A Zero Structure Theorem for Exponential Polynomials

Daniel Richardson,
Department of Mathematics, University of Bath *
email : dsr@uk.ac.bath.maths

Abstract

An exponential system is a system of equations ($S = 0, E = 0$), where S is a finite set of polynomials in $\mathbf{Q}[x_1, ..., x_n, y_1, ..., y_n]$, and E is a subset of $\{y_1 - e^{x_1}, ..., y_n - e^{x_n}\}$. In this paper, Wu's method is used effectively to decompose such systems into finitely many subsystems which have triangular algebraic part, and whose solution sets in C^{2n} are equidemensional and also, in a sense to be explained, non singular. The problem of solving exponential systems in bounded regions of R^n is also discussed.

1 Introduction

An exponential system is a system of equations $S = 0, E = 0$, where S is a finite set of polynomials in $\mathbf{Q}[x_1, ..., x_n, y_1, ..., y_n]$, and E is a subset of $\{y_1 - e^{x_1}, ..., y_n - e^{x_n}\}$. In this paper, Wu's method is used effectively to decompose such systems into finitely many subsystems which have triangular algebraic part, and whose solution sets in C^{2n} are equidemensional and also, in a sense to be explained, non singular.

The resulting zero structure theorem is partly motivated by interest in the elementary points and numbers, defined as follows: an *elementary point* is a point in C^{2n} which is a non-singular solution of an exponential system $(S, E) = 0$, whose solution set has dimension 0; an *elementary number* is a complex number of the form $p(x_1, ..., x_n, y_1, ..., y_n)$, where p is a polynomial with rational coefficients, and $(x_1, ..., x_n, y_1, ..., y_n)$ is an elementary point.

A basic unsolved problem about the elementary numbers is how to decide, given a description, as above, of an elementary number, whether or not the number is zero. This is called the elementary constant problem [see Richardson, 1992]. The elementary constant problem is related to Schanuel's conjecture, which says that if $x_1, ..., x_n$ are complex numbers linearly independent over the rationals, then $(x_1, ..., x_n, e^{x_1}, ..., e^{x_n})$ have transcendence rank at least n.

In the second section, two simple applications of the zero structure theorem are given. It is shown that if a point in C^{2n} is an isolated solution of an exponential system, then the point itself is elementary, that is, another system can be found of which the point is a non singular solution. It is also shown that any counterexample to Schanuel's conjecture is necessarily elementary, unless it is part of a curve of counterexamples.

The zero structure theorem can also be used to help decide whether or not an exponential system has a solution in a bounded region in R^n, and to find all the solutions if it does have any. The idea here is to break the zero set of a system up into non singular parts, and then to use topological methods to solve the parts. This is discussed in the last section. The problem of solving zero dimensional exponential systems is reduced to certain oracles, notably an oracle for the elementary constant problem.

2 Zero Structure Theorem

Assume that the variables, $x_1, ..., x_n, y_1, ..., y_n$ are ordered in some way by importance, and extend this in the usual way to lexicographic order on the polynomials.

Systems in triangular form are in some ways easy to deal with and understand. Wu's method is a systematic way to put systems of equations in triangular form. The basic definitions, given below, are from Wu.

2.1 basic definitions for Wu's method

The leading variable of a polynomial is the variable most important in the ordering which occurs in the polynomial. We assume here that polynomials are written, in normal form, as polynomials in their leading variable,

*This paper was written with the support of CEC, ESPRIT BRA contract 6846 "POSSO"

ACM-ISSAC '93-7/93/Kiev, Ukraine
© 1993 ACM 0-89791-604-2/93/0007/0144...$1.50

with coefficients which are polynomials, also in normal form, in less important variables. So if y is the leading variable of a polynomial p, p would be in the form

$$C_n y^n + \ldots + C_0$$

where n is called the degree of p, and C_n, assumed to be non zero, is called the leading coefficient of p.

If p and q are polynomials, and y is the leading variable of q, we will say that p is reduced with respect to q if the degree of y in p is less than the degree of y in q. It may happen that p is reduced with respect to q although the leading variable of p is more important than the leading variable of q.

For polynomials p and q, we will say $p \prec q$ if the leading variable of p is less important than the leading variable of q, or if the leading variables are the same and the degree of p is less than the degree of q. If both the leading variables and the degrees of p and q are the same, we will say $p \sim q$.

