THE ACKERMANN FUNCTION IN ELEMENTARY ALGEBRAIC GEOMETRY

by
Harvey M. Friedman
friedman@math.ohio-state.edu
http://www.math.ohio-state.edu/~friedman/
October 21, 2000

1. THE ACKERMANN HIERARCHY.

Let $f:Z^+$ into Z^+ be strictly increasing. Define $f':Z^+$ into Z^+ by $f'(n) = f...f(1)$, where there are n f's.

Define $A_1(n) = 2n$. For each $k \geq 1$, define $A_{k+1} = A_k'$. Finally, define $A(k,n) = A_k(n)$, and $A(k) = A(k,k)$.

We can equivalently present this by the recursion equations $f_1(n) = 2n$, $f_{k+1}(1) = f_k(1)$, $f_{k+1}(n+1) = f_k(f_{k+1}(n))$, where $k,n \geq 1$. We define $A(k,n) = f_k(n)$.

$A(3,5) = 2^{65,536}$. $A(4,3) = 65,536$. $A(4,4) = E^*(65,536)$. And $A(4,5)$ is $E^*(E^*(65,536))$.

It seems safe to assert, e.g., that $A(5,5)$ is incomprehensibly large. We propose this number as a sort of benchmark.

The following facts about A are useful, and are easily proved in the order stated.

THEOREM 1.1. For all $k,n \geq 1$, $n < A_k(n) < A_k(n+1)$. For all $k \geq 1$ and $n \geq 3$, $A_k(n) < A_{k+1}(n)$. For all $k,n \geq 1$, $A_k(n)$ □ $A_{k+1}(n)$. For all $k \geq 1$, $A_k(1) = 2$, $A_k(2) = 4$, and $A_k(3) \geq 2^{k+1}$. For all $k \geq 3$, $A_k(3) \geq A_{k-2}(2^k) > A_{k-2}(k-2)$. If $k \geq n+5$ then $A_k(3) > A_n(k)$.

Ackerman's original definition is similar but is ternary. The growth rates are the same.

1. FULL SUBIDEALS.

Here we take the degree of an ideal in a polynomial ring over a field is the least d such that the ideal has a set of generators all of which have degree at most d. When we discuss algebraic sets, we will consider the usual notion of degree in algebraic geometry.

Let $k \geq 0$ and I be an ideal in the polynomial ring $F[x_1,...,x_k]$, F a field. I has finite degree by the Hilbert basis theorem. We write d(I) for the degree of I.

For each $n \geq 0$, we let I*n be the ideal generated by the elements of I of degree n. We call these the full subideals of I.

We let I*≤n be the ideal generated by the elements of I of degree ≤ n.

THEOREM 1.1. Let F be a field, $k \geq 1$, and I be an ideal in F[x1,...,xk]. For all $n \geq 0$, I*n = I*≤n. I*0 ⊆ ... ⊆ I*d(I) = I = I*d(I)+1 = ... For all $n \geq 0$, I*n = I*d(I*n). Any two full subideals with the same degree are equal. If $I \neq F[x_1,...,x_n]$ then I*0 = {0}.

Proof: For the first claim, let P in I have degree < n. By multiplication, let Q in I have degree n. Then Q+P in I has degree n. Hence P lies in I*n.

Now suppose I*n has degree d. Let K be a set of generators of I each of degree ≤ d. Then I*n ⊆ I*d. Also d ≤ n since I*n is generated by the elements of I of degree ≤ n. Hence I*d ⊆ I*≤n = I*n.

From the first claim, clearly the full subideals of I are the ideals I*≤n, which form a chain under inclusion of length at most d(I)+1.

I*n is generated by its elements of degree ≤ d(I*n). Since I*n is also generated by its elements of degree ≤ n (which are all polynomials of degree ≤ n), we have d(I*n) ≤ n. Hence I*n is generated by the set of polynomials of degree ≤ d(I*n). Therefore I*n = I*d(I*n).

The next claim is immediate. For the final claim, note that if $I \neq F[x_1,...,x_n]$ then I cannot contain any constants. Hence I*0 is generated by 0, and hence is {0}. QED

We say that I is perfect if and only if I*0,I*1,...,I*d(I) are distinct. By Theorem 1.1, I is perfect if and only if the full subideals form a chain of length deg(I)+1 if and only if the full subideals have degrees 0,1,...,d(I).

THEOREM 1.2. Every full subideal of every perfect ideal is perfect. The presentation degrees of perfect ideals in $F[x_1,...,x_k]$ form an initial segment of the nonnegative integers.

Proof: Let I be a perfect ideal and J = I*n be given. Then I,J both have the same elements of degree $\leq$n. Hence J*0,...,J*n is the same as I*0,...,I*n. Since I is perfect, J is perfect. The second claim follows immediately. QED

THEOREM 1.3. The degrees of the perfect ideals of $F[x_1,...,x_k]$ form a finite initial segment of the nonnegative integers. The union of these finite initial segments over all fields F is still finite.

Proof: This follows from the results in section 5 on ascending chains of ideals, originally due to A. Seidenberg. QED

Upper bounds for Theorem 1.3 follow from upper bounds in section 4.

