THE JOURNAL OF SYMBOLIC LOGIC
Volume 53, Number 3, Sept. 1988

ORDINAL NUMBERS AND THE HILBERT BASIS THEOREM

STEPHEN G. SIMPSON

§1. Introduction. In [5] and [21] we studied countable algebra in the context of "reverse mathematics". We considered set existence axioms formulated in the language of second order arithmetic. We showed that many well-known theorems about countable fields, countable rings, countable abelian groups, etc. are equivalent to the respective set existence axioms which are needed to prove them.

One classical algebraic theorem which we did *not* consider in [5] and [21] is the Hilbert basis theorem. Let K be a field. For any natural number m, let $K[x_1, \ldots, x_m]$ be the ring of polynomials over K in m commuting indeterminates $x_1, \ldots, x_m$. The Hilbert basis theorem asserts that for all K and m, every ideal in the ring $K[x_1, \ldots, x_m]$ is finitely generated. This theorem is of fundamental importance for invariant theory and for algebraic geometry. There is also a generalization, the Robson basis theorem [11], which makes a similar but more restrictive assertion about the ring $K\langle x_1, \ldots, x_m \rangle$ of polynomials over K in m *noncommuting* indeterminates.

In this paper we study a certain formal version of the Hilbert basis theorem within the language of second order arithmetic. Our main result is that, for any or all countable fields K, our version of the Hilbert basis theorem is equivalent to the assertion that the ordinal number ω^ω is well ordered. (The equivalence is provable in the weak base theory RCA_0.) Thus the ordinal number ω^ω is a measure of the "intrinsic logical strength" of the Hilbert basis theorem. Such a measure is of interest in reference to the historic controversy surrounding the Hilbert basis theorem's apparent lack of constructive or computational content. Recall Gordan's famous remark: "That is not mathematics, that is theology!" (See Bell [1] and Noether [8].)

We also prove that the analogous formal version of the Robson basis theorem is equivalent to the assertion that the ordinal number ω^{ω^ω} is well ordered. (Again the equivalence is provable in RCA_0.) Thus the "intrinsic logical strength" of the Robson basis theorem is strictly and measurably greater than that of the Hilbert basis theorem.

The plan of this paper is as follows. In §2 we give the precise statements of our main results relating basis theorems to ordinal numbers. In §3 the main results are proved using several definitions and lemmas related to the theory of well partial orderings. The proofs of three of those lemmas are postponed to §4.

Received September 25, 1986; revised May 29, 1987.

0022-4812/88/5303-0021/$02.40

This research was partially supported by NSF grant MCS-8317874. I would like to thank my colleague Edward Formanek for bringing Robson's papers [10] and [11] to my attention.

§2. Hilbertian and Robsonian rings within RCA_0. Recall that RCA_0 is the subsystem of second order arithmetic with Σ_1^0 induction and Δ_1^0 comprehension. The reader is assumed to be familiar with RCA_0 and to have at least some acquaintance with the technique of formalizing mathematics within RCA_0. Roughly speaking, the mathematical content of RCA_0 is similar to the positive content of recursive mathematics. The biggest difference is that RCA_0 allows only a very restricted form of induction on the natural numbers, while recursive mathematics allows unrestricted induction. For basic information about RCA_0, see [5], [17], [20], and [21].

Most of the definitions and arguments of this paper are meant to be formalized within RCA_0. Within RCA_0 we use $\mathbf{N}$ to denote the set of all natural numbers. (If we are working within a non-ω-model of RCA_0, then $\mathbf{N}$ includes the nonstandard integers.) We use $i, j, k, l, m, n, \ldots$ as variables ranging over elements of $\mathbf{N}$.

As in [5] and [21], a *countable commutative ring* R is defined within RCA_0 to consist of a set $|R| \subseteq \mathbf{N}$ together with binary operations

$$+_R, \cdot_R \colon |R| \times |R| \to |R|,$$

a unary operation $-_R\colon |R| \to |R|$, and distinguished elements $0_R, 1_R \in |R|$ satisfying the usual commutative ring axioms, including $0 \neq 1$. We routinely write R instead of $|R|$ and employ the usual notation of modern algebra. (Also within RCA_0 we can similarly define the notions of countable field, countable ring, countable partial ordering, etc.)

Within RCA_0 we can prove that for any countable field K and any $m \in \mathbf{N}$, there exists a countable commutative ring $K[x_1, \ldots, x_m]$ consisting of 0 plus all (Gödel numbers of) expressions of the form

$$f(x_1, \ldots, x_m) = \sum_{i_1 + \cdots + i_m \leq n} a_{i_1 \cdots i_m} x_1^{i_1} \cdots x_m^{i_m},$$

where $\langle i_1, \ldots, i_m\rangle \in \mathbf{N}^m$, $m \in \mathbf{N}$, $a_{i_1 \cdots i_m} \in K$, and $a_{i_1 \cdots i_m} \neq 0$ for at least one $\langle i_1, \ldots, i_m\rangle \in \mathbf{N}^m$ with $i_1 + \cdots + i_m = n$. This is the ring of *polynomials in* m *commuting indeterminates* $x_1, \ldots, x_m$ *over* K.

2.1. Definition. Within RCA_0, let R be a countable commutative ring. We say that R is *Hilbertian* if for every sequence $\langle r_k \colon k \in \mathbf{N}\rangle$ of elements of R, there exists $k \in \mathbf{N}$ such that for all $j \in \mathbf{N}$ there exist $s_0, \ldots, s_k \in R$ such that $r_j = \sum_{i \leq k} r_i \cdot s_i$.

2.2. Remark. There is a subsystem of second order arithmetic known as ACA_0 which is somewhat stronger than RCA_0. (See [5], [17], and [20].) Within ACA_0, it is not hard to show that a countable ring R is Hilbertian if and only if every ideal of R is finitely generated. (An *ideal* of R is a set $I \subseteq R$ such that $0 \in R$, $1 \notin R$, $r_1 + r_2 \in I$ for all $r_1, r_2 \in I$, and $r \cdot s \in I$ for all $r \in I$ and $s \in R$.) In RCA_0 however, the assertion that R is Hilbertian seems to be a little stronger than the assertion that every ideal of R is finitely generated. We may explain the distinction as follows. As in [5] and [17], define a Σ_1^0 *ideal* of R to be a sequence $\langle r_k \colon k \in \mathbf{N}\rangle$ such that (1) $r_k \in R$ and $r_k \neq 1$ for all $k \in \mathbf{N}$; (2) for all $i, j \in \mathbf{N}$ there exists $k \in \mathbf{N}$ such that $r_i + r_j = r_k$; and (3) for all $i \in \mathbf{N}$ and $s \in R$ there exists $j \in \mathbf{N}$ such that $r_i \cdot s = r_j$. Within RCA_0, the notion of a Σ_1^0 ideal of R is more general than the notion of an ideal of R. It is not hard to show within RCA_0 that R is Hilbertian if and only if every Σ_1^0 ideal of R is finitely generated.

In our main result (Theorem 2.7 below), it would be possible to replace "$K[x_1, \ldots, x_m]$ is Hilbertian" by "every ideal of $K[x_1, \ldots, x_m]$ is finitely generated". We have chosen to emphasize the Hilbertian property, mainly because it seems to be more useful in applications to algebraic geometry, etc. In addition, most of the work of proving our main result goes into showing that the well orderedness of ω^ω *implies* Hilbertianness of $K[x_1, \ldots, x_m]$ for all $m \in \mathbf{N}$. Thus our use of the Hilbertian property leads to a more definitive result.

