# DECREASING CHAINS OF ALGEBRAIC SETS

by
Harvey M. Friedman
friedman@math.ohio-state.edu
www.math.ohio-state.edu/~friedman/
November 12, 1999

## 1. IDEALS IN k VARIABLE POLYNOMIAL RINGS.

An ideal in a commutative ring R with unit is a nonempty $I \subseteq R$ such that for all $x,y \in I$, $z \in R$, we have $x+y$ and $xz \in I$. A set of generators for I is a subset of I such that I is the least ideal containing that subset.

One main formulation of the Hilbert basis theorem asserts that for every $k \geq 1$, every ideal in the k variable polynomial ring over any field is finitely generated.

An equivalent way of saying this is that for every $k \geq 1$, there is no strictly ascending sequence of ideals in the k variable polynomial ring over any field.

The presentation degree of an ideal I in the polynomial ring $F[x_1,...,x_k]$ is the least d such that there is a set of generators for I consisting entirely of polynomials of degree at most d.

Note that by linear algebra, there is a number f(k,d) such that for all fields F, any ideal of presentation degree at most d in the k variable polynomial ring over F has a set of generators of degree at most d, of cardinality at most f(k,d).

THEOREM 1.1. For all k,p there exists n such that the following holds. Let F be a field. There is no strictly ascending sequence of ideals in $F[x_1,..., x_k]$ of length n, indexed from 1, indexed from 1 through n, such that the i-th ideal is of presentation degree $\leq p+i$.

Proof: Fix k,p, and suppose that this is false for all n. For each n, let T[k,p,n] be the following theory in first order predicate calculus in the language of fields, aug-mented with unary predicate symbols $P_1,...,P_n$.

i) the field axioms;

ii) for $1 \leq i \leq n$, $P_i$ is an ideal in the k variable polynomial ring over F;
iii) for all $1 \leq i \leq n-1$, $P_i \neq P_{i+1}$;
iv) for $1 \leq i \leq n$, $P_i$ has a set of ideal generators of presentation degree $\leq p+i$, of car-dinality $\leq f(k,d)$.

Clearly, for each n, T[k,p,n] has a model. Hence there is a model of the union of the T[k,p,n] (compactness theorem for predicate calculus with equality). This model gives us a field F together with a strictly ascending sequence of ideals. This contradicts the Hilbert basis theorem. QED

We define I(k,p) be the least n given by Theorem 1.1. We also define I(F,k,p) to be the least n given by Theorem 1.1 for a given field F. Obviously I(k,p) is the minimum over all F of I(F,k,p).

We can read off some crude upper bounds for I(k,p) using machinery from logic. Of course, more precise upper bounds can be obtained by getting rid of the logic and going into the guts of the situation.

Specifically, we use logic to show that the function I(k,p), k fixed, is primitive recursive in p. Fix $k \geq 1$.

Step 1. We have to put the statement "for all p, I(k,p) exists" into a more concrete form. Note that I(k,p) has the property that the theory T[k,p,I(k,p)] has no model. By the completeness theorem for predicate calculus with equality, this means that the theory T[k,p,I(k,p)] is inconsistent. Thus we can put the statement "for all p, I(k,p) exists" in the form

*) for all p, there exists n such that T[k,p,n] is inconsistent,

where any n with this property is at least as large as I(k,p). Note that this statement is of the form

**) $\forall p \exists n$ such that R(p,n),

where R is purely existential.

Step 2. We observe that the statement "$\forall p$, I(k,p) exists" is provable in a certain formal system $WKL_0$. Familiarity with the

technology makes this an easy exercise, and such familiarity can be obtained by looking at [Si99].

Step 3. We also observe that the statment *) is likewise provable in $WKL_0$.

Step 4. Finally, we apply my old metatheorem that any sentence of the form **) that is provable in $WKL_0$ must be primitive recursively true. See [Si99] for a proof of this metatheorem.

Step 5. Thereby conclude that the function I(k,p) of p is bounded by a primitive recursive function.