Lower bounds for Theorem 1.3 are obtained by the following construction, even for monomial ideals in any $F[x_1,...,x_k]$.

Let $z_1,...,z_t$ be elements of N^k, where

1) for each i, the sum of the coordinates of z_i is i;
2) for all $i < j$, it is not the case that $z_i \leq z_j$ coordinatewise.

For each $z \in N^k$, let M(z) be the monomial $x_1^{z1} x_2^{z2} ... x_k^{zk}$. Let I be the ideal in $F[x_1,...,x_k]$ generated by $M(z_1),...,M(z_t)$.

LEMMA 1.4. Let $k \geq 1$ and F be a field. The ideal $I \subseteq F[x_1,...,x_k]$ generated by $M(z_1),...,M(z_t)$ is perfect. In

particular, for all $0 \leq n \leq t$, I_n is the ideal generated by $M(z_1),...,M(z_n)$.

Proof: Let k,F,I be as given. Let $1 \leq i \leq t$. Then the polynomials in I of degree i must be generated by $M(z_1),...,M(z_i)$. To see this, let $f \in I$ have degree i, and write f as a sum of multiples of $M(z_1),...,M(z_t)$. Every monomial in f must be a multiple of one of the $z_1,...,z_t$. Hence every monomial in f must be a multiple of one of the $z_1,...,z_i$. Hence f is generated by $M(z_1),...,M(z_i)$.

Also clearly I contains no nonzero constants, and hence $I*0 = \{0\}$.

It remains to verify that for all $0 \leq n \leq t$, $M(z_n)$ is not in the ideal generated by $M(z_1),...,M(z_{n-1})$. This is clear since all monomials in all polynomials generated by $M(z_1),...,M(z_{n-1})$ must be variablewise $\geq$ some $M(z_i)$, $1 \leq i \leq n-1$, and hence cannot be $M(z_n)$. QED

For $k \geq 1$ let F(k,n) be the longest length of a sequence $z_1,...,z_t$ from N^k, where

1) for each $i \geq 1$, the sum of the coordinates of z_i is $n+i-1$;
2) for all $i < j$, it is not the case that $z_i \leq z_j$ coordinatewise.

LEMMA 1.5. For each $k,n \geq 1$, F(k,n) exists.

Proof: Fix $n \geq 1$. Consider the tree of all of the relevant finite sequences. This tree is finitely branching. It cannot have an infinite path, since in any infinite sequence from N^k, some term is coordinatewise $\leq$ some later term. Hence the tree is finite. QED

LEMMA 1.6. $F(2,n) \geq 2n$.

Proof: $(n,0),(n-1,2),...,(0,2n),(0,2n-1),...,(0,0)$. QED

LEMMA 1.7. $F(k+1,n) \geq F_kF_k...F_k(1)$, where $F_k(n) = F(k,n)$, and there are n F_k's.

Proof: First write down an appropriate sequence of elements of N^k of length $F_k(1)$. Then write down an appropriate sequence of elements of N^k of length $F_kF_k(1)$. Continue this process for n steps. Then extend each k-tuple by another coordinate,

where in the first sequence, the new coordinate is n-1, and n-2 in the second sequence, and so forth down to 0. QED

LEMMA 1.8. For $k,n \geq 1$, $F(k+1,n) \geq A(k,n)$.

THEOREM 1.9. Let $k \geq 1$ and F be a field. There exists perfect ideals in $F[x_1,...,x_k]$ of every presentation degree $\geq A(k,n)$.

2. ALGEBRAIC APPROXIMATIONS VIA PRESENTATIONS.

In this section, we will take the presentation approach. In the next section, we will reconcile it with the algebraic approach, at least in the case of algebraically closed fields.

Let F be a field and $k \geq 1$. An algebraic subset of F^k is the set of simultaneous zeros of a nonempty finite set of polynomials in k variables with coefficients from F. The degree of an algebraic set $A \subseteq F^k$ is the least d such that it is the set of simultaneous zeros of a nonempty finite set of polynomials in k variables each of which have degree at most d. We write this as d(A).

Let A be any subset of F^k. For each $n \geq 0$, we let A*n be the intersection of all algebraic subsets of F^k of degree n that contain A. If there are no such subsets then we take $A*n = F^k$.

We henceforth assume that F is an infinite field and $k \geq 1$.

LEMMA 2.1. Every polynomial over F that vanishes everywhere is the zero polynomial.

Proof: By induction on the number of variables in the polynomial. Write P as a polynomial in the last variable x_k with coefficients from the polynomial ring $F[x_1,...,x_{k-1}]$. For any choice of $x_1,...,x_{k-1}$, the polynomial in the one variable x_k vanishes everywhere, and hence has infinitely many roots (we are using that F is infinite), and therefore must be the zero polynomial. So all of the polynomial coefficients must vanish everywhere. QED

LEMMA 2.2. Let P be a polynomial over F in k variables, where for all $x_1,...,x_{k-1}$ in F, $\{x_k: P(x_1,...,x_k) = 0\}$ is infinite. Then P is the zero polynomial.

