segment of y. We say that x,y are comparable if and only if x □ y   y □ x.

Now let f:□ □ □\{0} be one-one. In RCA_0, we construct a linear ordering <□ on D □ □, where D is some set of nonempty finite sequences, as follows. (Since no nonempty finite sequence is an element of □, this is a disjoint union.) We index nonempty finite sequences x from 1 through the length of x, written lth(x). We consider two finite sequences comparable if one is an initial segment of the other.

Let D be the set of all finite sequences $(n_1,...,n_k)$, k ≥ 1, such that

i) for all 1 □ i □ k, n_i = 0 or n_i = $f^{\square 1}(i)$;
ii) for all 1 □ i □ k, if $f^{-1}(i)$ □ max($n_1,...,n_k$,k) then n_i = $f^{\square 1}(i)$.

We order the elements of D □ □ as follows. Let x,y □ D □ □.

a. x,y □ □. Take x <□ y if and only if x > y.
b. x,y □ D. Take x <□ y if and only if either x □ y or at the first place at which x,y differ, y is 0.
c. x □ □, y □ D. Take x <□ y if and only if there exists 1 □ i □ lth(y) such that y_i = 0 and $f^{\square 1}(i)$ □ x.
d. x □ D, y □ □. Take x <□ y if and only if not y <□ x.

Note that <□ on D is just the usual lexicographic ordering of $\square^{\square}$ on D, where □ is given its usual linear ordering except that 0 is placed at the top. Hence <□ on D is a linear ordering.

LEMMA 2.4. <□ is a linear ordering on D □ □.

Proof: We first claim that <□ obeys trichotomy. This is immediate in case a above. For case b, we have already remarked that <□ on D is a linear ordering. For the remaining cases, we have x ≠ y, and so we need only verify that x <□ y y <□ x, but not both. This is clear by case d.

To complete the proof, we need only check transitivity. Suppose x <□ y and y <□ z.

We first show that x,y,z are distinct. Clearly x ≠ y and y ≠ z by trichotomy. Suppose x = z. Then x <□ y and y <□ x, which contradicts trichotomy.

There are eight cases. Thus in each case, we can either show x <□ z directly, or assume z <□ x and derive a contradiction.

case 1. x,y,z □ □. Obviously x <□ z.

case 2. x,y,z □ D. As remarked above, <□ on D is a linear ordering, and so x <□ z.

case 3. x □ D, y,z □ □. Suppose z <□ x. By case c, y <□ x, which is a contradiction.

case 4. x □ D, y □ □, z □ D. By case c, let z_i = 0 and $f^{□1}$(i) □ y. By the definition of D, every coordinate of z is < $f^{□1}$(i). In particular, every coordinate of z is < y.

First let j be the first place at which x,z differ. If x_j = 0 then z_j = $f^{□1}$(j) < y, and so y <□ x. Therefore $x_j \neq 0$ and z_j = 0. Hence x <□ z.

Now suppose there is no place at which x,z differ. Then x,z are comparable. If z □ x, then y <□ x follows from y <□ z. Hence x □ z, and so x <□ z.

case 5. x,y □ D, z □ □. Assume z <□ x. Then y <□ z <□ x, and so by case 4, y <□ x.

case 6. x □ □, y,z □ D. Suppose z <□ x. By case 4, z <□ y.

case 7. x □ □, y □ D, z □ □. Suppose z <□ x. By case 3, z <□ y.

case 8. x □ □, y □ □, z □ D. Suppose z <□ x. By case 3, z <□ y.

QED

LEMMA 2.5. For each n □ □, {x: n <□ x} is a finite set.

Proof: Let x = (x_1,...,x_k) □ D. We claim that for all n <□ x, max(x_1,...,x_k,k) < n. To see this, let x_i = 0, $f^{□1}$(i) □ n. Since x □ D, we have $f^{□1}$ (i) □ max(x_1,...,x_k,k) □ x_i = f^{-1}(i). Hence max(x_1,...,x_k,k) < $f^{□1}$(i) □ n. And for x □ □, if n <□ x then x < n. QED

We say that x is correct if and only if x □ D and (□i)(1 □ i □ lth(x) □ (x_i > 0 □ i is a value of f).