Let $S = (p_1, \ldots, p_r)$ be a list of polynomials. We will say that S is an ascending set if, for each $i < r$, the leading variable of p_i is less important than the leading variable of p_{i+1}, and if, for all $j < i$, p_i is reduced with respect to p_j.

The next step is to put an order on ascending sets. If $S_r = (p_1, \ldots, p_r)$ and $S_s = (q_1, \ldots, q_s)$ are ascending sets, we will say $S_r \prec S_s$ if, for some k, $p_1 \sim q_1$ and ... and $p_k \sim q_k$ and $p_{k+1} \prec q_{k+1}$, or if $s < r$ and $p_1 \sim q_1$ and ... and $p_s \sim q_s$.

Ascending sets are well ordered by $\prec$.

If p and Q are polynomials, let $pseudoRemainder(Q, p)$ be the result of expressing p and Q as polynomials in the leading variable of p, dividing p into Q, and then multiplying the remainder by some power of the leading coefficient of p to clear denominators.

If $S = (p_1, \ldots, p_r)$ is an ascending set , and Q is a polynomial, there is a polynomial $Rem(Q, S)$, which is reduced with respect to every polynomial in S, and satisfies

$$\prod I_i^{n_i} Q = \sum q_i p_i + Rem(Q, S)$$

where I_i is the leading coefficient of p_i, and the exponents n_i are chosen to be minimal. $Rem(Q, S)$ is obtained by successive division of polynomials of S into Q, and then clearing denominators. That is, $Rem(Q, (p_1, \ldots, p_r)) = Rem(pseudoRemainder(Q, p_r), (p_1, \ldots p_{r-1}))$. $Rem(Q, S)$ is called the pseudo remainder of Q with respect to S.

Characteristic set algorithm: Using the method of Wu, we can, given any finite set S of polynomials, find an ascending set A so that the polynomials in A are all in the ideal generated by the polynomials in S, and $Rem(Q, A) = 0$ for all Q in S. Thus $A = 0$ implies $S = 0$, provided that $I(A) \neq 0$, where $I(A)$ is the product of the leading coefficients of A. Such an ascending set A is called a characteristic set of S. A method of finding a characteristic set is the following. First pick any ascending set, A_1, of minimal order, which is a subset of S. Then find pseudo remainders of members of S with respect to A_1. If all the pseudo remainders are 0, then A_1 is characteristic. If not all pseudo remainders are zero, use a non zero remainder to construct an ascending set A_2 of lower order than A_1, with the polynomials in A_2 in the ideal generated by S. Continue this process. The ascending sets generated are decreasing in order, and the ordering on ascending sets is well founded, so the process eventually terminates with a characteristic set.

2.2 Decomposition of algebraic and exponential systems

If S is a finite set of polynomials, in variables $z_1, \ldots, z_k$, let $C^k(S = 0)$ be the subset of complex k space on which $S = 0$. In general, if Ls is a list of conditions, using k variables, $C^k(Ls)$ will be the subset of C^k on which Ls is true.

Wu-Ritt Zero Structure Theorem. *Given any finite set of polynomials, S, in variables $z_1, \ldots, z_k$, we can effectively write $C^k(S = 0)$ as a union, for $i = 1, \ldots, m$ of $C^k(S_i = 0, I_i \neq 0)$, where S_i is an ascending set and I_i is the product of leading coefficients of S_i.*

Proof. (Slightly modified from Wu.) We generate a list of ascending sets as follows. Suppose we find A, a characteristic set of S. Let I be the product of leading coefficients of A. We note

$$C^k(A = 0, I \neq 0) \subseteq C^k(S = 0) \subseteq C^k(A = 0)$$

Take the pseudo remainder, R, of I with respect to A. If this is not zero, add $(A = 0, I \neq 0)$ to the list of ascending sets. Then add R to S, and repeat the process.

It might happen, however, that the remainder of I with respect to A is zero. This means that $(A = 0, I \neq 0)$ is not possible. We know then that one of the leading coefficients of A must be zero, but we don't know which one. Let $C_1, \ldots, C_r$ be a minimal sublist of the leading coefficients of polynomials in A, such that their product has pseudo remainder zero with respect to A. Form S_i, for $i = 2, \ldots, r$ by adding C_i to S. Continue the process with each S_i in turn, terminating each branch only when an inconsistent ascending set is formed, i.e. one which sets a non zero rational to zero. On each branch the ascending sets constructed are descending in order, so the whole process eventually terminates.