Proof: Again, write P as a polynomial in the one variable x_k with coefficients from $F[x_1,...,x_{k-1}]$. Then for all choices of $x_1,...,x_{k-1}$ in F, P is the zero polynomial. Hence all of these polynomial coefficients vanish everywhere. By Lemma 2.1, they must be the zero polynomial. Hence P is the zero polynomial. QED

LEMMA 2.3. If A is an algebraic set such that $F^k \backslash A$ is finite, then $A = F^k$.

Proof: Suppose $F^k \backslash A$ is finite. Let P be a polynomial which is zero on all of A. Then by Lemma 2.2, P must be the zero polynomial. So A must be the simultaneous zeros of only the system of polynomials consisting of just the zero polynomial; i.e., $A = F^k$. QED

LEMMA 2.4. Let A be an algebraic set of degree d, B an infinite subset of $F \backslash A$, and $r \geq d$. We can add finitely many elements of B to A to obtain a algebraic set of presentation degree r.

Proof: Successively add elements of B one at a time to A. Every time we add an element of B we get an algebraic set whose degree is at most 1 higher. It suffices to show that this process produces algebraic sets whose degrees are arbitrarily large. This is clear, for otherwise we would get arbitrarily long finite chains of algebraic sets of a given degree, which violates linear algebra. QED

LEMMA 2.5. Let A be an algebraic set of degree d, and $r > d$. Then $A^*r = A^*\square r = A$. Also $A^*d = A^*\square d = A$.

Proof: Suppose $F^k \backslash A$ is infinite. Let B,B' be disjoint infinite subsets of $F^k \backslash A$. By Lemma 2.4, we can add finitely many elements of B to A and finitely many elements of B' to A to obtain algebraic sets of degree r. By taking their intersection, we see that $A^*r = A$, and hence $A^*r = A^*\square r = A$. By Lemma 2.3, if $F^k \backslash A$ is finite then $A = F^k$, in which case we are done. The final statement is obvious. QED

THEOREM 2.6. Let A be an algebraic subset of F^k, F infinite. For all $n \geq 0$, $A^*n = A^*\square n$.

Proof: Let the degree of A be d. By Lemma 2.5, we assume that $n < d$. We need to show that $A^*n \subseteq A^*\square n$. It suffices to show that A^*n is included in every algebraic superset B of A of

degree < n. Fix B to be an algebraic superset of A of degree < n.

If $F^k \backslash B$ is infinite then choose C,C' to be disjoint finite subsets of $F^k \backslash B$ such that B union C and B union C' have degree n, by Lemma 2.4. Their intersection is included in A*n but is simply B. If $F^k \backslash B$ is finite then by Lemma 2.3, $B = F^k$, and we are done. QED

THEROEM 2.7. Let A be an algebraic subset of F^k, F infinite. A*n = A*d(A*n). $A*0 \supseteq \ldots \supseteq A*d(A) = A = A*d(A)+1 = \ldots$. Any two algebraic approximations with the same degree are equal.

Proof: For the first claim, let A*n have degree d. Now A*n has degree $\leq$ n since it is an intersection of algebraic sets of presentation degrees $\leq$ n. Hence d $\leq$ n. Now A*d is the intersection of all supersets of A of degree d, and hence A*d $\supseteq$ A*n. On the other hand, A*n = A*$\leq$n is the intersection of all supersets of A of degree $\leq$ n, and so A*n $\supseteq$ A*d. Hence A*n = A*d.

From Theorem 2.6, we see that the algebraic approximations of A form a chain under inclusion of length at most deg(A)+1. Let A*n and A*m have the same degree d. Then A*n = A*m = A*d. QED

We say that A is perfect if and only if A*0,A*1,...,A*deg(A) are distinct. By Theorem 2.7, A is perfect if and only if its approximations form a chain of length deg(A)+1 if and only if the approximations have degrees 0,1,...,d(A).

THEOREM 2.8. Every algebraic approximation of every perfect algebraic set is perfect. The degrees of perfect algebraic subsets of F^k form an initial segment of the nonnegative integers.

Proof: For the first claim, let A be a perfect algebraic set and B = A*n be a algebraic approximation. Then B*n has degree n. We claim that B*0,...,B*n is the same as A*0,...,A*n. To see this, note that every superset of A of degree $\leq$ i $\leq$ n is a superset of B of degree $\leq$ i because B is an intersection of the supersets of A of degree $\leq$ n.

The second claim follows since the algebraic approximations of A have every degree $\leq$ deg(A) represented. QED

THEOREM 2.9. The degrees of perfect algebraic subsets of F^k form a finite initial segment of the nonnegative integers. The union of these finite initial segments over all fields F is still finite.

Proof: The first statement is by Theorem 2.8. The second statement is by Theorems 1.3, which in turn follow from the statements about strictly ascending sequences of ideals in section 5. Also any upper bound for Theorem 1.3 or statements in section 5 are also upper bounds for Theorem 2.10. QED

3. ALGEBRAIC APPROXIMATIONS IN ALGEBRAICALLY CLOSED FIELDS.

If F is algebraically closed and $k \geq 1$ then the algebraic subsets of Fk defined in the previous section are the same as the algebraic subsets of Fk in the sense of algebraic geometry. However, the degree defined in the previous section are not the same as the usual algebraic degree used in algebraic geometry.