LEMMA 2.6. x is correct □ (□n □ □)(x <□ n). x is correct □ {y: y <□ x} exists and is finite.

Proof: Let x be correct and n □□□. Then x □ D, and so n <□x. Let x_i = 0, $f^{□1}(i)$ □ n. Then x is not correct.

Let (□n □ □)(x <□n). Then x □ D, and write x = $(x_1,...,x_k)$. Suppose 1 □ i □ k, x_i = 0, and i is a value of f. Then $f^{-1}(i)$ <□x, contradicting the hypothesis on x. And by the definition of D, if x_i > 0 then i is a value of f. This establishes the first claim.

For the second claim, note that any two correct x are comparable elements of D. Also, if y <□x and x is correct, then y is correct. Hence if y <□x and x is correct then y □ x. QED

LEMMA 2.7. For all p □ □, there is a unique correct x of length p.

Proof: Note that by Lemma 2.6, correctness is a $□^0_1$ predicate. Hence by $□^0_1$ induction, there is a correct x of length p. Uniqueness is obvious. QED

LEMMA 2.8. If the set of correct x exists then rng(f) exists.

Proof: Suppose the set of correct x exists. We claim that for all p □ □, p is a value of f if and only if p ≠ 0 and (□ correct x)(lth(x) = p □ x_p > 0). The forward direction is immediate. For the reverse direction, use Lemma 2.7.

We have given a $□^0_1$ definition of rng(f), which also has an obvious $□^0_1$ definition. Hence rng(f) exists. QED

LEMMA 2.9. <□is not well founded. Every nonempty tail in <□ with no <□least element is the set of incorrect x □ D □ □.

Proof: <□is obviously not well founded since □ has no <□ least element. Now let □ be a nonempty tail in <□with no <□ least element. By Lemma 2.6, if □ has a correct element, then □ has a <□least element. Hence all elements of □ are incorrect.

We now claim that □ □ □. Suppose n □ □, n □ □. Since □ is a tail, every element of □ is >□n. By Lemma 2.5, □ is finite, which is a contradiction.

We have thus proved that □ □ □. The Lemma follows from Lemma 2.6 since □ is a tail. QED

LEMMA 2.10. Let x □ D □ □. Then <□ is well founded up to x if and only if x is correct.

Proof: If x is not correct, let n □□ x. Now [n,) has no least element, and so <□ is not well founded up to x. On the other hand, if x is correct, apply Lemma 2.6. QED

Let x □ □. Then both sides of the equivalence are false using the fact that □ has no <□ least element. Let x □ D. If the right side is true then by Lemma 2.6, the left side is true. If the right side is false then the left side is false since □ has no <□ least element. QED

THEOREM 2.11. The following are provably equivalent over RCA_0.
i) ACA_0.
ii) for all linear orderings $<^□$ on □ and x □ □, {y: (□n □ x) (n $□^□$ y)} exists;
iii) for all linear orderings on □, if the tail well founded part exists then the well founded part exists;
iv) every tail well founded linear ordering on □ is well founded;
v) in every tail well founded linear ordering on □, the well founded part exists.

Proof: It is obvious that i) implies ii) implies iii). Now assume iii). Let $<^□$ be tail well founded. Then the tail well founded part of $<^□$ exists and is □, and therefore the well founded part of $<^□$ exists. By Theorem 2.2, the well founded part of <□ is also □. Hence $<^□$ is well founded.

It is obvious that iv) implies v). We have only to prove v) implies i). Assume v). Since our choice of one-one f:□ □ □\{0} was arbitrary, by Lemma 2.3 it suffices to show that rng(f) exists.