In an ascending set, call the leading variables of polynomials dependent, and the other variables independent. The Wu-Ritt zero structure theorem breaks algebraic sets into unions of sets defined by ascending sets. It would be nice if an ascending set had the property that its dependent variables were always locally defined as non singular functions of the independent variables. An ascending set modified to have this property will be called stable. Only a small change is needed to get this desirable property.

We define a stable ascending set of conditions to be $(S = 0, I \neq 0, J \neq 0)$, where S is an ascending set and I is the product of leading coefficients of S, and J is the product of the partial derivatives of the polynomials in S with respect to their leading variables.

Note that if $(S = 0, I \neq 0, J \neq 0)$ is a stable ascending set, and we regard the independent variables as parameters, then S has the same number of dependent variables as functions, and J above is just the determinant of the Jacobian of S.

Stable Algebraic Zero Structure Theorem *Given any finite set of polynomials, S, in variables $z_1, ..., z_k$, we can effectively write $C^k(S = 0)$ as a union, for $i = 1, ..., m$ of stable ascending sets $C^k(S_i = 0, I_i \neq 0, J_i \neq 0)$, where S_i is an ascending set and I_i is the product of leading coefficients of S_i, and J_i is the product of the partial derivatives of the polynomials in S_i with respect to their leading variables.*

Proof. The proof is almost the same as before. Let A be a characteristic set of S. Let I be the product of leading coefficients, and let J the the product of partial derivatives of polynomials in A with respect to their leading variables. Of course $(A = 0, I \neq 0, J \neq 0)$ is a stable ascending set of conditions. Now form the product of J and I and take the pseudo remainder of this with respect to A. Call this remainder R.

If R is non zero, put the stable ascending set $(A = 0, I \neq 0, J \neq 0)$ on the list being constructed. Then add R to S and continue as before.

Otherwise, if R is zero, we know that one of the factors of I or J must be zero. All of these factors by themselves are reduced with respect to A. Form a minimal sublist of these factors whose product has remainder zero with respect to A. The algorithm branches as above, one branch for each factor in the sublist.

2.3 Exponential Systems

The intention now is to carry the above constructions over to exponential systems. We want to break the zero sets up into equidimensional, non singular parts.

Exponential systems are complicated by the not very well understood interaction between algebraic and exponential conditions.

Example.

$$(x_1 - 1)(x_1 - 2) = 0$$

$$2x_1 + x_2 - x_3 = 0$$

$$y_1^2 y_2 - x_1 y_3 = 0$$

$$y_1 = e^{x_1}$$

$$y_2 = e^{x_2}$$

$$y_3 = e^{x_3}$$

As it stands this set of equations is not independent. The value of x_1 must be 1, so the third equation is a consequence of the others and the functional equation for e^x. So the same zero set could be defined from two polynomial equations, and three exponential equations.

However, one of the main problems about exponential systems is how to extract all the algebraic information which is implicit in them. We want to put as much information as possible into the algebraic part of the system. The hope, in fact, is that all the algebraic consequences of the whole system should be already consequences of the algebraic part of the defining equations of the system.

¿From the point of view of this paper, the above example would break into three parts: 1) the three polynomial equations, 2) the first two exponential equations, and 3) the last exponential equation, which is called redundant. The first five equations are independent. The zero set defined by the first five equations divides into two branches, depending on the value of x_1. On one of the branches, the redundant equation is identically true; on the other branch, the redundant equation is never satisfied. The only effect of the redundant equation is to pick out a certain subset of the connected components defined by the other equations. In this example, the subset can also be defined algebraically, but I don't know whether or not this always happens.

In this example the solution set may be described as a curve, with all variables defined as functions of x_2. So we would say x_2 can be taken as an independent variable, and the others can be taken as dependent. On the curve the transcendence rank of $(x_1, y_1, x_2, y_2, x_3, y_3)$ is three at a generic point x_2, but drops to one if x_2 is rational.