We now show that for algebraically closed fields, we arrive at the same notions of algebraic approximations and perfect algebraic sets using algebraic degrees.

We write deg(A) for the algebraic degree. We will use only two facts about deg(A) in F^k, F algebraically closed.

a. The zero set of any polynomial of degree p is of algebraic degree $\leq$ p.
b. Every set of algebraic degree p is the set of simultaneous zeros of a set of polynomials of degree $\leq$ p.

THEOREM 3.1. Let $k \geq 1$, $n \geq 0$, $A \subseteq F^k$ be algebraic, where F be algebraically closed. Then A*n is the same as the intersection of all algebraic supersets of A of algebraic degree $\leq$ n.

Proof: Let this second intersection be A**n. Obviously A*n is the intersection of zero sets of polynomials of degree $\leq$ n. By a, this is the intersection of algebraic supersets of A of algebraic degree $\leq$ n. Hence A**n $\supseteq$ A*n. On the other hand, by b, every superset of A of algebraic degree $\leq$ n is of presentation degree $\leq$ n. Hence A*$\subseteq$n $\supseteq$ A**n, and so A*n $\subseteq$ A**n. QED

For a general field F, algebraic geometers will view F as a subspace of its algebraic closure F#. Thus the algebraic subsets of F^k are the intersections of algebraic subsets of $F\#^k$ with F^k. Also, the algebraic degree of an algebraic subset A of F^k is the least d such that A is the intersection of an algebraic subset of $F\#^k$ of algebraic degree d with F^k.

For our purposes, this amounts to using only algebraically closed fields F, and studying algebraic approximations of subsets of F^k and perfect subsets of F^k which are not necessarily algebraic. For example, we might require that the subsets of F^k be subsets of G^k for a given subfield G of F.

The results of the next section can be adapted to this point of view.

4. LOWER BOUNDS FOR ALGEBRAIC APPROXIMATIONS.

Lower bounds for degrees of perfect algebraic sets require a new construction which we give here. The lower bounds given here depend on F being an infinite field, which we fix.

An interesting aspect of these lower bounds is that we obtain them by considering finite sets only. Finite sets are automatically algebraic, but their degree is generally an intricate matter.

For $A \subseteq F^{k+1}$ and $z \in F$, let $A<z> = \{y \in F^k: (y,z) \in A\}$.

We say that A is good for (k,n,m) if and only if

i) $0 \leq n < m$;
ii) A is an algebraic subset of F^k;
iii)i $A*n,...,A*m$ are distinct;
iv) $A*n = F^k$.

LEMMA 4.1. Let $n,k,p \geq 1$ and $A_1 \subseteq ... \subseteq A_n$ be finite subsets of F^k. Let $a_1,...,a_n$ be distinct elements of F. Let $B = A_1 \times \{a_1\} \cup ... \cup A_n \times \{a_n\}$. Let $1 \leq i \leq n \leq r$. Assume that for all j in (i,n], $A_j*p+j-n = F^k$. Then $B*p<a_i> = A_i*p+i-n$.

Proof: We claim that $A_i*p+i-n \times \{a_1,...,a_i\} \cup F^k \times \{a_{i+1},...,a_n\}$ is a degree $\leq p$ superset of B. To see this, first note that the first term is $A_i*p+i-n \times F$ intersect $F^k \times \{a_1,...,a_i\}$, and so has degree $\leq \max(p+i-n,i) = p+i-n$. The

second term has degree $\leq$ n-i. Hence the union has degree $\leq$ p as claimed. Hence $B*p\langle a_i\rangle$ containedin $A_i*p+i-n$.

Now let E be a degree $\leq$ p superset of B. It suffices to show that $E\langle a_i\rangle$ contains $A_i*p+i-n \times \{a_i\}$. Let P be a polynomial in a defining set of polynomials for E of degrees $\leq$ p. It suffices to show that for all z in $A_i*p+i-n$, $P(z,a_i) = 0$.

Formally write $P(z,w) = (x_{k+1} - a_n)Q(z,w) + R(z)$, where z is the first k variables $x_1,\ldots,x_k$ and w is the variable x_{k+1}. It is important that x_{k+1} does not appear in R. Now for all z in A_n, $P(z,a_n) = 0$. Hence R vanishes on A_n. But R has degree $\leq$ deg(P) $\leq$ p. Since $A_n*p = F^k$, we see that R vanishes on F^k, and hence must be zero. So $P(z,w) = (x_{k+1} - a_n)Q(z,w)$. Note that deg(Q) $\leq$ p-1. Clearly Q vanishes on all elements of $A_1 \times \{a_1\} \cup \ldots \cup A_{n-1} \times \{a_{n-1}\}$.

We can repeat the above argument for Q, using $A_{n-1}*p-1 = F^k$, writing $Q(z,w) = (x_{k+1} - a_{n-1})R(z,w)$. We continue in this way until we arrive at the factorization $Q(z,w) = (x_{k+1} - a_n)(x_{k+1} - a_{n-1})\ldots(x_{k+1} - a_{i+1})T(z,w)$, where deg(T) $\leq$ p+i-n. Now $Q(z,a_i)$ vanishes on A_i, and hence $T(z,a_i)$ vanishes on A_i. Since $T(z,a_i)$ has degree $\leq$ p+i-n, we see that $T(z,a_i)$ vanishes on $A_i*p+i-n$. Hence $P(z,a_i)$ vanishes on $A_i*p+i-n$. QED

We put Lemma 4.1 in a more directly useable form.