Suppose rng(f) does not exist. By Lemma 2.8, the set of correct x does not exist. By Lemma 2.9, every nonempty tail has a least element. Hence <□ is tail well founded. Therefore the tail well founded part exists. Hence by v), the well founded part exists. Hence by Lemma 2.10, the set of correct x exists. Therefore by Lemma 2.8, rng(f) exists. QED

LEMMA 2.12. Each of the following implies ACA_0 over RCA_0. The well founded part of every linear ordering on □ exists. The tail well founded part of every linear ordering on □ exists.

Proof: Suppose the well founded part of every linear ordering on □ exists. Then the well founded part of <□ exists. By Lemma 2.10, the set of correct x exists. By Lemma 2.8, rng(f) exists.

Suppose the tail well founded part of every linear ordering on □ exists. We now modify <□ to <□ so that the tail well founded part is again the set of correct x. For this purpose, we introduce new domain elements which are triples (n,m,□1), n,m □ □. The set of all new domain elements will be written as D□.

We extend <□ by

i) (n,m,□1) <□ (r,s,-1) if and only if n > r (n = r □ m > s);
ii) (n,m,□1) <□ r if and only if n ≥ r;
iii) r <□ (n,m,□1) if and only if n < r;
iv) for all x □ D, (n,m,□1) <□ x if and only if n <□ x;
v) for all x □ D, x <□ (n,m,□1) if and only if x <□ n.

We leave it to the reader to verify that <□ is a linear ordering on D □ □ □ D□ that extends <□.

Thus for each n □ □, the n,(n, 0,□1),(n, 1,□1),(n,2,□1),... forms a consecutive descending sequence in <□.

It is clear that for all n □ □, <□ is not tail well founded up to n, because {(n,m,-1): m ≥ 0} is a nonempty tail below n with no least element. Hence for all x □ D □ □ □ D□, if (□n □ □)(n <□ x) then <□ is not tail well founded up to x. On the other hand, suppose (□n □ □)(x <□ n). Then x □ D and x is correct. Therefore using Lemma 2.10, <□ is tail well founded up to x.

From this we conclude that <□ is tail well founded up to x if and only if x is correct. Since the tail well founded part of <□ exists, the set of correct x exists. Hence by Lemma 2.8, rng(f) exists. QED

A tree is a nonempty subset of □□ which is closed under initial segments (and hence contains the empty sequence). A tree □ is said to be well founded if and only if there is no infinite sequence x_1 □ x_2 □ ... of elements of □.

For any tree □ and x □ □, we write □[x] for the tree {y □ □: x,y are comparable}.

LEMMA 2.13. The following are provably equivalent over RCA_0.
i) $\square^1{}_1$-CA_0;
ii) For any tree □, {x: □[x] is well founded} exists;
iii) For any sequence of trees $\square_0, \square_1, \ldots$, {n: $\square_n$ is well founded} exists.

Proof: i) implies ii) is obvious. Assume ii), and let $\square_0, \square_1, \ldots$ be a sequence of trees. We define the tree □ = $\{(n_1,\ldots,n_k): k \geq 1$ □ $(n_2,\ldots,n_k)$ □ $\square_{n\_1}\}$. Then obviously for all n □ □, □[(n)] is well founded if and only if $\square_n$ is well founded. So {n: □[(n)] is well founded} exists and is {n: $\square_n$ is well founded}.

iii) implies i) is from [Si99], p. 217. QED

THEOREM 2.14. The following are provably equivalent over RCA_0.
i) $\square^1{}_1$-CA_0;
ii) The well founded part of every linear ordering on □ exists;
iii) The tail well founded part of every linear ordering on □ exists.

Proof: i) □ ii) is obvious. ii) □ iii) is by 2.2. We now assume iii) and derive i). By Lemma 2.12, we have ACA_0, and therefore ii).

By Lemma 2.13, it suffices to let □ be a tree and prove that {x: □[x] is well founded} exists.