In general, low transcendence rank of $(x_1, ..., x_n, y_1, ..., y_n)$ in exponential systems is related to linear relations among $(x_1, ..., x_n)$. The best discussion of this is in a paper by Rosenlicht [1976].

Before the zero structure theorem we need some definitions.

If p is a polynomial, let ∇p be the gradient of p. This gradient is orthogonal to any level surface of p.

Let $v(x_1), ..., v(x_n), v(y_1), ..., v(y_n)$ be unit vectors on the coordinate axes for variables $x_1, ..., x_n, y_1, ..., y_n$ respectively. Associated with each exponential condition $y_i = e^{x_i}$ is the polynomial vector field

$$-y_i v(x_i) + v(y_i)$$

which is orthogonal to the graph of this exponential function, $x_i v(x_i) + e^{x_i} v(y_i)$.

As before we suppose that E is the full set of exponential conditions, $\{y_1 - e^{x_1}, ..., y_n - e^{x_n}\}$, and let E_1 be a subset of E. Suppose E_1 is $\{w_1 - e^{z_1}, ..., w_j - e^{z_j}\}$. Let $S = \{p_1, ..., p_r\}$ be a set of polynomials in $\mathbf{Q}[x_1, ..., x_n, y_1, ..., y_n]$. We will say that the conditions $(S = 0, E_1 = 0)$ are independent at a point if the vectors $\{\nabla p_1, ..., \nabla p_r, -w_1 v(z_1)+v(w_1), ..., w_j v(z_j)+v(w_j)\}$ are linearly independent at that point.

Independence, at a solution point, means that the surfaces described by the separate conditions are transversal. At a general point, independence means that the level surfaces of the functions are transversal at that point.

Associated with the set of vectors is the differential matrix, $df(S, E_1)$. This has r rows from the polynomial gradients, and j rows from the exponential conditions, and it has $2n$ columns. $df(S, E_1) =$

$$\begin{pmatrix} \partial p_1/\partial x_1 & ... & ... & \partial p_1/\partial y_n \\ ... & ... & ... & ... \\ ... & ... & ... & ... \\ \partial p_r/\partial x_1 & ... & ... & \partial p_r/\partial y_n \\ ... & -w_1 & ...1 & ... \\ ... & ... & ... & ... \\ ... & ... & -w_j ... & 1... \end{pmatrix}$$

The $2n$ columns of the differential matrix correspond to the variables, and the rows correspond to equations. We can either think of the matrix as defining a vector field, or we can think of it as defining a relationship among the differentials.

To say that the conditions in $(S, E_1) = 0$ are independent is equivalent to saying that $r+j \leq 2n$ and some maximal (i.e. $r+j$ by $r+j$) minor of the differential matrix has determinant which is not zero. Associated with any such minor is a subset of $r+j$ of the variables.

Define a smooth curve in C^{2n} to be the image of a function $C : [0,1] \to C^{2n}$, each coordinate of which is represented by an absolutely convergent power series on the domain.

We define a *triangular condition* to be one of the form $(S = 0, E_1 = 0, E_2 = 0, I \neq 0, J \neq 0)$, where the following five properties hold:

1) S is an ascending set in $\mathbf{Q}[x_1, ..., x_n, y_1, ..., y_n]$

2) (E_1, E_2) is a partition of the full exponential set E

3) I is the product of the leading coefficients of S

4) $J \neq 0 \to (S, E_1)$ independent; J is the determinant of a maximal minor of the differential matrix. $Rem(J, S) \neq 0$.

5) E_2 is such that if $C(t)$ is any smooth curve in C^{2n} on which $(S = 0, E_1 = 0, I \neq 0, J \neq 0)$, then any $y_i - e^{x_i}$ in E_2 is either identically zero on $C(t)$ or never zero.

The conditions in E_2 will be called redundant. On each connected component defined by the other conditions, the redundant conditions are either identically true, or never true. The redundant conditions pick out a subset of the components defined by the others. (In terms of differential algebra, if we extend $Q[x_1, ..., x_n, y_1, ..., y_n]$ to a differential field on which a triangular condition is true, the redundant terms, $y_j - e^{x_j}$, would be constants.)