LEMMA 4.2. Let $k,n \geq 1$ and $0 = r_1 < \ldots < r_{n+1}$. Let $A_1 \subseteq \ldots \subseteq A_n$ be finite subsets of F^k. Let $a_1,\ldots,a_n$ be distinct elements of F. Assume that for all $1 \leq i \leq n$, A_i is good for (k,r_i,r_{i+1}). Let $B = A_1 \times \{a_1\} \cup \ldots \cup A_n \times \{a_n\}$. Let $1 \leq i \leq n \leq p \leq r_{i+1} -i-1+n$. Then $B*p\langle a_i\rangle = A_i*p+i-n$. Also $B*r_{n+1}\langle a_n\rangle = A_n*r_{n+1}$.

Proof: Assume hypotheses. We first verify that for all j in (i,n], $p+j-n \leq r_j$. Let $j \in (i,n]$. This is clear for j = i+1. But at j moves up by one, r_j moves up by at least one. We now see that for all j in (i,n], $Aj*p+j-n = F^k$.

By Lemma 4.1, we see that for all $1 \leq i \leq n$, $B*p\langle a_i\rangle = A_i*p+i-n$. If i = n then this equation holds for all $p \geq 1$. QED

LEMMA 4.3. Let $k,n \geq 1$ and $0 = r_1 < \ldots < r_{n+1}$. Let $A_1 \subseteq \ldots \subseteq A_n$ be finite subsets of F^k. Let $a_1,\ldots,a_n$ be distinct elements of F. Assume that for all $1 \leq i \leq n$, A_i is good for

(k,r_i,r_{i+1}). Let $B = A_1 \times \{a_1\} \cup \ldots \cup A_n \times \{a_n\}$. Then B is good for $(k+1,n-1,r_{n+1})$.

Proof: Assume hypotheses. We will show that
i) for all p in $[n,r_{n+1}-2]$, there exists i such that $1 \le i \le n \le p \le p+1 \le r_{i+1} -i-1+n$, and $r_i \le p+i-n < r_{i+1}$;
ii) $B*r_{n+1}-1 \ne Br_{n+1}$;
iii) $B*n \ne B*_{n-1} = F^{k+1}$.

We then conclude that B is good for $(k+1,n-1,r_{n+1})$ as follows. Let p in $[n,r_{n+1}-2]$. Let $1 \le i \le n \le p \le p+1 \le r_{i+1} -i-1+n$, and $r_i \le p+i-n < r_{i+1}$. By Lemma 3.2, $B*p\langle a_i\rangle = A_i*p+i-n$ and $B*p+1\langle a_i\rangle = A_i*p+1+i-n$. Since A_i is good for (k,r_i,r_{i+1}), we have $B*p\langle a_i\rangle \ne B*p+1\langle a_i\rangle$. This shows that $B*n, B*n+1, \ldots, B*r_{n+1}-1$ are distinct. By ii),iii), B is good for $(k+1,n-1,r_{n+1})$.

For i), let p in $[n,r_{n+1}-2]$. If i = n then $1 \le i \le n \le p \le p+1 \le r_{i+1} -i-1+n$. Choose i to be least such that $1 \le i \le n \le p \le p+1 \le r_{i+1} -i-1+n$. Then $p+1+i+1-n \le r_{i+1}$, and so $p+i-n+1 < r_{i+1}$. If i = 1 then $r_i \le p+i-n$. So we can assume $i > 1$. Then $1 \le i-1 \le n \le p \le p+1 \le r_i -(i-1)-1+n$ is false. Hence $p+1 > r_i -i+1-1+n = r_i +n-i$. Hence $r_i < p+1-n+i$, and so $r_i <= p+i-n$ as required.

For ii), by Lemma 3.2 with i = n and $p = r_{n+1} -1$, we have $B*p\langle a_n\rangle = A_n*p$. Also by Lemma 3.2, $B*p\langle a_n\rangle = A_n*p$ holds for $p = r_{i+1}$.

For iii), note that $B*n \ne F^{k+1}$ since $F^k \times \{a_1,\ldots,a_n\}$ is a degree $\le n$ superset of B. On the other hand, $B*n-1 = F^{k+1}$ by the following argument. Let P be a polynomial of degree $\le n-1$ whose zero set contains B*. Write $P = (x_{k+1} - a^2)Q + R$, where $x_{k+1} \notin R$, and R has degree $\le n-1$. The zero set of R contains A_2, and hence must be F^k. So R is the zero polynomial, and we write $P = (x_{k+1} - a_2)Q$.

Similarly, P is divisible by each $(x_{k+1} - a_i)$, $2 \le i \le n$. So we can write $P = (x_{k+1} - a_2)\ldots(x_{k+1} - a_n)T$, where T is a constant. Since A_1 is nonempty, we see that T must be 0, and hence P must be zero. QED

It is a little more convenient to have this in slightly altered form.