We now use the Kleene-Brouwer ordering. This is the linear ordering $<^\square$ on $\square^\square$ defined by x $<^\square$ y if and only if

y □ x or x is smaller than y
at the first place at which they differ.

We consider the linear ordering (□, $<^\square$), which is $<^\square$ restricted to the domain □. We know that the well founded part of (□, $<^\square$) exists.

We now claim that for all x □ □, □[x] is well founded if and only if x lies in the well founded part of (□, $<^\square$). From this it immediately follows that {x: □[x] is well founded} exists.

Let x □ □ and suppose □[x] is not well founded. Let x = x_0 □ x_1 □ x_2 ... lie in □. Then x = x_0 $>^□$ x_1 $>^□$ ..., and so x is not in the well founded part of (□, $<^□$).

Finally, let x □ □ and suppose x is not in the well founded part of (□, $<^□$). Let x = x_0 $>^□$ x_1 $>^□$ ... . We prove by induction on k ≥ 1 that the k-th terms of the x's are eventually constant. The argument is well known, and makes heavy use of ACA_0, which is available to us. QED

3. MAXIMAL NONFINITELY GENERATED ALGEBRAS.

We are now prepared to treat 1.1 from the point of view of reverse mathematics.

We caution the reader that it cannot be proved in RCA_0 that the subalgebra generated by finitely many elements exists. In fact, we have the following.

THEOREM 3.1. The following are provably equivalent over RCA_0.
i) ACA_0;
ii) In every countable algebra, the subalgebra generated by finitely many elements exists;
iii) In every F:ℕ → ℕ there exists n such that the subalgebra generated by n exists.

Proof: i) → ii) → iii) is immediate. Assume iii), and let F:$ℕ^2$ → $ℕ^2$. (We have switched domains from ℕ to $ℕ^2$). Also let g:ℕ\{0} → ℕ\{0} be one-one. It suffices to prove that rng(g) exists.

Define F(n,m) as follows.

case 1. n > 0, ¬(∃k ≤ m)(g(n) = m). Set F(n,m) = (n,m+1).

case 2. n > 0, (∃k ≤ m)(g(n) = m). Set F(n,m) = (0,g^{-1}(n)).

case 3. n = 0, m > 0. Set F(n,m) = (g(m)+1, 0).

case 4. n = m = 0. Set F(n,m) = (1, 0).

Assume that the subalgebra generated by (p,q) exist. We now describe the orbit of F at (p,q). First assume p > 0. By case 1, we first repeatedly add 1 to q until case 2 applies, at which point we obtain (0,g^{-1}(p)) followed by (p+1,0). Then we repeatedly add 1 until we arrive at

$(p+1, g^{□1}(p+1)), (0, g^{□1}(p+1)), (p+2, 0)$. We can prove in RCA_0 that for all $m \geq 0$, $(0,m)$ lies in the orbit of F at (p,q) if and only if m is a value of g on [p,). Hence rng(g) exists.

Now assume $p = 0$, $q > 0$. By case 3, we obtain $(g(q)+1, 0)$. By the previous paragraph, we see that for all $m \geq 0$, $(0,m)$ lies in the orbit of F at (p,q if and only if m is a value of g on [p,) or m = q. Hence again rng(g) exists.

Finally assume $p = q = 0$. Then for all $m \geq 0$, $(0,m)$ lies in the orbit of F at (p,q) if and only if m is a value of g. Hence rng(g) exists. QED

THEOREM 3.2. The following are provably equivalent over RCA_0.
i) Theorem 1.1 for a single binary function from □ into □;
ii) $□^1_1$-CA_0.

Proof: ii) □ i) is from Lemma 1.2. Now assume i).

By Theorem 2.14, it suffices to prove that the tail well founded part of every linear ordering on □ exists.

Let <□ be a linear ordering on □. We will prove that the tail well founded part of <□ exists. We can assume without loss of generality that <□ is not tail well founded.