We now discuss ordinal notations.

2.3. DEFINITION. We define the set E of *notations for ordinals less than* ε_0, and the ordering $<$ of these notations. The definition is given by the following inductive clauses.

1. If $\alpha_1 \geq \cdots \geq \alpha_m$ belong to E, then $\omega^{\alpha_1} + \cdots + \omega^{\alpha_m}$ belongs to E.
2. If $\alpha_1 \geq \cdots \geq \alpha_m$ and $\beta_1 \geq \cdots \geq \beta_n$ belong to E, then

$$\omega^{\alpha_1} + \cdots + \omega^{\alpha_m} < \omega^{\beta_1} + \cdots + \omega^{\beta_n}$$

if and only if either (a) $m < n$ and $\alpha_1 = \beta_1, \ldots, \alpha_m = \beta_m$; or (b) $\alpha_1 = \beta_1, \ldots, \alpha_k = \beta_k$, $\alpha_{k+1} < \beta_{k+1}$ for some $k < \min(m, n)$.

We use $\alpha, \beta, \gamma, \ldots$ to denote elements of E, and we refer to such elements as *ordinals less than* ε_0. We sometimes identify $\beta < \varepsilon_0$ with the set of its predecessors, i.e. $\beta = \{\alpha : \alpha < \beta\}$. We use 0 to denote the element of E which is the empty sum, i.e. $0 = \omega^{\alpha_1} + \cdots + \omega^{\alpha_m}$ where $m = 0$. We also write $1 = \omega^0$ and $\omega = \omega^1$. We identify $m \in \mathbf{N}$ with the element of E which is the sum of m ones, i.e., $m = 1 + \cdots + 1$ (m times).

2.4. PROPOSITION. *The following facts are provable within* RCA_0.

1. *The set* $E = \{\alpha : \alpha < \varepsilon_0\}$ *exists.*
2. *The binary relation* $<$ *exists and is a linear ordering of* E.
3. $0 \leq \alpha$ *for all* α.
4. $\alpha + 1$ *is the immediate successor of* α.
5. $\alpha < \omega$ *if and only if* $\alpha = m$ *for some* $m \in \mathbf{N}$.
6. $\alpha < \omega^\omega$ *if and only if* $\alpha < \omega^m$ *for some* $m \in \mathbf{N}$.
7. $\alpha < \omega^{\omega^\omega}$ *if and only if* $\alpha < \omega^{\omega^m}$ *for some* $m \in \mathbf{N}$.

PROOF. Within RCA_0 we can prove that the universe of all total number-theoretic functions is closed under composition, primitive recursion, and minimalization. (See §2 of [20] or Chapter II of [17].) Thus the usual proof that E and $<$ are primitive recursive can be imitated to show within RCA_0 that these sets exist. The rest of the lemma is straightforward.

(Generalizing parts 5, 6 and 7 of the above proposition, we may note that RCA_0 proves the following. *For any* $\alpha < \varepsilon_0$ *and limit ordinal* $\beta < \varepsilon_0$, $\alpha < \beta$ *if and only if* $\alpha < \beta[m]$ *for some* $m \in \mathbf{N}$. Here $\langle \beta[m] : m \in \mathbf{N} \rangle$ is the standard fundamental sequence for β, as defined for instance in Buchholz and Wainer [2].)

2.5. DEFINITION. Within RCA_0 we make the following definitions. A *descending sequence through* ε_0 is a function $f : \mathbf{N} \to \{\alpha : \alpha < \varepsilon_0\}$ such that $f(k + 1) < f(k)$ for all

$k \in \mathbf{N}$. We say that ε_0 *is well ordered*, abbreviated $\mathrm{WO}(\varepsilon_0)$, if there is no descending sequence through ε_0. We say that $\alpha < \varepsilon_0$ *is well ordered*, abbreviated $\mathrm{WO}(\alpha)$, if there is no descending sequence through ε_0 beginning with α.

From Gentzen's work, it is well known that ACA_0 does not prove $\mathrm{WO}(\varepsilon_0)$, but that, for each (standard) $\alpha < \varepsilon_0$, ACA_0 proves $\mathrm{WO}(\alpha)$. In the case of the weaker system RCA_0, we have the following.

2.6. PROPOSITION. 1. *For each (standard) natural number m,* RCA_0 *proves* $\mathrm{WO}(\omega^m)$.

2. RCA_0 *does not prove* $\mathrm{WO}(\omega^\omega)$.

3. RCA_0 *proves*: $\mathrm{WO}(\omega^\omega)$ *if and only if* $\mathrm{WO}(\omega^m)$ *for all* $m \in \mathbf{N}$.

4. RCA_0 *proves*: $\mathrm{WO}(\omega^{\omega^\omega})$ *if and only if* $\mathrm{WO}(\omega^{\omega^m})$ *for all* $m \in \mathbf{N}$.

PROOF. Part 1 is straightforward.

Part 2 is a consequence of the following result which is essentially due to Parsons [9] (although Parsons did not consider the system RCA_0). *The provably total recursive functions of* RCA_0 *are just the primitive recursive functions.* If $\mathrm{WO}(\omega^\omega)$ were provable in RCA_0, we could use this to show that the Ackermann function is a provably total recursive function of RCA_0, contradicting Parsons' result. (For a Gentzen-style proof of Parsons' result, see Sieg [14]. For a model-theoretic proof, see Chapter IX of Simpson [17].)

Parts 3 and 4 follow immediately from parts 6 and 7 of Proposition 2.4. (More generally, RCA_0 *proves*: *for any limit ordinal* $\beta < \varepsilon_0$, $\mathrm{WO}(\beta)$ *if and only if* $\mathrm{WO}(\beta[m])$ *for all* $m \in \mathbf{N}$. This is an immediate consequence of the parenthetical remark following the proof of Proposition 2.4.)

The following theorem is the main result of this paper.

2.7. THEOREM. *Within* RCA_0 *it is provable that the following assertions are pairwise equivalent.*

1. *For all* $m \in \mathbf{N}$ *and all countable fields K, the commutative ring* $K[x_1, \ldots, x_m]$ *is Hilbertian. (This is our formal version of the Hilbert basis theorem.)*

2. *For each* $m \in \mathbf{N}$, *there exists a countable field K such that the commutative ring* $K[x_1, \ldots, x_m]$ *is Hilbertian.*

3. $\mathrm{WO}(\omega^\omega)$, *i.e. the ordinal number* ω^ω *is well ordered.*

This theorem will be proved in §§3 and 4.

We now discuss Robson's noncommutative generalization of the Hilbert basis theorem.

Within RCA_0 we make the following definitions. Given $m \in \mathbf{N}$, let $x_1, \ldots, x_m$ be m noncommuting indeterminates. We use $W_m = \{x_1, \ldots, x_m\}^* = \{x_1, \ldots, x_m\}^{<\omega}$ to denote the set of monomials in $x_1, \ldots, x_m$. Another way to view W_m is as the free monoid generated by $x_1, \ldots, x_m$. (A *monoid* is a semigroup with a distinguished identity element.) Yet another way to view W_m is as the set of all finite sequences of elements of the set $\{x_1, \ldots, x_m\}$ (including the empty sequence). This is referred to in computer science as the set of *words* on the *alphabet* $x_1, \ldots, x_m$ (including the empty word).