LEMMA 4.4. Let $k \ge 1$, $n \ge 0$, and $0 = r_0 < \ldots < r_{n+1}$. Let $A_0 \subseteq \ldots \subseteq A_n$ be finite subsets of F^k. Let $a_0,\ldots,a_n$ be distinct

elements of F. Assume that for all $0 \leq i \leq n$, A_i is good for (k,r_i,r_{i+1}). Let $B = A_0 \times \{a_0\} \cup \ldots \cup A_n \times \{a_n\}$. Then B is good for $(k+1,n,r_{n+1})$.

Proof: Let $k,n,r_0,\ldots,r_{n+1},A_0,\ldots,A_n,F,a_0,\ldots,a_n$ be as given. Let $n' = n+1$, $r_1',\ldots,r_{n+2}' = r_0,\ldots,r_{n+1}$, $A_1',\ldots,A_{n+1}' = A_0,\ldots,A_n$, and $a_1',\ldots,a_{n+1}' = a_0,\ldots,a_n$. Then for all $1 \leq i \leq n$, A_i' is good for (k,r_{i-1},r_i), and hence good for (k,r_i',r_{i+1}'). By Lemma 3.3, $A_1' \times \{a_1'\}$ union ... union $A_{n'}' \times \{a_{n'}'\}$ is good for $(k+1,n'-1,r_{n'+1}')$, and hence good for $(k+1,n,r_{n+2}')$. I.e., $A_0 \times \{a_0\} \cup \ldots \cup A_n \times \{a_n\}$ is good for $(k+1,n,r_{n+1})$. QED

LEMMA 4.5. Let $k,m \geq 1$ and A,B be finite subsets of F^k,F^q respectively. For all $r \geq 0$, $(A \times B)^*r[1] = A^*r$, and $(A \times B)^*r[2] = B^*r$.

Proof: Note that $A^*r \times F^q$ is a degree $\leq r$ superset of AxB. Hence $(AxB)^*r$ is contained in $A^*r \times F^q$, and so $(AxB)^*r[1]$ is contained in A^*r.

Let $w \in B$. We claim that $A^*r \times \{w\} \subseteq (AxB)^*r$. To see this, let P be a degree $\leq r$ polynomial whose zero set contains AxB. Then $\{z: P(z,w) = 0\}$ is a degree $\leq r$ superset of A, and hence contains A^*r. So $A^*r \times \{w\}$ is contained in the zero set of P.

It is now obvious that $A^*r \subseteq (AxB)^*r[1]$, using w. The two conclusions are symmetric. QED

LEMMA 4.6. Let $k,m \geq 1$ and A,B be finite subsets of F^k,F^q respectively. Assume A is good for (k,n,m) and B is good for (q,m,r). Then AxB is good for (k+q,n,r).

Proof: Let $n \leq p < m$. By Lemma 4.3, $AxB^*p[1] = A^*p$, $AxB^*p+1[1] = A^*p+1$. Hence $AxB^*p \neq AxB^*p+1$. Let $m \leq p < r$. By Lemma 4.3, we also see that $AxB^*p \neq AxB^*p+1$. It suffices to prove that $AxB^*n = F^{k+q}$. Let $P = P(x_1,\ldots,x_k,y_1,\ldots,y_k)$ be a polynomial of degree $\leq n$ whose zero set contains AxB. Now A,B are nonempty. Let $w = (w_1,\ldots,w_k) \in B$. Then $P(x_1,\ldots,x_k,w_1,\ldots,w_k)$ is a degree $\leq n$ polynomial whose zero set contains B. Hence $P(x_1,\ldots,x_k,w_1,\ldots,w_k)$ is the zero polynomial. It is easy to see that $\{(w_1,\ldots,w_k): P(x_1,\ldots,x_k,w_1,\ldots,w_k)$ is the zero polynomial$\}$ is a degree $\leq n$ finite set which contains B. Hence it must be F^q. Therefore the set of zeros of P must be F^{k+q}. QED

We fix $a_0,a_1,\ldots$ to be distinct elements of F.

LEMMA 4.7. There exist finite subsets $A_0 \subseteq A_1 \subseteq \ldots$ of F such that each A_i is good for $(1,i,i+1)$.

Proof: Let $A_i = \{a_0,\ldots,a_i\}$. QED

LEMMA 4.8. There exist finite subsets $B_0 \subseteq B_1 \subseteq \ldots$ of F^2 such that each B_i is good for $(2,i,i+2)$.

Proof: Let the A's be as given by Lemma 4.7. Let $B_i = A_i \times A_{i+1}$. By Lemma 4.6, B_i is good for $(2,i,i+2)$. QED

LEMMA 4.9. There exist finite subsets $C_0 \subseteq C_1 \subseteq \ldots$ of F^3 such that each C_i is good for $(3,i,2i+2)$.

Proof: Let the B's be as given by Lemma 4.7. Let $C_i = B_0 \times \{a_0\} \cup B_2 \times \{a_1\} \ldots \cup B_{2i} \times \{a_i\}$. Note that B_0 is good for $(2,0,2)$, B_2 for $(2,2,4)$, ..., B_{2i} for $(2,2i,2i+2)$. By Lemma 4.4, C_i is good for $(3,i,2i+2)$. QED

We can restate this using the Ackermann function as follows.