$WKL_0$ is the so called second principal system of reverse mathematics:

$RCA_0$, $WKL_0$, $ACA_0$, $ATR_0$, $\Pi^1_1$-$CA_0$.

Another way of stating this result is by defining the Ackerman hierarchy of unary functions on N = the set of all nonnegative integers. For each strictly increasing $f:N \to N$, define $f':N \to N$ by $f'(k) = ff...f(1)$, where there are k f's. Take $f_1$ to be doubling. Take $f_{k+1} = (f_k)'$.

A function is bounded by a primitive recursive function if and only if it is bounded by some $f_k$. Thus

THEOREM 1.2. For each k, the function of p, I(k,p), is bounded by some $f_r$.

A more detailed study should reveal a good r = r(k) so that I(k,p) is eventually dominated by $F_r$, and how long you have to wait for the domination. This can probably be done by avoiding the logic and going after the technical guts of the problem. However, there are additional metatheorems from logic that could be used to get some sort of reasonable estimate for this, but perhpas not as good as really getting your hands dirty.

And there is the question of comparing the function I(k,p) of two variables with the function A(k,p) of two varia-bles. We make the same remarks as above.

Notice that we have avoided saying that the functions I(k,p), k fixed, is primitive recursive. In fact, we don't even know if they are recursive.

CONJECTURE: Each I(k,p), k fixed, is primitive recursive. I(k,p) is recursive.

We now come to lower bounds. We will even discuss the lower bounds to the weaker theorem that requires the i-th ideal to have degree exactly p+i+1 - not just $\leq$ p+i+1.

We can already get big lower bounds if we just look at ideals consistting entirely of monomials with coefficient 1, no matter what the field is.

We use N for the set of all nonnegative integers. For n in Nk, write M(x) for the monomial $x_1^{n_1}...x_k^{n_k}$.

LEMMA 1.3. Let F be a field, A $\subseteq$ $N^k$, and n $\in$ $N^k$. M(n) is in the ideal generated by {M(m): m $\in$ A} if and only if there exists m $\in$ A such that m $\leq$ n coordinatewise. Also the ideal generated by {M(m): m $\in$ A} has presentation degree exactly the maximum of the $l_1$ norms of the elements of A.

LEMMA 1.4. Let F be a field. Let $n_1,...,n_r \in N^k$ have $l_1$ norms p+1,...,p+n, where for no i < j is $n_i \leq n_j$ coordinatewise. Then L(F,k,p) > r.

In 3 dimensions, can have $l_1$ norms p+1,...,$p+2^n$. Then we can start an induction through the Ackerman hierarchy of functions. Get L(F,k,p) > A(k-1,p) for k $\geq$ 3. With more work, can do better.

Gallo and Mishra, A solution to Kronecker's problem, Applicable Algebra in Engineering, Communication and Computing, 5(6):343-370, 1994,

consider such chains of ideals - only over the integers - in connection with the polynomial ideal membership problem over the integers. The latter problem was given an effective procedure by

Ayoub, On constructing bases for ideals in polynomial rings over the integers, J. of Number Theory, 17:204-225, 1983.

Gallo and Mishra show that upper bounds for these chains give upper bounds for the sizes coming up in this ideal membership problem. Gallo and Mishra give upper bounds in terms of the Ackerman func-tion. In our setup, their upper bounds would involve looking at the 8k-th level of the Ackerman hierarchy in dimension k. They do not discuss lower bounds, although the above lower bounds would serve for their chains also. However, there are no good lower bounds for the polynomial ideal membership problem over the integers. Over the standard fields, it is known to be at most double exponential (Hermann, etcetera).

I suspect that one could read off primitive recursive bounds from Ayoub's paper using logic, thereby obtaining the main conclusion of Gallo and Mishra immediately from Ayoub, but I have to look.

## 2. ALGEBRAIC SETS IN K DIMENSIONS OVER A FIELD.

Let F be a field and $k \geq 1$. An algebraic set in $F^k$ is the set of simultaneous zeros of a system of polynomials in k variables over F.