For all $w \in W_m$ we write $|w| =$ the *length* of w. A typical element of W_m is a formal product $w = x_{i_1} \cdots x_{i_l}$, and in this case we have $|w| = l$.

Within RCA_0 we can prove that, for all countable fields K and all $m \in \mathbf{N}$, there exists a ring $K\langle x_1, \ldots, x_m \rangle$ consisting of 0 plus all (Gödel numbers of) expressions of the form $f = \sum_{|u| \leq n} a_u u$, where $n \in \mathbf{N}$, $u \in W_m$, $a_u \in K$, and $a_u \neq 0$ for at least one u with $|u| = n$. Thus $K\langle x_1, \ldots, x_m \rangle$ is the ring of polynomials over K in m noncommuting indeterminates $x_1, \ldots, x_m$.

A polynomial $h \in K\langle x_1, \ldots, x_m \rangle$ is said to be *homogeneous of degree* l if it is nonzero and of the form

$$h = \sum_{|w| = l} c_w w \tag{1}$$

where $w \in W_m$ and $c_w \in K$. In this case we write $|h| = l$.

If $w \in W_m$ is of length l, say $w = x_{i_1} \cdots x_{i_l}$, then for any $u_0, u_1, \ldots, u_l \in W_m$ we write

$$w[u_0, \ldots, u_l] = u_0 x_{i_1} u_1 \cdots x_{i_l} u_l.$$

If $h \in K\langle x_1, \ldots, x_m \rangle$ is homogeneous of degree l as in (1) above, then we write

$$h[u_0, \ldots, u_l] = \sum_{|w| = l} c_w w[u_0, \ldots, u_l].$$

Thus $|h[u_0, \ldots, u_l]| = |u_0| + \cdots + |u_l| + l$.

An ideal is said to be *homogeneous* if it is generated by its homogeneous elements. A homogeneous ideal I of $K\langle x_1, \ldots, x_m \rangle$ is said to be *insertive* if for all $l \in \mathbf{N}$ and all homogeneous polynomials h of degree l, $h \in I$ implies $h[u_0, \ldots, u_l] \in I$ for all $u_0, \ldots, u_l \in W_m$. The *Robson basis theorem* (cf. Theorem 3.15 of [11]) asserts that for any field K and any $m \in \mathbf{N}$, every insertive homogeneous ideal of $K\langle x_1, \ldots, x_m \rangle$ is finitely generated *qua* insertive homogeneous ideal. We shall consider a slightly different, but equivalent, formulation. (Compare Remark 2.2 above.)

2.8. Definition. Within RCA_0 we make the following definition. Let K be a countable field. For $m \in \mathbf{N}$, we say that $K\langle x_1, \ldots, x_m \rangle$ is *Robsonian* if, for every sequence $\langle h_k : k \in \mathbf{N} \rangle$ of homogeneous elements of $K\langle x_1, \ldots, x_m \rangle$, there exists $k \in \mathbf{N}$ such that for all $j \in \mathbf{N}$ we have

$$h_j = \sum_{i \leq k} \sum_{|u_0| + \cdots + |u_{l_i}| + l_i = l_j} a_{i, u_0, \ldots, u_{l_i}} h_i[u_0, \ldots, u_{l_i}]$$

for some $a_{i, u_0, \ldots, u_{l_i}} \in K$, where $l_k = |h_k|$ for all $k \in \mathbf{N}$.

The second main result of this paper is as follows.

2.9. Theorem. *Within* RCA_0 *it is provable that the following assertions are pairwise equivalent.*

1. *For all countable fields and all* $m \in \mathbf{N}$, *the ring* $K\langle x_1, \ldots, x_m \rangle$ *is Robsonian. (This is our formal version of the Robson basis theorem.)*
2. *For each* $m \in \mathbf{N}$, *there exists a countable field* K *such that the ring* $K\langle x_1, \ldots, x_m \rangle$ *is Robsonian.*
3. $\mathrm{WO}(\omega^{\omega^\omega})$, *i.e. the ordinal number* ω^{ω^ω} *is well ordered.*

This theorem will be proved in §§3 and 4 along with Theorem 2.7.

§3. Well partial orderings. The purpose of this section is to prove the main results of the previous section, Theorems 2.7 and 2.9. In order to do so, we need to discuss certain aspects of the theory of well partial orderings, within RCA_0. Our discussion is self-contained. For general background on well partial orderings, the reader may consult [3], [4], [11], [12], [13], [15], [19], and [22].

Within RCA_0 we make the following definitions. A *countable partial ordering* A consists of a set $|A| \subseteq \mathbf{N}$ together with a binary relation $\leq_A \subseteq |A| \times |A|$ which is reflexive ($a \leq_A a$ for all $a \in |A|$), transitive ($a \leq_A a'$ and $a' \leq_A a''$ imply $a \leq_A a''$) and antisymmetric ($a \leq_A a'$ and $a' \leq_A a$ imply $a = a'$). We usually write A instead of $|A|$ and $\leq$ instead of $\leq_A$.

3.1. DEFINITION (RCA_0). A countable partial ordering A is said to be *well partially ordered* if, for all infinite sequences $\langle a_k : k \in \mathbf{N}\rangle$ of elements $a_k \in A$, there exist i and j such that $i < j$ and $a_i \leq a_j$.

3.2. LEMMA. *The following is provable in* RCA_0. *For any countable partial ordering A, the following assertions are equivalent.*

1. *A is well partially ordered.*
2. *For all infinite sequences $\langle a_k : k \in \mathbf{N}\rangle$ of elements $a_k \in A$, there exists k such that for all j there exists $i \leq k$ such that $a_i \leq a_j$.*

PROOF. We reason within RCA_0. The implication from 2 to 1 is trivial (take $j = k + 1$). We prove the implication from 1 to 2.

Assume that A is well partially ordered. Let $\langle a_k : k \in \mathbf{N}\rangle$, $a_k \in A$, be given. By recursive comprehension, let X be the set of all $j \in \mathbf{N}$ such that $\sim \exists i (i < j \wedge a_i \leq a_j)$.

We claim that $\forall j\, \exists i (i \in X \wedge a_i \leq a_j)$. Suppose not. Let j be such that $\forall i (a_i \leq a_j \rightarrow i \notin X)$. By recursion on k we shall define an infinite sequence of natural numbers $\langle i_k : k \in \mathbf{N}\rangle$. We begin by putting $i_0 = j$. Assume inductively that $a_{i_k} \leq a_j$. Then $i_k \notin X$, so we can find $i_{k+1} < i_k$ such that $a_{i_{k+1}} \leq a_{i_k} \leq a_j$. Thus $\langle i_k : k \in \mathbf{N}\rangle$ is an infinite descending sequence of natural numbers. This contradiction proves our claim.

We claim that X is finite. If not, let $\pi_X : \mathbf{N} \rightarrow X$ be the one-to-one function which enumerates the elements of X in increasing order. Consider the sequence $\langle a_{\pi_X(k)} : k \in \mathbf{N}\rangle$. Since A is well partially ordered, there exist i and j such that $i < j$ (hence $\pi_X(i) < \pi_X(j)$) and $a_{\pi_X(i)} \leq a_{\pi_X(j)}$. This contradicts the fact that $\pi_X(j) \in X$. Our claim is proved.