The determinant J is obtained from some set of columns of the differential matrix. The variables corresponding to these columns will be called dependent. In case several sets of variables would give the same determinant J, we pick the set of dependent variables to be the minimal such set in the lexicographic ordering. The other variables, if any, will be called independent. Since $J \neq 0$, the dependent variables are locally smooth non singular functions of the independent ones. The set defined by a triangular condition is either equidimensional and non singular, or empty. If non empty, the dimension can be read off: it is $2n - r - j$.

Triangular conditions are ordered according to the order on their ascending sets.

Let $(S = 0, E = 0)$ be an exponential system. A maximal triangular condition for this is a condition $(A = 0, E_1 = 0, E_2 = 0, I \neq 0, J \neq 0)$, where

1) A is an ascending set and a subset of the ideal generated by S, and I is the product of the leading coefficients of A

2) $Rem(S, A) = 0$, $Rem(J, A) \neq 0$

3) $J \neq 0$ implies that $(A = 0, E_1 = 0)$ are independent.

4) E_1 is maximal. This means that if we formed E_1^+ by taking an exponential $w - e^z$ from E_2 and adding it to E_1, and if J^+ was the determinant of any maximal sized minor of the differential matrix associated with $(A = 0, E_1^+ = 0)$, then $Rem(J^+, A) = 0$.

5) (E_1, E_2) is a partition of E

Maximal triangular conditions play the same role for exponential systems as characteristic sets do for polynomial systems.

Maximal triangular conditions are also triangular conditions. We need to verify that the conditions E_2 are redundant. Let $C(t)$ be a smooth curve in C^{2n}. Suppose that on $C(t)$ we have $(A = 0, E_1 = 0, I \neq 0, J \neq 0)$. So $C(t)$ is orthogonal to the vectors associated with

$(A = 0, E_1 = 0)$. Let $w - e^z$ be in E_2. $-wv(z) + v(w)$ is a linear combination of vectors orthogonal to $C(t)$. Let $z(t)$ and $w(t)$ be the components of z and w on $C(t)$. We have $z'(t)w - w'(t) \equiv 0$. Thus $w = ke^z$, for some constant k on $C(t)$. So $w - e^z$ is either never 0 or identically zero on the curve.

It is clear that maximal triangular sets can be found for any exponential system $(S = 0, E = 0)$. We just find a characteristic set A for S, and then pick E_1 maximal. The maximality condition depends only on taking pseudo remainders, and can, therefore, be tested.

Stable Exponential Zero Structure Theorem. *For any exponential system, $(S = 0, E = 0)$, we can effectively find finitely many triangular conditions $\Delta_i = (S_i = 0, E_{1,i} = 0, E_{2,i} = 0, I_i \neq 0, J_i \neq 0)$, $i = 1, ..., k$ so that*

$$C^{2n}(S = 0, E = 0) = \bigcup_{i=1,...,k} C^{2n}(\Delta_i)$$

Proof. Find a maximal triangular set for $(S = 0, E = 0)$. Suppose this is $(A = 0, E_1 = 0, E_2 = 0, I \neq 0, J \neq 0)$. Let $R = Rem(I * J, A)$. If R is not zero, add the maximal triangular condition to the list being formed. Also add R to S, and continue the process. In case R is zero, we know that the maximal triangular condition we have found is impossible. Either J or one of the factors of I must be zero if S is zero. Choosing from J and the set of leading coefficients, form a minimal product which has pseudo remainder zero. Let $C_1, ..., C_r$ be the factors in this minimal product. Now form $S_1, ..., S_r$ by adding, respectively $C_1, ..., C_r$ to S. Continue the process on each of $S_1, ..., S_r$.

The process terminates because the triangular conditions found on each branch of this process are decreasing in order.

Remark. It seems useful to think of the triangular sets obtained above as arranged in a tree. The subtree below each triangular condition $(S = 0, E_1 = 0, E_2 = 0, I \neq 0, J \neq 0)$ is a decomposition of $(A = 0, S = 0, E_1 = 0, E_2 = 0, IJ = 0)$, where (A, E_1, E_2) is the original system.