The presentation degree of an algebraic set in $F^k$ is the least d such that there is a set of generators for I consisting entirely of polynomials of degree at most d.

Note that by linear algebra, there is a number f(k,d) such that for all fields F, any algebraic set in $F^k$ of presen-tation degree at most d in the k variable polynomial ring over any field is the zero set of a system of k variable polynomials of degree at most d, of cardinality at most f(k,d).

THEOREM 2.1. For all k,p there exists n such that the follow-ing holds. Let F be a field. There is no strictly decreasing sequence of algebraic sets in $F^k$, indexed from 1 through n, such that the i-th set is of presentation degree $\not\leq$ p+i.

Notation: Let A be algebraic in $F^k$. Write I(A) for the ideal of all k variable polynomials over F which vanish on A.

Theroem 2.1 follows immediately from

LEMMA 2.2. Let F be a field and A,B be algebraic in $F^k$, where $A \supseteq\neq B$. Then $I(A) \not\subseteq I(B)$. Also the degree of I(A) is at most the presentation degree of A.

Proof: Assume hypotheses. Clearly $I(A) \subseteq I(B)$. Now the presenting polynomials for B do not vanish on all of A, and so I(B) does not vanish on all of A. Hence I(B) is not I(A).

In fact, this argument shows that any upper bound for Theorem 1.1 is an upper bound for Theorem 2.1.

Now we discuss the lower bounds for Theorem 2.1. In fact, define L(F,k,p) to be the longest strictly decreasing of algebraic sets in $F^k$, indexed from 1, such that the presentation degrees successively go up by 1, starting with presentation degree p. We give lower bounds for L(F,k,p) that work for all infinite fields F simultaneously.

By the upper bound results for ideals, we can, for each k, find primitive recursive upper bounds for L(F,k,p) that work for all fields F simultaneously.

Fix dimension k, an infinite field F, and $p \geq 1$. We will show that L(F,k,p) is large by showing that it is at least as large as a number arising out of a purely combinatorial problem about finite trees. We do this by constructing a very long sequence of sets algebra-ic in $F^k$ of presentation degrees p,p+1,...,p+n.

Our long sequence of algebraic sets will actually be finite unions of finite intersections of equations $x_i = c_i$, where only some of the $1 \leq i \leq n$ are mentioned.

The first order of business is to show that if we have a decreasing sequence of algebraic sets $A_1,A_2,...,A_n \subseteq F^k$ of degrees $\geq p, \geq p+1,...,\geq p+n$, where each $A_{i+1} \backslash A_i$ is infinite, then we can adjust them to have degrees p,p+1,...,p+n.

LEMMA 2.3. Let A be algebraic in $F^k$ of degree d and b in $F^k$. Then $A \cup \{b\}$ has degree $\leq d+1$.

Proof: Let $b = (b_1,...,b_k)$, and $A' = A \cup \{b\}$. Then A' is the intersection of the sets $B_i = A \cup \{x: x_i = b_i\}$. Let A be the common zeros of a set of polynomials X. Now $B_i$ consists of the common zeros of the set of polynomials obtained by multi-

plying the elements of X by $x_i - b_i$. Hence A' has degree $\leq$ d+1. QED

LEMMA 2.4. Let A be algebraic in $F^k$ of degree d and d' $\geq$ d. Then finitely many elements can be added to A so that the degree is exactly d'.

Proof: By Lemma 2.3, we can succeively add points without increasing the degree by more than one. Thus it suffices to show that we cannot succes-sively add points forever and keep the degrees bounded. If we could, we would get arbitrarily long strictly descend-ing sequences of algebraic sets, all with a bound on the degrees. This violates Theorem 2.1, or even linear algebra. QED

LEMMA 2.5. Let $A_1,A_2,...,A_n$ be strictly decreasing sets algebraic in $F^k$ with degrees $\delta_p,\delta_{p+1},...,\delta_{p+n}$, where each $A_{i+1}\backslash A_i$ is infinite. Then we can find such $A_1',A_2',...,A_n'$ with degress p,p+1,...,p+n.