Since X is finite, let $k \in \mathbf{N}$ be an upper bound for X. Our first claim implies that $\forall j\, \exists i (i \leq k \wedge a_i \leq a_j)$. This completes the proof of Lemma 3.2.

3.3. DEFINITION (RCA_0). If $\langle A_i : 1 \leq i \leq m\rangle$ is a finite sequence of countable partial orderings, we can form the *m-fold Cartesian product*

$$A_1 \times \cdots \times A_m = \prod_{i=1}^{m} A_i = \{\langle a_1, \ldots, a_m\rangle : a_1, \ldots, a_m \in A\}.$$

This is again a countable partial ordering under the product relation: $\langle a_1, \ldots, a_m\rangle \leq \langle a'_1, \ldots, a'_m\rangle$ if and only if $a_1 \leq a'_1$ and ... and $a_m \leq a'_m$.

In particular, we have the m-fold Cartesian power $\mathbf{N}^m = \mathbf{N} \times \cdots \times \mathbf{N}$ (m factors), where $\mathbf{N}$ is the set of natural numbers with the usual ordering.

3.4. LEMMA. *The following is provable in* RCA_0. *For any $m \in \mathbf{N}$ and any countable field K, the following are equivalent.*

1. *The commutative ring $K[x_1, \ldots, x_m]$ is Hilbertian.*
2. *The m-fold Cartesian power $\mathbf{N}^m$ is well partially ordered.*

PROOF. We reason within RCA_0. Fix m and K.

Assume first that $K[x_1, \ldots, x_m]$ is Hilbertian. Let $\langle\langle e_{k1}, \ldots, e_{km}\rangle : k \in \mathbf{N}\rangle$ be an infinite sequence of elements of $\mathbf{N}^m$. For each $k \in \mathbf{N}$ define a monomial

$$M_k \quad = \quad x_1^{e_{k1}} \cdots x_m^{e_{km}} \quad \in \quad K[x_1, \ldots, x_m].$$

Since $K[x_1,\ldots,x_m]$ is Hilbertian, we have $\exists k \forall j\ M_j = g_0M_0 + \cdots + g_kM_k$ for some $g_0,\ldots,g_k \in K[x_1,\ldots,x_m]$. Take for instance $j = k + 1$. A simple cancellation argument shows that M_j is divisible by M_i for at least one $i \le k$. Thus $\langle e_{i1},\ldots,e_{im}\rangle \le \langle e_{j1},\ldots,e_{jm}\rangle$ in $\mathbf{N}^m$, and $i < j$. Since the sequence $\langle\langle e_{k1},\ldots,e_{km}\rangle: k \in \mathbf{N}\rangle$ is arbitrary, we see that $\mathbf{N}^m$ is well partially ordered. This proves that 1 implies 2.

For the converse implication, assume that $\mathbf{N}^m$ is well partially ordered. Let $\langle f_k: k \in \mathbf{N}\rangle$ be an infinite sequence of elements of $K[x_1,\ldots,x_m]$. Let $\varphi(h)$ be the Σ^0_1 formula which says that $h \in K[x_1,\ldots,x_m]$ and $h = f_0g_0 + \cdots + f_kg_k$ for some $k \in \mathbf{N}$ and $g_0,\ldots,g_k \in K[x_1,\ldots,x_m]$. Since $\varphi(h)$ is Σ^0_1, we can prove within RCA_0 that there exists a sequence $\langle h_k: k \in \mathbf{N}\rangle$ such that $\forall h\ (\varphi(h) \leftrightarrow \exists k\ (h = h_k))$. (See [20, Lemma 2.1].) Now for each $k \in \mathbf{N}$ let M_k be the *leading monomial* of h_k. This means that M_k is the lexicographically first monomial in h_k of highest total degree. Identify $M_m = x_1^{e_{k1}} \cdots x_m^{e_{km}}$ with the m-tuple $\langle e_{k1},\ldots,e_{km}\rangle \in \mathbf{N}^m$. Since $\mathbf{N}^m$ is well partially ordered, we see by Lemma 3.2 that there exists k such that for all j there exists $i \le k$ such that M_j is divisible by M_i.

Fix such a k. We claim that, for all j,

$$h_j = g_0h_0 + \cdots + g_kh_k \tag{2}$$

for some $g_0,\ldots,g_k \in K[x_1,\ldots,x_m]$. We shall prove this by induction on the ordering of leading monomials. Given j, let $i \le k$ be such that M_j is divisible by M_i, say $M_j = M_iN_j$ where N_j is another monomial. Then, for an appropriate constant $c_j \in K$, $h_j - c_jN_jh_i$ has a leading monomial which is prior to M_j in the ordering of leading monomials. Also $h_j - c_jN_jh_i = h_l$ for some $l \in \mathbf{N}$. Hence by the inductive hypothesis

$$h_j - c_jN_jh_i = g_0^*h_0 + \cdots + g_k^*h_k$$

for some $g_0^*,\ldots,g_k^* \in K[x_1,\ldots,x_m]$. Hence (2) holds with $g_i = g_i^* + c_jN_j$, and $g_l = g_l^*$ for all $l \le k$, $l \ne i$.

This completes the proof of Lemma 3.4.

3.5. Remark. The above proof that 3.4.2 implies 3.4.1 is similar to a proof of the Hilbert basis theorem which is due to Gordan [6], [7].

3.6. Lemma. *The following is provable in* RCA_0. *For any* $m \in \mathbf{N}$, *the following are equivalent.*

1. *The m-fold Cartesian power* $\mathbf{N}^m$ *is well partially ordered.*
2. *The ordinal* ω^m *is well ordered.*

The proof of this lemma will be presented in §4.

Proof of Theorem 2.7. The theorem follows immediately from Proposition 2.6.3 and Lemmas 3.4 and 3.6.

3.7. Definition (RCA_0). If A is a countable partial ordering, we can form the countable set A^* of all finite sequences of elements of A. We partially order A^* by putting $\langle a_i: i < k\rangle \le \langle b_j: j < l\rangle$ if and only if there exist $j_0 < \cdots < j_{k-1} < l$ such that $a_0 \le b_{j_0},\ldots,a_{k-1} \le b_{j_{k-1}}$. Thus A^* is a countable partial ordering.

In particular, taking $A = \{x_1,\ldots,x_m\}$ where $x_1,\ldots,x_m$ are noncommuting indeterminates, we have the set of monomials $W_m = \{x_1,\ldots,x_m\}^*$ as in §2. Using the notation of §2, we see that for all w and $w' \in W_m$, $w \le w'$ if and only if $w[u_0,\ldots,u_l] = w'$ for some $u_0,\ldots,u_l \in W_m$, where $l = |w|$.

3.8. LEMMA. *The following is provable in* RCA_0. *For any* $m \in \mathbf{N}$ *and any countable field* K, *the following assertions are equivalent.*

1. *The ring* $K\langle x_1, \ldots, x_m \rangle$ *is Robsonian.*
2. *The set of monomials* W_m *is well partially ordered.*

PROOF. We omit the proof, which is entirely analogous to the proof of Lemma 3.4 above.