Sampling Theorem *Let X be a connected component of the solution set, in C^{2n} or R^{2n}, of an exponential system $(S, E) = 0$. Then X contains an elementary point.*

Proof. We may as well assume that X is described by a triangular condition of dimension d, $(A = 0, E_1 = 0, E_2 = 0, I \neq 0, J \neq 0)$. All we need is to find some lower dimensional subset of X which is described by an exponential system. This can be obtained from any non constant function which has a minimum or a maximum on X, regarding everything as a function of the independent variables. For this function we could use, for example, a sum of the squares of the variables and $(1/I)^2 + (1/J)^2$; it is not possible to escape from the component without sending such a sum to infinity, so the sum must have a minimum point on the component. Or, more simply, since the dependent variables are locally functions of the independent ones, we could just substitute some rational numbers for the independent variables.

3 Applications

The point of the first theorem is just that isolated solutions of an exponential system are also non singular solutions of another exponential system.

Theorem *If α is a point in C^{2n} which is an isolated solution of an exponential system $(S = 0, E = 0)$, then α is an elementary point.*

Proof. Decompose $(S = 0, E = 0)$ into triangular conditions, as in the zero structure theorem. The point α must satisfy one of these conditions, say $(A = 0, E_1 = 0, E_2 = 0, I \neq 0, J \neq 0)$. A triangular condition satisfied by α can't have dimension greater than zero, or α would not be isolated. So α satisfies a triangular condition of dimension zero, i.e. α is a non singular solution of $A = 0, E_1 = 0)$. So α is elementary.

Theorem *Either every counterexample to Schanuel's conjecture is elementary, or there is an analytic non constant curve $(x_1(t), ..., x_n(t))$ such that $(x_1(t), ..., x_n(t))$ are linearly independent over the rationals, but the transcendence rank of $(x_1(t), ..., x_n(t), e^{x_1(t)}, ..., e^{x_n(t)})$ is $< n$.*

Proof. Let $(x_1, ..., x_n)$ be a counterexample to Schanuel's conjecture. The numbers $(x_1, ..., x_n)$ are linearly independent over the rationals, and $(x_1, ..., x_n, e^{x_1}, ..., e^{x_n})$ has transcendence rank less than n. Let $(y_1, ..., y_n) = (e^{x_1}, ..., e^{x_n})$. Let S be an ascending set of lowest order so that $S = 0$ at this point. S has more than n polynomials in it. Now decompose $(S = 0, E = 0)$ into triangular conditions. Let $(A = 0, E_1 = 0, E_2 = 0, I \neq 0, J \neq 0)$ be a triangular condition in this decomposition which contains $(x_1, ..., x_n, y_1, ..., y_n)$.

If the dimension of the set defined by this condition is zero, the points are elementary, and we are finished.

Suppose the dimension of the set defined by this condition were more than zero. Let $(x_1(t), ..., x_n(t))$ be an analytic curve in the solution set. These functions are linearly independent over the rationals. On the other hand, A has more than n independent polynomials in it, so the transcendence rank of $(x_1(t), ..., x_n(t), e^{x_1(t)}, ..., e^{x_n(t)})$ is less than n.

4 Finding real solutions of exponential systems

Let (S, E) be an exponential system, and suppose $f = (S, E) : R^k \to R^k$. Let D be an open bounded semialgebraic subset of R^k. We want to discover the number of distinct solutions of $f = 0$ in D and isolate them.

We will suppose known in advance that $f = 0$ has at most finitely many solutions in D, and that there is no solution on the boundary of D. It is shown below that the problem can be solved, provided we had oracles for three other problems:

p1) The elementary constant problem

p2) Find the topological degree of $f = (A, E) : R^k \to R^k$ over a domain D' which is an open, bounded semialgebraic subset of R^k, and which has no solution of $f = 0$ on its boundary.

p3) Given isolated solution α of exponential system $(S = 0, E = 0)$ in D, find a neighbourhood $N_\epsilon(\alpha)$ which contains only one solution of $(S = 0, E = 0)$. (The system here may have any finite number of equations.) We suppose we are given α in the standard way as the nonsingular solution of an exponential system $(A = 0, E_1 = 0)$, with $2n$ equations and the same number of unknowns. We are also given a neighbourhood in which this defining system for α has only one solution.

Problem p2) can be done by standard methods, involving construction of a triangulation of the boundary of D' [Cronin, 1964]. Some progress has recently been made with p1), depending on Schanuel's conjecture. I do not know how to do the innocuous looking p3).