Now we construct long such $A_1,A_2,...,A_n$. Let T be a finite tree with at least two vertices, where every path excluding the root is of length $\leq$ k. Assume that every vertex except the root is labeled by an element of F, where no label is repeated. The algebraic meaning of a vertex at the i-th level above the root with label c is that $x_i = c$. The algebraic meaning of a path is the conjunction of the algebraic meaning of each vertex along that path other than the root. The algebraic meaning of the tree T is the set [T] of all elements of $F^k$ that obey the algebraic meaning of at least one of the paths.

These T are called the good trees.

Thus [T] is a certain union of intersections. The length of the union is #T = the number of terminal vertices of T. When we write [T] as an intersection of unions, note that the unions are still of length #T, although there may be redundancies. Write each union as a monomial by multiplying the relevant factors x-c. Hence the degree of [T] is at most #T.

We need to develop a sufficient criterion for [T] to properly contain [T'].

LEMMA 2.6. Let T,T' be good trees. Suppose T' is obtained from T by adding one or more child to a terminal vertex. Or suppose T' is obtained from T by deleting one of the children of a vertex that has at least two children (and of course all vertices above the one deleted). Then [T] properly contains [T']. Also [T]\[T'] is infinite.

Now all we have to do is to deal with the combinatorics of these two tree operations. Obviously any good tree with only a root and children of the root has degree equaled to the number of children.

Let G(k,p) be the longest sequence of good trees of height k starting with a root with p children, where each tree is obtained from the preceding tree by one of these two operations, and has 1 more terminal vertex.

Let's look at G(k+1,p). Make p children to a root. Off of the first child create two children, and imitate the sequence used there for G(k,1). When finished there, we will have G(k,1)+p-1 terminal vertices. Remove this left child and all vertices above it, leaving p-1 terminal vertices, and then create G(k,1)+2 children above the second original child of the root. Continue this process p times. This is at least the iteration of G(k,_) p times starting at 1. So we have at least primitive recur-sion, provided we can get going. We don't get going with k = 1 since G(1,p) = p. But G(2,p) = (p)(p+1). So we get G(k,p) ≥ A(k-1,p), k ≥ 2. In particular, G(3,p) > $2^{2^{\wedge}p}$, G(4,p) > E*(2p). Detailed calculations give G(4,1) = $2^{2^{\wedge}72}$ and G(4,1) = 2^2^2^2^72.

## 3. SEMILINEAR DYNAMICS

Semilinear dynamics appears not only of interest in its own right, but also can serve as an elegant interpretation of recursion theory.

The basic idea is that ration-al semilinear functions simulate Turing degrees. In par-ticular, the structure of orbits has the requisite power.

A semilinear set in $R^n$ is a finite Boolean combination of halfplanes in $R^n$. Halfplanes are given by T(x) > 0 or T(x) ≥ 0, where T is an affine tranformation (the shift of a linear transformation).

A rational semilinear set in Rn is a finite Boolean combination of rational halfplanes in $R^n$. Rational halfplanes are given by $T(x) > 0$ or $T(x) \geq 0$, where T is an affine transformation whose matrix (including coordinates of the constant term) has only rational entries.

A (rational) semilinear func-tion from $R^n$ into $R^m$ is a function whose graph is (rational) semilinear in $R^{n+m}$.

Quantifier elimination for the field of real numbers is more than enough to establish var-ious nice properties of semilinear functions. Quantifier elimination for the ordered group of real numbers is enough to establish various nice properties of rational semilinear functions.

An important special case is that of rational continuous semilinear functions from $R^2$ into $R^2$, and also from $[0,1]^2$ into $[0,1]^2$.

The basic idea behind the re-sults is that there is a us-able simulation of Turing machines in the rational semilinear functions on R and on $I^2$, and also in the continuous ones.