3.9. LEMMA. *The following is provable in* RCA_0. *For all* $m \in \mathbf{N}$, *if the set of monomials* W_{m+1} *is well partially ordered, then the ordinal* ω^{ω^m} *is well ordered.*

3.10. LEMMA. *The following is provable in* RCA_0. *For all* $m \in \mathbf{N}$, *if the ordinal* $\omega^{\omega^{m+1}}$ *is well ordered, then the set of monomials* W_m *is well partially ordered.*

The proofs of the previous two lemmas will be presented in §4.

PROOF OF THEOREM 2.9. The theorem follows immediately from Proposition 2.6.4 and Lemmas 3.8, 3.9 and 3.10.

§4. Effective reification. The purpose of this section is to complete the arguments of §3 by proving Lemmas 3.6, 3.9 and 3.10. Two of the proofs are based on the notion of *reification* which is defined below.

The following definitions are made within RCA_0. Let A be a countable partial ordering. A finite sequence $s = \langle a_i : i < k \rangle$ of elements $a_i \in A$ is said to be *bad* if there do not exist i and j such that $i < j < k$ and $a_i \leq a_j$. In this case we write

$$\begin{aligned} A_s &= \{a \in A : a_i \not\leq a \text{ for all } i < k\} \\ &= \{a \in A : s^\frown\langle a \rangle \text{ is bad}\}. \end{aligned}$$

For any $a \in A_s$ we write

$$A_s(a) = A_{s^\frown\langle a \rangle} = \{b \in A_s : a \not\leq b\}.$$

The countable set consisting of all bad finite sequences of elements of A is denoted $\mathrm{Bad}(A)$. Note that the existence of $\mathrm{Bad}(A)$ is provable in RCA_0.

4.1. DEFINITION (RCA_0). Let A be a countable partial ordering. For $\alpha < \varepsilon_0$, a *reification of* A *by* α is a mapping $f: \mathrm{Bad}(A) \to \alpha + 1$ such that $f(s^\frown\langle a \rangle) < f(s)$ for all $s \in \mathrm{Bad}(A)$ and $a \in A_s$.

4.2. LEMMA. *The following is provable in* RCA_0. *Let* A *be a countable partial ordering. If there exists a reification of* A *by* α, *and if* α *is well ordered, then* A *is well partially ordered.*

PROOF. We reason within RCA_0. Let $f: \mathrm{Bad}(A) \to \alpha + 1$ be a reification of A by α. Suppose that A is not well partially ordered. Then there exists an infinite sequence $\langle a_k : k \in \mathbf{N} \rangle$ of elements $a_k \in A$ which is *bad*, i.e. there do not exist $i, j \in \mathbf{N}$ such that $i < j$ and $a_i \leq a_j$. For each $k \in \mathbf{N}$ put $\alpha_k = f(\langle a_i : i < k \rangle)$. Then $\langle \alpha_k : k \in \mathbf{N} \rangle$ is an infinite descending sequence of ordinals less than or equal to α. This contradicts the assumption that α is well ordered. Our lemma is proved.

4.3. REMARK. A large part of the work in this section is devoted to finding explicit, effectively given reifications of the well partial orderings which were considered in §3. Our treatment of reification is self-contained. For general background on reification, the reader may consult DeJongh and Parikh [3], Schmidt [12], and Statman [22].

We shall make use of the following definition and lemma.

4.4. DEFINITION. Within RCA_0 we define the *natural sum* of ordinals less than ε_0 by

$$(\omega^{\alpha_1} + \cdots + \omega^{\alpha_m}) + (\omega^{\beta_1} + \cdots + \omega^{\beta_n}) = \omega^{\gamma_1} + \cdots + \omega^{\gamma_{m+n}}$$

where $\langle \gamma_1, \ldots, \gamma_{m+n} \rangle$ is a permutation of $\langle \alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n \rangle$ such that $\gamma_1 \geq \cdots \geq \gamma_{m+n}$. The *natural product* is defined by

$$(\omega^{\alpha_1} + \cdots + \omega^{\alpha_m}) \times (\omega^{\beta_1} + \cdots + \omega^{\beta_n}) = \omega^{\alpha_1 + \beta_1} + \cdots + \omega^{\alpha_i + \beta_j} + \cdots + \omega^{\alpha_m + \beta_n}$$

where $i = 1, \ldots, m$ and $j = 1, \ldots, n$. Note that in this paper we use $+$ and $\times$ exclusively to denote the natural sum and natural product.

4.5. LEMMA. *The following facts are provable within* RCA_0.

1. $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$.
2. $\alpha + \beta = \beta + \alpha$.
3. $\alpha + \beta_1 < \alpha + \beta_2$ *if and only if* $\beta_1 < \beta_2$.
4. ω^γ *is **additively indecomposable**, i.e.* $\alpha < \omega^\gamma$ *and* $\beta < \omega^\gamma$ *imply* $\alpha + \beta < \omega^\gamma$.
5. $(\alpha \times \beta) \times \gamma = \alpha \times (\beta \times \gamma)$.
6. $\alpha \times \beta = \beta \times \alpha$.
7. $\alpha \times \beta_1 < \alpha \times \beta_2$ *if and only if* $\beta_1 < \beta_2$.
8. $(\alpha + \beta) \times \gamma = (\alpha \times \gamma) + (\beta \times \gamma)$.
9. ω^{ω^γ} *is **multiplicatively indecomposable**, i.e.* $\alpha < \omega^{\omega^\gamma}$ *and* $\beta < \omega^{\omega^\gamma}$ *imply* $\alpha \times \beta < \omega^{\omega^\gamma}$.

PROOF. The proof is straightforward.

We now prepare for the proof of Lemma 3.6.

For $u \leq v \leq \omega$ we write $[u, v) = \{a : u \leq a < v\}$. Given an m-fold Cartesian product $\prod_{i=1}^m [u_i, v_i)$ with $u_i \leq v_i \leq \omega$ for each i, we define

$$\left| \prod_{i=1}^m [u_i, v_i) \right| = \prod_{i=1}^m (v_i - u_i)$$

where on the right-hand side $\prod$ denotes natural product.

4.6. SUBLEMMA (RCA_0). *Suppose that* $\langle a_1, \ldots, a_m \rangle \in \prod_{i=1}^m [u_i, v_i)$ *where* $u_i \leq v_i \leq \omega$ *for each i. Then*

$$\sum_\sigma \left| \prod_{i=1}^m [u_i(\sigma), v_i(\sigma)) \right| < \left| \prod_{i=1}^m [u_i, v_i) \right|. \tag{3}$$

Here $\sum$ *denotes natural sum,* $\sigma = \langle \sigma_i : 1 \leq i \leq m \rangle$ *ranges over all m-tuples of zeros and ones which do not consist entirely of ones, and*

$$[u_i(\sigma), v_i(\sigma)) = \begin{cases} [u_i, a_i) & \text{if } \sigma_i = 0, \\ [a_i, v_i) & \text{if } \sigma_i = 1. \end{cases}$$

PROOF. We reason within RCA_0. Let k be the number of i's such that $v_i = \omega$. Suppose first that $k = 0$. In this case, the sublemma follows easily by observing that the disjoint union

$$\bigcup_\sigma \prod_{i=1}^m [u_i(\sigma), v_i(\sigma))$$

is a proper subset of the finite set $\prod_{i=1}^m [u_i, v_i)$.