LEMMA 4.10. There exist finite subsets $C_0 \subseteq C_1 \subseteq \ldots$ of F^3 such that each C_i is good for $(3,i,A_1(i+1))$.

LEMMA 4.11. Let $k \geq 3$. There exists finite subsets $C_0 \subseteq \ldots$ of F^k such that each C_i is good for $(k,i,A_{k-2}(i+1))$.

Proof: By induction on k. Let $k \geq 3$ and $C_0 \subseteq \ldots$ be finite subsets of F^k such that each C_i is good for $(k,i,A_{k-2}(i+1))$.

Let $i \geq 0$. We define D_i as follows. Consider the sequence of pairs

$0,A_{k-2}(1)$
$A_{k-2}(1),A_{k-2}A_{k-2}(1)$
...
$A_{k-1}(i),A_{k-1}(i+1)$

There are i+1 pairs. Note that $C_0,C\_A_{k-1}(1),C\_A_{k-1}(2),\ldots,C\_A_{k-1}(i)$ are good for these pairs, respectively.

Set $D_i = C_0 \times \{a_0\} \cup C\_A_{k-1}(1) \times \{a_1\} \cup \ldots \cup C\_A_{k-1}(i) \times \{a_i\}$. By Lemma 4.4, D_i is good for $(k+1,i,A_{k-1}(i+1))$. QED

LEMMA 4.12. Let $k \geq 1$. There is a finite set which is good for $(k+6,0,A_k(k))$.

Proof: By Lemma 4.8, let A be a finite subset of F^2 which is good for (2,0,2). By Lemma 4.11, let B be a finite subset of F^k which is good for $(k+4,2,A_{k+2}(3))$. Since $k \geq 1$, B is good for $(k+4,2,A_k(k))$. By Lemma, AxB is a finite subset of F^{k+6} which is good for $(k+6,0,A_k(k))$. QED

THEOREM 4.13. Let $k \geq 1$ and F be an infinite field. There is a perfect finite subset of F^{k+6} of degree $A_k(k)$.

Proof: By Lemma 4.12, let B be a finite subset of F^{k+6} such that $B*0,\ldots,B*A_k(k)$ are distinct. Set $C = B*A_k(k)$. Then C has degree $A_k(k)$ and is perfect. QED

THEOREM 4.14. Let $k \geq 1$ and F be a sufficiently large finite field. There is a perfect subset of F^{k+6} of degree $A_k(k)$.

In fact, the finite field need only be a little bit larger than A(k), which we will eventually take the trouble to make precise.

5. ASCENDING CHAINS OF IDEALS - HISTORICAL NOTES.

The results here about ascending chains of ideals were obtained in the 80's and discussed here in postings #40 and #43.

Seidenberg had earlier intensively investigated the same statement about ascending chains of ideals in the following papers:

A. Seidenberg, An elimination theory for differential algebra, Univ. Calif. Pubs. Math. 3 (1956), 31-65.

A. Seidenberg, On the length of a Hilbert ascending chain, Proc. AMS, Vol. 29, No. 3, August 1971, 443-450.

A. Seidenberg, Constructive proof of Hilbert's theorem on ascending chains, Trans. AMS, Vol. 174, December 1972, 305-312.

The first paper is quoted in the last two and has a partial result.

Actually, his is more general in that he considers arbitrary bounds on the degrees of the ideals. I had also dealt with this formulation but did not report it in #40 and #43. Of course, my work is all after Seidenberg.

Seidenberg proves no lower bounds. Also, he states a multi recursive bound in each dimension k, rather than my primitive recursive bounds. He states only primitive recursive bounds in dimension ≤ 2, and states that primitive recursivity for dimension ≥ 3 is "doubtful." Also, Seidenberg does not consider corresponding statements about algebraic sets, which of course follows from these statements about ideals.

Seidenberg also discusses these chains in

A. Seidenberg, Survey of constructions in Noetherian rings, Univ. of Cal. Berkeley.

A. Seidenberg, Constructions in algebra, Trans. AMS, Vol. 197, 1974, 273-313.

I think he also discusses it in a fifth paper and probably others, entitled "What is Noetherian" but I haven't got a hold of a copy of that paper.

Seidenberg's theorem can be viewed as a kind of finite form of the Hilbert basis theorem. He himself viewed it as a constructive form of the Hilbert basis theorem.

**Our original finite forms of Kruskal's theorem in 1981-82 are to Kruskal's theorem as Sidenberg's theorem is to the Hilbert basis theorem. Bounds on the degrees become bounds on the number of vertices of the trees. It is interesting to note that Seidenberg and I had the same idea for getting finite forms in the two contexts - Hilbert's basis theorem and Kruskal's theorem - namely to look at finite sequences with bounds placed on the terms. **

Yet we searched hard for a good finite form of Kruskal's theorem involving a single tree rather than a sequence of trees. We were quite successful with this, and reported the results in posting #27, together with sketches of the proofs. After some experience with lecturing on this, my favorite is:

1) if T is a sufficiently tall thin tree, there exists $1 \leq i < j \leq \text{hgt}(T)$ and an inf preserving embedding from $T[\leq i]$ into

T[≤j] which maps T[i] into T[j]. I.e., if T is a sufficiently tall tree of valence ≤ k, then there exists ... .