We define a function $f:□^2$ □ □ as follows. Let n,m □ □.

case 1. n = m. Define f(n,m) to be the numerically least r such that n <□ r if it exists; n otherwise.

case 2. n <□ m. Define f(n,m) to be the numerically least r > m such that n <□ r if it exists; n otherwise.

case 3. n >□ m. Define f(n,m) = f(m,n).

Let $n \geq 0$. By case 1, n generates the numerically least r such that n <□ r, if it exists. Then repeated applications of case 2 generate all of the r such that r ≥□ n.

We now claim that every nonempty subalgebra is a tail. To see this, let n be in the subalgebra and r ≥□ n. By the previous paragraph, r lies in the subalgebra.

We also claim that every tail is a subalgebra. This is clear by inspecting cases 1 - 3 above.

We next claim that a nonempty subalgebra is finitely generated if and only if it has a <□ least element. Suppose the subalgebra has a least element n. Then n generates the subalgebra, and so it is finitely generated. Conversely, suppose the subalgebra has a finite set □ of generators. By an obvious induction argument on terms, every element of the subalgebra is ≥□ min(□), where the min refers to <□. Hence min(□) is its least element.

Since there are nonempty tails in <□ with no <□ least element, we see that there exists a nonfinitely generated subalgebra.

By hypothesis, let □ be a maximal nonfinitely generated subalgebra. It suffices to prove that □ is the non tail well founded part of <□.

Let n □ □. Note that □ is a tail with no <□ least element, with elements <□ n. Hence □ up to n is a tail up to n with no <□ least element. Therefore <□ is not tail well founded up to n.

Conversely, suppose <□ is not tail well founded up to n. Let □ be a nonempty tail up to n with no least element. Then $□^□$ = □ □ {m ≥□ n} is a nonempty tail with no least element, and so $□^□$ is a subalgebra. In fact, it is a nonfinitely generated subalgebra. Hence $□^□$ □ □. Therefore n □ □. QED

The Cartesian square of a set □ is the set $□^2$.

THEOREM 3.3. The following are provably equivalent over RCA_0.
i) 1.1 for two unary functions from □ into □;
ii) $□^1_1$-CA_0.

Proof: As in the proof of Theorem 3.2, it suffices to prove that the tail well founded part of every linear ordering on □ exists.

Let <□ be a linear ordering on □. We prove that the tail well founded part of <□ exists. We can assume without loss of generality that <□ is not tail well founded.

It will be convenient to shift the domain to $□^2$. We define f,g:$□^2$ □ $□^2$ as follows. Let n,m □ □.

case 1. n = m. Let r be the numerically least r such that n <□ r if it exists; n otherwise. Define f(n,m) = (n,r), and g(n,m) = (r,r).

case 2. n <□m. Let r be the numerically least r > m such that n <□r if it exists; n otherwise. Define f(n,m) = (n,r), and g(n,m) = (m,n).

case 3. n >□m. Define f(n,m) = (n,n), g(n,m) = (m,m).

We first claim that the Cartesian square of any tail in <□is a subalgebra of (□^{2},f,g). This is clear by examining cases 1 - 3 above.

Now let □ be a subalgebra and (n,m) □ □. We secondly claim that if p,q ≥□min(n,m) then (p,q) is generated from the single element (n,m), where min refers to <□. To see this, first assume p,q ≥□n. We will obtain (p,q) from (n,m).

If n □□m then by case 2 for g we obtain (m,n), and then by case 3 for g we obtain (n,n). By case 1 for f and repeated applications of case 2 for f, we obtain (n,p),(n,q). By case 2 for g, we obtain (p,n),(p,n). By case 3 for f we obtain (p,p),(q,q). If p <□q then we obtain (p,q) using cases 1 and 2 for f. If q <□p then we obtain (q,p) using cases 1 and 2 for f, and then (p,q) using case 2 for g. If p = q then we already have (p,q).