Suppose now that $k > 0$. The right-hand side of (3) is of the form $\omega^k \times n$ where $n < \omega$. Let us say that σ is *wild* if $\sigma_i = 0$ for some i such that $v_i = \omega$; otherwise σ is *tame*. If σ is wild, the contribution of σ to the left-hand side of (3) is of the form $\omega^{k'} \times n'$, where $k' < k$ and $n' < \omega$. Hence, by Lemma 4.5.4, the total contribution of all the wild σ's is $< \omega^k$. On the other hand, the total contribution of all the tame σ's is of the form $\omega^k \times n''$ where $n'' < n$. (The inequality $n'' < n$ follows from the special case $k = 0$ which has already been proved.) Thus the total left-hand side is $< \omega^k + (\omega^k \times n'') \leq \omega^k \times n$. This completes the proof of Sublemma 4.6.

4.7. SUBLEMMA. *The following is provable in* RCA_0. *For each* $m \in \mathbf{N}$, *there exists a reification of* $\mathbf{N}^m$ *by* ω^m.

PROOF. We reason within RCA_0. Fix $m \in \mathbf{N}$. We shall define a reification $f\colon \mathrm{Bad}(\mathbf{N}^m) \to \omega^m + 1$. For $s \in \mathrm{Bad}(\mathbf{N}^m)$ we shall define $f(s) \leq \omega^m$ by primitive recursion on the length of s. (See [20, pp. 788–789].) The value of $f(s)$ will be obtained in terms of a decomposition of $(\mathbf{N}^m)_s$ into a disjoint union,

$$(\mathbf{N}^m)_s \subseteq \bigcup_{j \in J} \prod_{i=1}^{m} [u_{ij}, v_{ij}), \tag{4}$$

where J is a finite index set and $u_{ij} \leq v_{ij} \leq \omega$ for all $j \in J$ and $i = 1, \ldots, m$. We shall then define

$$f(s) = \sum_{j \in J} \left| \prod_{i=1}^{m} [u_{ij}, v_{ij}) \right|.$$

We begin with the trivial decomposition $(\mathbf{N}^m)_{\langle\ \rangle} = \mathbf{N}^m = \prod_{i=1}^m [0, \omega)$, and accordingly we define

$$f(\langle\ \rangle) = \left| \prod_{i=1}^{m} [0, \omega) \right| = \omega^m.$$

Now fix $s \in \mathrm{Bad}(\mathbf{N}^m)$ and assume inductively that we have already defined $f(s)$ according to a decomposition (4) of $(\mathbf{N}^m)_s$. Given $s' = s^\frown\langle a \rangle \in \mathrm{Bad}(\mathbf{N}^m)$, we want to define $f(s')$. Since $a \in (\mathbf{N}^m)_s$, there is a unique $j' \in J$ such that $a = \langle a_1, \ldots, a_m \rangle \in \prod_{i=1}^m [u_{ij'}, v_{ij'})$. As our decomposition of $(\mathbf{N}^m)_{s'}$, we take (4) with $\prod_{i=1}^m [u_{ij'}, v_{ij'})$ replaced by

$$\bigcup_{\sigma} \prod_{i=1}^{m} [u_{ij'}(\sigma), v_{ij'}(\sigma))$$

as in Sublemma 4.6. It is easy to check that this provides a decomposition of $(\mathbf{N}^m)_{s'}$ as required. The fact that $f(s') < f(s)$ follows from Sublemma 4.6 and Lemma 4.5.4.

This completes the proof of Sublemma 4.7.

PROOF OF LEMMA 3.6. We reason within RCA_0. Fix $m \in \mathbf{N}$.

Assume first that ω^m is well ordered. By Sublemma 4.7 there exists a reification of $\mathbf{N}^m$ by ω^m. Hence by Lemma 4.2 it follows that $\mathbf{N}^m$ is well partially ordered. This proves half of our lemma.

For the other half, assume that $\mathbf{N}^m$ is well partially ordered. Define a mapping $g\colon \omega^m \to \mathbf{N}^m$ by $g(\sum_{i<m} a_i \times \omega^i) = \langle a_i : i < m \rangle$. Note that $g(\alpha) \leq g(\beta)$ implies $\alpha \leq \beta$. Now if ω^m is not well ordered, let $\langle \alpha_k : k \in \mathbf{N} \rangle$ be an infinite descending sequence of ordinals less than ω^m. Then $\langle g(\alpha_k): k \in \mathbf{N}\rangle$ is a sequence of elements of $\mathbf{N}^m$. Since by assumption $\mathbf{N}^m$ is well partially ordered, there exist i and j such that $i < j$ and $g(\alpha_i) \leq g(\alpha_j)$. It follows that $\alpha_i \leq \alpha_j$, a contradiction. This completes the proof of Lemma 3.6.

PROOF OF LEMMA 3.9. We reason within RCA_0. By recursion on $m \in \mathbf{N}$ we define mappings $\bar{g}_m: \omega^{\omega^m} \to W_{m+1}$ with the property that $\bar{g}_m(\alpha) \leq \bar{g}_m(\beta)$ implies $\alpha \leq \beta$. For $m = 0$, if $\alpha < \omega^{\omega^0} = \omega$, we put

$$\bar{g}_0(\alpha) \quad = \quad \underbrace{x_1 \cdots x_1}_{n} \quad \in \quad W_1$$

where $\alpha = n < \omega$. Trivially $\bar{g}_0(\alpha) \leq \bar{g}_0(\beta)$ implies $\alpha \leq \beta$.

Assume now that $\bar{g}_m$ has been defined. To define $\bar{g}_{m+1}$, let $\alpha < \omega^{\omega^{m+1}}$ be given. Let $k = k_\alpha$ be as small as possible such that $\alpha < \omega^{\omega^m \times k}$. Then we have

$$\alpha = \omega^{\omega^m \times (k-1)} \times \alpha_{k-1} + \cdots + \omega^{\omega^m} \times \alpha_1 + \alpha_0 \tag{5}$$

where $\alpha_{k-1}, \ldots, \alpha_1, \alpha_0$ are all less than ω^{ω^m}. Hence $\bar{g}_m(\alpha_{k-1}), \ldots, \bar{g}_m(\alpha_1), \bar{g}_m(\alpha_0) \in W_{m+1}$, and we define

$$\bar{g}_{m+1}(\alpha) \quad = \quad \bar{g}_m(\alpha_{k-1})x_{m+2} \cdots x_{m+2}\bar{g}_m(\alpha_1)x_{m+2}\bar{g}_m(\alpha_0) \quad \in \quad W_{m+2}. \tag{6}$$

We claim that $\bar{g}_{m+1}(\alpha) \leq \bar{g}_{m+1}(\beta)$ implies $\alpha \leq \beta$. Assume $\bar{g}_{m+1}(\alpha) \leq \bar{g}_{m+1}(\beta)$. Then obviously $k_\alpha \leq k_\beta$. If $k_\alpha < k_\beta$, then trivially $\alpha < \beta$. Otherwise, let $k = k_\alpha = k_\beta$. Thus we have (5) and (6), and similarly

$$\beta \quad = \quad \omega^{\omega^m \times (k-1)} \times \beta_{k-1} + \cdots + \omega^{\omega^m} \times \beta_1 + \beta_0$$

so that

$$\bar{g}_{m+1}(\beta) \quad = \quad \bar{g}_m(\beta_{k-1})x_{m+2} \cdots x_{m+2}\bar{g}_m(\beta_1)x_{m+2}\bar{g}_m(\beta_0) \quad \in \quad W_{m+2}.$$

From $\bar{g}_{m+1}(\alpha) \leq \bar{g}_{m+1}(\beta)$ and $k_\alpha = k_\beta = k$, it follows that $\bar{g}_m(\alpha_{k-1}) \leq \bar{g}_m(\beta_{k-1}), \ldots, \bar{g}_m(\alpha_1) \leq \bar{g}_m(\beta_1)$, $\bar{g}_m(\alpha_0) \leq \bar{g}_m(\beta_0)$. Therefore, by induction on m, we have $\alpha_{k-1} \leq \beta_{k-1}, \ldots, \alpha_1 \leq \beta_1$, $\alpha_0 \leq \beta_0$ and hence, by Lemma 4.5, $\alpha \leq \beta$. This proves the claim.