It can be stated for arbitrary finite trees as follows.

2) for all k there exists n such that if T is any finite tree of valence ≤ k, there exists 1 ≤ i < j ≤ n and an inf preserving embedding from T[≤i] into T[≤j] which maps T[i] into T[j].

So it makes sense to search for theorems about a single ideal. We have found such a theorem. See section 1. We have also found theorems about a single algebraic set. See section 2.

6. ASCENDING CHAINS OF IDEALS.

We take an ideal (in a commutative ring with unit) to be any subgroup which is closed under multiplication by any ring element. Thus the smallest ideal is {0}. The ideal {0} is generated by the empty set (and also by {0}).

The degree of an ideal in a polynomial ring is the least d such that the ideal has a set of generators all of which have degree at most d.

Here is Seidenberg's theorem on ascending chains:

THEOREM 5.1. For all k,p ≥ 1 there exists n ≥ 1 such that the following holds. For any field F, there is no strictly ascending sequence of ideals in $F[x_1,...,x_k]$ of length n, where the i-th ideal has degree at most p+i (i.e., a set of generators each of which has degree at most p+i).

Actually, Seidenberg states this for any bound on the degree of the i-th ideal. Exactly analogous results hold. We prefer to state this as above because of our interest in lower bounds and the elementary nature of the result.

Seidenberg established a primitive recursive bound only for k ≥ 2, and doubted whether a primitive recursive bound exists for even k = 3.

We first wish to reduce this to a more manageable form. It is easy to see that Theorem 5.1 follows from the following.

LEMMA 5.2. For all $k,p \geq 1$ there exists $n \geq 1$ such that the following holds. For any field F and polynomials $P_1,...,P_n$ from $F[x_1,...,x_k]$, where each P_i has degree $\leq p+i$, some P_i is in the ideal generated from $P_1,...,P_{i-1}$.

Proof of Lemma 5.2: Fix $k,p \geq 1$. Let $n \geq 1$. We define the theory T[k,p,n] in first order predicate calculus with equality as follows.

i) field axioms;
ii) by introducing constants for all relevant coefficients, state that we have polynomials P_i, where $1 \leq i \leq n$, of degree at most p+i, which cannot be written as an ideal element from the P_j, $j < i$, using polynomial coefficients of degrees at most n.

We now apply the compactness theorem. Suppose each T[k,p,n], $n \geq 1$, has a model. Then the union of the T[k,p,n] has a model, which consists of a field F and an infinite sequence of ideals presented by generators, which are strictly ascending. But this contradicts the Hilbert basis theorem. Hence some T[k,p,n] does not have a model. The Lemma follows immediately. QED

It is interesting to also consider

THEOREM 5.3. For all $k,p \geq 1$ there exists $n \geq 1$ such that the following holds. For any field F, there is no strictly ascending sequence of ideals in $F[x_1,...,x_k]$ of length n, where the i-th ideal has degree p+i.

Upper bounds for Theorem 5.2 give upper bounds for Theorem 5.3 and for Theorem 5.1. However, the lower bound for Theorem 5.3 needs to be rethought a bit.

We now give primitive recursive bounds for each k, in Theorem 5.2, using more logic.

Consider the Π^0_2 sentence

for all $k,p \geq 1$ there exists $n \geq 1$ such that T[k,p,n] is inconsistent.

Fix k. For any p, the least size of an inconsistency in T[k,p,n] is clearly an upper bound on the relevant number in Theorem 1.1, because already n is such an upper bound. But

that least size is a primitive recursive function of p because the above statement is provable in WKL_0 for any given k. This is because the compactness theorem, the completeness theorem, and the Hilbert basis theorem are all provable in WKL_0.

7. CHAINS OF ALGEBRAIC SETS - PRIMITIVE RECURSIVE BOUNDS.

Let F be a field and $k \geq 1$. An algebraic subset of F^k is the set of simultaneous zeros of some finite set of polynomials in k variables over F. The degree of an algebraic set is taken here to mean the least d such that it is the set of simultaneous zeros of some finite set of polynomials in k variables of degree at most d.

THEOREM 6.1. For all $k,p \geq 1$ there exists $n \geq 1$ such that the following holds. For any field F, there is no strictly decreasing sequence of algebraic sets in F^k of length n, where the i-th algebraic set has degree at most p+i (i.e., is the zero set of a finite system of k variable polynomials over F of degree at most p+i).

Theorem 6.1 follows immediately from Theorem 5.1, and our upper bounds for Theorem 5.1 also serve as upper bounds for Theorem 6.1.

It is interesting to also consider

THEOREM 6.2. For all $k,p \geq 1$ there exists $n \geq 1$ such that the following holds. For any field F, there is no strictly ascending sequence of ideals in $F[x_1,...,x_k]$ of length n, where the i-th algebraic set has degree p+i.

Upper bounds for Theorem 6.2 obviously give upper bounds for Theorem 5.3.

Lower bounds for Theorem 6.2 follow immediately from those given in section 3.