A Turing machine computation can be viewed as proceeding on a finite tape of squares, each holding a symbol from a finite alphabet of "symbols", with the reading head hovering above one of the squares, and where the machine as a whole is viewed as being in one of another finite alphabet of "states". We assume that these two alphabets are disjoint. The machine instructions are a list of quadruples

qaa'q'
qaRq'
qaLq'

The first means "if you are in state q and reading symbol a then replace it with symbol a' and go into state q'." The second means "if you are in state q and reading symbol a then move to the right and go in state q'." The third means "if you are in state q and reading symbol a then move to the left and go in state q'."

It is required that there are no conflicting quadruples; i.e., no two quadruples have the same first two terms.

There is a special element among the states called the initial state, and there is a special symbol called the blank.

Certain of the symbols are designated as input symbols, and certain are designated as output symbols. Some symbols are neither input nor output symbols. The blank cannot be an input or output symbol.

Inputs are strings of input symbols, and outputs are strings of output symbols. Computation is initiated by creating squares of tape to hold the input string preceded by the first square holding the blank, and on which the reading head rests. The machine is put into the initial state.

Output occurs if and when no instruction applies. The output consists of the string formed by the output symbols on the tape from left to right.

No squares of tape are ever destroyed. However, a new square of tape is created whenever a left or right instruction goes over the left or right edge. The new square is considered to have the blank placed on it.

Suppose the combined set of symbols and states is $\{v_0,...,v_p\}$, where $v_0$ is the blank. At any stage of computation, the global state of the machine is represented by

$x_1x_2...x_n:y_1y_2...y_m$

where $n \geq 0$ and $m \geq 2$. The colon indicates that the read-ing head is hovering over $y_1$, where $y_1$ is the state, and is reading the symbol $y_2$. The x's indicate the symbols to the left of the reading head, and the remaining y's indicate those to the right of the reading head.

We can represent this as an element of $[0,1]^2$ as follows.

$(.x_nx_{n-1}...x_1, .y_1y_2...y_m)$

where these are decimals in base 2p, with the blank $v_0$ recorded as 0, and $v_1,...,v_p$ recorded as $2,4,...,2p$.

Then the quadruples can be executed by simple rational semilinear functions on [0,1]. We only care about the action on the set of finite decimals in base 2p with even digits. In

fact, we can make the provisional domain the set of all elements of $[0,1]^2$ that can be written in base 2p, whose first coordinate has an even first digit, and whose second coordinate has its first two coordinates even. This amounts to having a provisional domain consisting of the union of a finite set of pairwise dis-joint closed rectangles. The function is rational affine on each rectangle. The mapping sends elements of $[0,1]^2$ that can be written as an infinite pair of decimals with even digits into themselves.

Now any rational continuous semilinear function defined on this provisional domain can be extended to a rational contin-uous semilinear function on $I^2$, or even on $R^2$.

In some constructions, we need to venture into decimals with no restrictions on the digits, rather than the more safe situation above. This has to be done carefully, especially if we are to stay continuous. So some of the results below are stated without continuity and some with. I won't be sure that I can stay within the continuous functions until a detailed writeup.

Let $f:X \to X$ and $x \in X$. The orbit of f at x is $\{x,fx,ffx,...\}$. The diameter of a nonempty bounded subset of the plane is the sup of the Euclidean distance between pairs of points in the subset.

THEOREM 3.1. The diameters of the bounded orbits of rational semilinear functions on $R^2$ at rational points are exactly the r.e. positive real num-bers. These are the positive real numbers whose left cut is an r.e. set of rationals.

The r.e. positive reals seem interesting. E.g., what can you say about their base 2 expansions? They are closed under addition and multiplica-tion, but not subtraction or division. Any recursive inc-reasing homeomorphism of R+ is an automorphism of the r.e. positive reals, but what other kinds of automorphisms should be sought?

THEOREM 3.2. The diameters of the bounded orbits of rational semilinear functions on $R^2$ at x are exactly the positive real numbers that are r.e. in x. As a consequence, let $x,y \in R^2$. Then x is recursive in y if and only if the diamaters obtained in this way from x are obtained in this way from y.

THEOREM 3.3. The r.e. subsets of $Z^2$ are exactly the integer points in orbits of rational continuous semilinear functions on $R^2$.