If m <□n then by case 3 for g we obtain (m,m). By cases 1 and 2 for f we obtain (m,n). Note that p,q ≥□m and we have obtained (m,n). Hence we are in the case of the previous paragraph, and so (p,q) is obtained from (m,n), which is in turned obtained from (n,m).

We still have to prove this second claim under the assumption p,q ≥□m. If n □□m then p,q ≥□n, and we are done by the above. So we assume m <□n. By case 3, we obtain (m,m), and then by cases 1 and 2 for f, we obtain (m,n). Note that p,q ≥□ m, and so by the above (p,q) is obtained from (m,n), which is in turn obtained from (n,m). This establishes the second claim.

We thirdly claim that every nonempty subalgebra is the Cartesian square of its field, which is a tail. To see this, let □ be a nonempty subalgebra. By the second claim, fld(□) = {n: (n,n) □ □}. Suppose (n,n) □ □ and n □□m. By the second claim, (m,m) □ □, and so m □ fld(□). Hence fld(□) is a tail. Now let (p,p),(q,q) □ □, p □□ q. Then (p,p) □ □ and p,q ≥□ min(p,p). By claim 2, (p,q),(q,p) are obtained from (p,p). This establishes that □ = fld(□)^2.

We fourthly claim that every nonempty subalgebra is finitely generated if and only if its field has a <□ least element. Let □ be a nonempty subalgebra. Suppose fld(□) has the least element, n. Let (p,q) □ □. Then p,q ≥□ n and (n,n) □ □. Hence by the second claim, (p,q) is generated from (n,n). I.e., (n,n) generates all of □. Conversely, let □ be a finite set of generators for □. Let r be the <□ least element of fld(□). It is clear by induction that every coordinate of every pair generated from □ is ≥□ r. I.e., every element of fld(□) is ≥□ r. Since r □ fld(□), r is the <□ least element of fld(□).

We fifthly claim that there is a nonfinitely generated subalgebra. Recall that <□ has a nonempty tail □ with no <□ least element. By the first claim, □^{2} is a subalgebra, and by the fourth claim, □^{2} is nonfinitely generated.

By hypothesis, we now let □ be a maximal nonfinitely generated subalgebra. We claim that fld(□) is the non tail well founded part of <□ To see this, first note that □ is nonempty by the first claim.

By the fourth claim, fld(□) is a nonempty tail with no least element. Then for all n □ fld(□), <□ up to n is not tail well founded.

On the other hand, let <□ be not tail well founded up to n. Let D be a tail in <□ including n, with no least element. By the first claim, D^2 is a nonfinitely generated subalgebra. Hence D^2 □ fld(□)^2, or D □ fld(□). Therefore n □ fld(□). QED

THEOREM 3.4. Theorem 1.1 for a single unary function from a subset of □ into itself is provable in RCA_0.

Proof: It suffices to show in RCA_0 that if such an algebra is finitely generated then all subalgebras are finitely generated. From this it follows that if there is a nonfinitely generated subalgebra then the entire algebra is nonfinitely generated.

In RCA_0 we can assume without loss of generality that the domain of the given function is □. Let f:□ □ □ be finitely generated. Let $a_1,...,a_p$ be a set of generators. Let □ □ □ be a subalgebra of f. We wish to show that □ is finitely generated.

Let D = {i: 1 □ i □ p □ some iterate of f at a_i lies in □}. D exists as a finite set by [Si99], p. 71. We now define the function h:D □ □ by h(i) = the first iterate of f at a_i that lies in □. Then rng(h) is a finite set. We claim that rng(h) generates □. To see this, let m □ □. Then m is generated by f at some a_i. Fix i. Then m is generated by f at the first iterate of a_i. Hence m is generated from rng(h). QED

REFERENCES

[Si99] S. Simpson, Subsystems of Second Order Arithmetic, Perspectives in Mathematical Logic, Springer, 1999.

FOOTNOTE

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