Now to prove the lemma, fix m and assume that W_{m+1} is well partially ordered. If ω^{ω^m} is not well ordered, let $\langle \alpha_k: k \in \mathbf{N}\rangle$ be an infinite descending sequence of ordinals less than ω^{ω^m}. Then $\langle \bar{g}_m(\alpha_k): k \in \mathbf{N}\rangle$ is a sequence of monomials in W_{m+1}. Since by assumption W_{m+1} is well partially ordered, there exist i and j such that $i < j$ and $\bar{g}_m(\alpha_i) \leq \bar{g}_m(\alpha_j)$; hence $\alpha_i \leq \alpha_j$, a contradiction.

This completes the proof of Lemma 3.9.

4.8. SUBLEMMA. *The following is provable in* RCA_0. *Let A be a countable partial ordering. If there exists a reification of A by α, then there exists a reification of A^* by $\omega^{\omega^{\alpha+1}}$.*

PROOF. The proof is essentially the same as the proof of Lemma 5.2 of [13]. Since that paper has not been translated into English, we repeat the proof here.

We reason within RCA_0. Let $f: \mathrm{Bad}(A) \to \alpha + 1$ be a reification of A by α. In terms of f we shall define a reification $f^*: \mathrm{Bad}(A^*) \to \omega^{\omega^{\alpha+1}} + 1$ of A^* by $\omega^{\omega^{\alpha+1}}$.

For each $t \in \mathrm{Bad}(A^*)$, in order to define $f^*(t) \leq \omega^{\omega^{\alpha+1}}$, we shall define a certain mapping

$$h_t\colon (A^*)_t \to C_t \tag{7}$$

where C_t is a certain countable partial ordering. The mapping h_t will have the property that $h_t(u) \leq h_t(v)$ implies $u \leq v$ for all $u, v \in (A^*)_t$. The countable partial ordering C_t will be of the form

$$C_t = \bigcup_{i \in I} \prod_{k \in K_i} B_{ik} \tag{8}$$

where I and the K_i, $i \in I$, are finite index sets, $\bigcup$ denotes finite disjoint union, $\prod$ denotes finite Cartesian product, and each B_{ik} is either A_s or $(A_s)^*$ for some $s \in \mathrm{Bad}(A)$. The *ordinal value* of any such countable partial ordering is defined in terms of f as follows: $|A_s| = \omega^{\omega^{f(s)}}$, $|(A_s)^*| = \omega^{\omega^{f(s)+1}}$, $|\prod_{k \in K} B_k| = \prod_{k \in K} |B_k|$ (natural product), and $|\bigcup_{i \in I} D_i| = \sum_{i \in I} |D_i|$ (natural sum). We then define $f^*(t) = |C_t|$ for each $t \in \mathrm{Bad}(A^*)$.

It remains to define the mappings h_t as in (7), for each $t \in \mathrm{Bad}(A^*)$. We shall do this by primitive recursion on the length of t. We begin by letting $h_{\langle\,\rangle}$ be the identity mapping of $(A^*)_{\langle\,\rangle} = A^*$ into $C_{\langle\,\rangle} = (A_{\langle\,\rangle})^* = A^*$. Thus we have

$$f(\langle\,\rangle) = |C_{\langle\,\rangle}| = |(A_{\langle\,\rangle})^*| = \omega^{\omega^{f(\langle\rangle)+1}} \leq \omega^{\omega^{\alpha+1}}.$$

Now let $t' = t^\frown\langle u\rangle \in \mathrm{Bad}(A^*)$ and assume that $h_t\colon (A^*)_t \to C_t$ and $f^*(t) = |C_t|$, with C_t as in (8), have already been defined. Our goal is to define $h_{t'}$. Since $u \in (A^*)_t$, we have $h_t(u) \in C_t$; hence $h_t(u) \in \prod_{k \in K_i} B_{ik}$ for a unique $i \in I$. Thus $h_t(u) = \langle c_k\colon k \in K_i\rangle$ where $c_k \in B_{ik}$ for each $k \in K_i$. For each

$$\langle d_k\colon k \in K_i\rangle \quad \in \quad D \quad = \quad \left(\prod_{k \in K_i} B_{ik}\right)(\langle c_k\colon k \in K_i\rangle),$$

we have $d_k \in B_{ik}$ for all $k \in K_i$, and $d_k \in B_{ik}(c_k)$ for at least one $k \in K_i$. Therefore, there is an obvious mapping of D into $\bigcup_{j \in K_i} \prod_{k \in K_i} B'_{jk}$, where $B'_{jk} = B_{ik}$ for $j \neq k$ and $B'_{kk} = B_{ik}(c_k)$.

We shall now define a mapping of B'_{jk} into another countable partial ordering B''_{jk}. We distinguish three cases.

Case 1. $j \neq k$. In this case we map $B'_{jk} = B_{ik}$ into $B''_{jk} = B'_{jk} = B_{ik}$ via the identity mapping.

Case 2. $j = k$, $B_{ik} = A_s$ with $s \in \mathrm{Bad}(A)$. In this case we have $c_k = a \in A_s$ and we map $B'_{kk} = B_{ik}(c_k) = A_s(a)$ into $B''_{kk} = A_s(a)$, via the identity mapping. Thus

$$|B''_{kk}| \quad = \quad |A_s(a)| \quad = \quad \omega^{\omega^{f(s^\frown\langle a\rangle)}} \quad < \quad \omega^{\omega^{f(s)}} \quad = \quad |A_s| \quad = \quad |B_{ik}|.$$

Case 3. $j = k$, $B_{ik} = (A_s)^*$ with $s \in \mathrm{Bad}(A)$. In this case we have $c_k = \langle a_l\colon l < n\rangle \in (A_s)^*$. For each $w \in B'_{kk} = B_{ik}(c_k) = (A_s)^*(\langle a_l\colon l < n\rangle)$, there is a smallest $m < n$ such that $\langle a_l\colon l \leq m\rangle \not\leq w$. Hence w is of the form

$$w \quad = \quad w_0{}^\frown\langle b_0\rangle^\frown \cdots {}^\frown w_{m-1}{}^\frown\langle b_{m-1}\rangle^\frown w_m$$

where $w_l \in A_s(a_l)^*$ and $b_l \in A_s$. Thus there is an obvious mapping of B'_{kk} into

$$B''_{kk} \quad = \quad \bigcup_{m<n} (A_s(a_0)^* \times A_s \times \cdots \times A_s(a_{m-1})^* \times A_s \times A_s(a_m)^*).$$