Note that if D' is a domain in which the Jacobian of f is non singular, and $f = 0$ has no solution on the boundary, then the absolute value of the topological degree of f over D' gives us just the number of solutions of $f = 0$ in the domain. It is remarkable that in such a domain we can decide whether or not $f = 0$ has a solution, even without solving the constant problem.

Theorem *Given oracles for p1), p2), and p3) and given an exponential system $f = (S, E) : R^k \to R^k$, and open, bounded, semialgebraic set $D \subset R^k$, such that $f = 0$ has at most finitely many solutions in D, and has no solutions on the boundary of D, we can decide how many distinct solutions of $f = 0$ there are in D, and isolate them.*

Proof. First decompose $f = 0$ into a tree of triangular conditions, using the exponential zero structure theorem. Discard all the conditions with dimension more than zero, since there are only finitely many solutions in D. (If a condition of dimension more than zero is satisfied at all in D, it is satisfied on a curve.) Now start at the bottom of the tree and work upwards, finding solutions to the conditions.

Assume, inductively, that we are looking at a particular condition

$$\Delta = (A = 0, E_1 = 0, E_2 = 0, I \neq 0, J \neq 0)$$

and that so far we have found, and made a list of, all the solutions to conditions below this.

Now, using p3), we find a little closed neighbourhood around each of these solutions which does not contain any other solution to $f = 0$. Remove the interior of all these neighbourhoods from D to obtain D'.

The solutions to conditions below Δ, which have been removed, were solutions to $(S = 0, A = 0, E = 0, IJ = 0)$. These were not solutions to Δ, (since Δ insists $IJ \neq 0$), and the neighbourhoods we removed did not accidentally contain solutions to Δ, since any solution of Δ must be an isolated solution to $f = 0$. So all the solutions to Δ which were in D are still in D'. There is no solution to $(f = 0, A = 0, IJ = 0)$ in the closure of D'.

Find a number M which is an upper bound for the directional derivatives of all functions in (f, A, IJ) over D. This can be done by standard methods, since the functions only involve addition, subtraction, multiplication and exponentiation.

Now pick a finite set of points in D' so that the closure of D' is covered by balls of radius δ centered at these points. Divide the points, γ, into three categories:

1) $(f = 0, A = 0)$ impossible in $N_{2\delta}(\gamma)$, since one of the functions in (f, A) has absolute value bigger than $2M\delta$ at γ.

2) $IJ = 0$ impossible in $N_{2\delta}(\gamma)$ since IJ is bigger in absolute value than $2M\delta$ at γ.

3) All other points.

Suppose, for the sake of a contradiction, that there were points in category three for arbitrarily small δ. Then there would be a limit point of category three points in the closure of D'. At this limit point we would have $(f = 0, A = 0, IJ = 0)$. Contradiction.

If δ is chosen sufficiently small, category three will be empty and the boundary of D' will be covered by balls around points in category one. Then all solutions lie in δ balls around points in category two. In these balls, consider $g = (A, E_1) : R^k \to R^k$. The Jacobian of g is not zero in one of these balls, since $J \neq 0$.

Now amalgamate the balls around points in category two into connected components. Let C be one of these components. Within C, the zero set of g must be zero dimensional, since J is not zero. On the boundary or within distance δ of the boundary of C, (f, A) is not 0, the Jacobian of g is not zero, and there are at most finitely many isolated solutions of $g = 0$. Within distance δ of the boundary of C, there are no solutions of Δ. It might happen, however, that if δ were picked badly, there could be a solution of $g = 0$ *exactly* on the boundary of C. (Such a point could not be a solution of $f = 0$, but it could still cause trouble in the computation of topological degree for g, since we need the assumption that $g \neq 0$ on the boundary.) Since we know, however, that there is no solution to $f = 0$ within δ of the boundary of C, we do not lose anything by drawing another boundary just inside C.

Inscribe a polyhedron in C so that every vertex is within distance δ of the boundary of C, and all of C which is not within distance δ of the boundary is inside the polyhedron, and none of the vertices of the polyhedron are on the boundary of C. Pick the vertices so that on the boundary of the polyhedron, there is no solution of $g = 0$. The idea is just to pick the vertices at random with rational coordinates, and attempt to verify that (A, E_1) is bounded away from zero on the boundary; if difficulties are met, perturb the vertices in the area of the problem, and try again until the condition is met.