Note that $|A_s| = \omega^{\omega f(s)} < \omega^{\omega f(s)+1}$ and

$$|A_s(a_l)^*| \quad = \quad \omega^{\omega f(s\ \langle a_l\rangle)+1} \quad < \quad \omega^{\omega f(s)+1}.$$

Hence by additive and multiplicative indecomposability of $\omega^{\omega f(s)+1}$, we see that

$$|B''_{kk}| \quad < \quad \omega^{\omega f(s)+1} \quad = \quad |(A_s)^*| \quad = \quad |B_{ik}|.$$

We now let $C_{t'}$ be the countable partial ordering which results from (8) when we replace the term $\prod_{k\in K_i} B_{ik}$ by $\bigcup_{j\in K_i}\prod_{k\in K_i} B''_{jk}$ and distribute Cartesian products over disjoint unions. The mapping $h_{t'}\colon (A^*)_{t'} \to C_{t'}$ is defined as the composition of h_t with the other mappings which were mentioned above.

We now compute:

$$\left|\bigcup_{j\in K_i}\prod_{k\in K_i} B''_{jk}\right| = \sum_{j\in K_i}\prod_{k\in K_i} |B''_{jk}|$$

where on the right-hand side $\sum$ and $\prod$ denote natural sum and natural product. For all j and k we have $|B''_{jk}| \le |B_{ik}|$ and $|B''_{kk}| < |B_{ik}|$. Hence, for each $j \in K_i$, $\prod_{k\in K_i}|B''_{jk}| < \prod_{k\in K_i}|B_{ik}|$. By the additive indecomposability of $\prod_{k\in K_i}|B_{ik}|$, it follows that

$$\sum_{j\in K_i}\prod_{k\in K_i} |B''_{jk}| < \prod_{k\in K_i} |B_{ik}|.$$

This implies that $f^*(t') = |C_{t'}| < |C_t| = f^*(t)$. The proof of Sublemma 4.8 is complete.

PROOF OF LEMMA 3.10. We reason within RCA_0. Fix $m \in \mathbf{N}$ and assume that $\omega^{\omega^{m+1}}$ is well ordered. Let $A = \{x_1,\dots,x_m\}$ with the discrete ordering: $x_i \le x_j$ if and only if $i = j$. Thus $A^* = W_m$. There is an obvious reification of A by m (namely $f(s) = m -$ (length of s) for all $s \in \mathrm{Bad}(A)$). Hence Sublemma 4.8 provides a reification f^* of A^* by $\omega^{\omega^{m+1}}$. Since by assumption $\omega^{\omega^{m+1}}$ is well ordered, Lemma 4.2 implies that $A^* = W_m$ is well partially ordered. This completes the proof.

Added in Proof. Recently we became aware of A. Seidenberg's interesting work on constructive aspects of the Hilbert basis theorem (see ***Proceedings of the American Mathematical Society***, vol. 29 (1971), pp. 443–450, and ***Transactions of the American Mathematical Society***, vol. 174 (1972), pp. 305–312). The results of the present paper have been used by Harvey Friedman to illuminate some problems which were raised by Seidenberg.

REFERENCES

[1] E. T. BELL, ***The development of mathematics***, McGraw-Hill, New York, 1940.

[2] W. BUCHHOLZ and S. WAINER, *Provably computable functions and the fast growing hierarchy*, in [16], pp. 179–198.

[3] D. H. J. DE JONGH and R. PARIKH, *Well partial orderings and hierarchies*, ***Koninklijke Nederlandse Akademie van Wetenschappen, Proceedings, Series A***, vol. 80 = ***Indagationes Mathematicae***, vol. 39 (1977), pp. 195–207.

[4] F. VAN ENGELEN, A. W. MILLER and J. STEEL, *Rigid Borel sets and better quasiorder theory*, in [16], pp. 199–222.

[5] H. FRIEDMAN, S. G. SIMPSON and R. L. SMITH, *Countable algebra and set existence axioms*, ***Annals of Pure and Applied Logic***, vol. 25 (1983), pp. 141–181; addendum, vol. 28 (1985), pp. 320–321.

[6] P. GORDAN, *Neuer Beweis des Hilbert'schen Satzes über homogene Funktionen*, ***Nachrichten von der Königliche Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse***, 1899, pp. 240–242.

[7] ———, *Les invariantes des formes binaires*, ***Journal de Mathématiques Pures et Appliquées***, ser. 5, vol. 6 (1900), pp. 141–156.

[8] M. NOETHER, *Paul Gordan*, ***Mathematische Annalen***, vol. 75 (1914), pp. 1–45.

[9] C. PARSONS, *On a number-theoretic choice schema and its relation to induction*, ***Intuitionism and proof theory*** (J. Myhill et al., editors), North-Holland, Amsterdam, 1970, pp. 459–473.

[10] J. C. ROBSON, *Polynomials satisfied by matrices*, ***Journal of Algebra***, vol. 55 (1978), pp. 509–520.

[11] ———, *Well quasi-ordered sets and ideals in free semigroups and algebras*, ***Journal of Algebra***, vol. 55 (1978), pp. 521–535.

[12] D. SCHMIDT, *Well-partial-orderings and their maximal order types*, Habilitationsschrift, Heidelberg, 1979.

[13] K. SCHÜTTE and S. G. SIMPSON, *Ein in der reinen Zahlentheorie unbeweisbarer Satz über endliche Folgen von natürlichen Zahlen*, ***Archiv für Mathematische Logik und Grundlagenforschung***, vol. 25 (1985), pp. 75–89.

[14] W. SIEG, *Fragments of arithmetic*, ***Annals of Pure and Applied Logic***, vol. 28 (1985), pp. 33–71.

[15] S. G. SIMPSON, *BQO theory and Fraïsse's conjecture*, Chapter 9 in R. MANSFIELD and G. WEITKAMP, ***Recursive aspects of descriptive set theory***, Oxford University Press, Oxford, 1985, pp. 124–138.

[16] ——— (editor), ***Logic and combinatorics***, Contemporary Mathematics, vol. 65, American Mathematical Society, Providence, Rhode Island, 1987.

[17] ———, ***Subsystems of second order arithmetic***, in preparation.

[18] ———, *Subsystems of Z_2 and reverse mathematics*, appendix to G. Takeuti, ***Proof theory***, 2nd ed., North-Holland, Amsterdam, 1986, pp. 434–448.

[19] ———, *Unprovable theorems and fast-growing functions*, in [16], pp. 359–394.

[20] ———, *Which set existence axioms are needed to prove the Cauchy/Peano theorem of ordinary differential equations?* this JOURNAL, vol. 49 (1984), pp. 783–802.

[21] S. G. SIMPSON and R. L. SMITH, *Factorization of polynomials and Σ_1^0 induction*, ***Annals of Pure and Applied Logic***, vol. 31 (1986), pp. 289–306.

[22] R. STATMAN, *Well partial orderings, ordinals and trees*, preprint, Rutgers University, November, 1980, 13 pages.

DEPARTMENT OF MATHEMATICS
PENNSYLVANIA STATE UNIVERSITY
UNIVERSITY PARK, PENNSYLVANIA 16802