We can calculate the topological degree of g over the polyhedron inside C, by p2). The absolute value of this gives us just the number of distinct solutions of $g = 0$ inside the polyhedron. Once we know the number of solutions, we can isolate them, by random bisection. Using p1), we can then decide which of these are also solutions of Δ.

Continuing up the tree of conditions in this way, we eventually get all the solutions to $f = 0$ in D.

5 Conclusions

The stable exponential zero structure theorem breaks exponential conditions ($S = 0, E = 0$ into finite unions of triangular conditions. This may help in solving the elementary constant problem. It may also help in solution finding for exponential systems. Suppose we have an exponential system ($S = 0, E = 0$) and we know that there are only finitely many solutions in R^n, and we want to find how many there are and locate them. We could break ($S = 0, E = 0$) into triangular conditions. We need only look at the dimension zero triangular conditions. If we could solve these we could solve the original problem. Solutions to triangular conditions are of necessity non singular. Since it may be easier to find non singular solutions (being invariant under homotopy for example), this should make the original problem easier to solve. The general idea is to use algebra to break zero sets into unions of non singular zero sets, and then to use topological methods to find the non singular zero sets.

6 References

J. Ax, Schanuel's Conjecture, Ann Math 93 (1971), 252-68

A. Baker, *Transcendental Number Theory*, Cambridge University Press, 1975

J. Bochnak, M. Coste and M. F. Roy, *Geometrie Algebrique Reelle*, Ergebnisse vol 12, Springer-Verlag, 1987.

B. F. Caviness and M. J. Prelle, A note on algebraic independence of logarithmic and exponential constants, SIGSAM Bulletin, vol 12, no 2, pp 18-20, 1978

Cronin, J., *Fixed Points and Topological Degree in Nonlinear Analysis*, American Mathematical Society, 1964

B. I. Dahn, On Exponential Logarithmic Terms, Fundamenta Mathematicae, vol 127, pp 45-50, 1986

P. Gianni, B. Trager, G. Zacharias, Groebner Bases and Primary Decomposition of Polynomial Ideals, Journal of Symbolic Computation 1988, 6, pp 149-167

G.H. Hardy, Orders of Infinity, Cambridge 1910

S. Lang, *Introduction to Transcendental Numbers*, Addison-Wesley, 1966

N. G. Lloyd, *Degree Theory*, Cambridge University Press, 1978

A. Macintyre, Schanuel's Conjecture and Free Exponential Rings, preprint, Oxford 1991

D. Richardson, Finding roots of equations involving solutions of first order algebraic differential equations, pp 427-440 in *Effective Methods in Algebraic Geometry*, (Teo Mora and Carlo Traverso Eds), Birkhauser 1991

D.Richardson, Wu's method and the Khovanskii finiteness theorem, Journal of Symbolic Computation, 1991, 12, pp 127-141

D. Richardson, Computing the topology of a bounded non-algebraic curve in the plane, J. Symbolic Computation 14, 1992, pp 619-643

D.Richardson, The Elementary Constant Problem, ISSAC 92.

M. Rosenlicht, On Liouville's theory of elementary functions, Pacific Journal of Mathematics, vol 65, no 2, 1976, pp 485-492

B. Salvy, *Asymptotique Automatique et Fonctions Generatrices*, Thesis, Ecole Polytechnique

J. Shackell, Limits of Liouvillian Functions, preprint 1991

N.N. Vorobjov, Deciding consistency of systems of polynomial in exponent inequalities in subexponential time, pp 491-500 in *Effective Methods in Algebraic Geometry*, (Teo Mora and Carlo Traverso Eds), Birkhauser 1991

A.J. Wilkie, Some model completeness results for expansions of the ordered field of real numbers by Pfaffian functions, preprint, Mathematics Institute, Oxford.

S.C. Chou, W. F. Schelter, and J. G. Yang, Characteristic Sets and Grobner Bases in Geometry Theorem Proving, Draft, Institute for Computing Science, The University of Texas, Austin, TX 78712

Wu, W.T., Basic Principles of Mechanical Theorem Proving in Elementary Geometries, J. Sys. Sci. and Math. Scis, f(3), 1984, 207-235