LIMITATIONS TO ALGORITHM SOLVABILITY: GALOIS METHODS AND MODELS OF COMPUTATION

Chanderjit Bajaj

CSD-TR-567
January 1986

Limitations to Algorithm Solvability: Galois Methods and Models of Computation

Chanderjit Bajaj

Department of Computer Science,
Purdue University,
West Lafayette, IN 47907

Abstract: We use simple arguments from Galois theory to prove the impossibility of exact algorithms for problems under various models of computation. In particular we show that there exist applied computational problems for which there are no closed form solutions over models such as $Q(+, -, *, /, \sqrt{})$, $Q(+, -, *, /, k\sqrt{})$, and $Q(+, -, *, /, k\sqrt{}, q(x))$, where Q is the field of rationals and $q(x) \varepsilon Q[x]$ are polynomials with non-solvable Galois groups.

1. Introduction

The now well known Theorem of Abel-Ruffini, (proved by Ruffini in 1813 and independently by Abel in 1827) states that the 'general' equation of nth degree, ($n \geq 5$), is not solvable by *radicals*†. Galois' discoveries in the theory of equations not only provided a proof of the Abel-Ruffini theorem but it gave a criterion for solvability by radicals of any equation not just the 'general' one. Gauss showed that for the integers n=17,257 and 65537 the regular n-gon can be constructed with straight-edge and compass. Gauss' results were obtained by elementary and lengthy calculations involving the roots of unity [J]. With the advent of Galois theory these results can now be obtained rather quickly and elegantly. Our efforts here our modest, but in the same vein. We use simple arguments from Galois theory to answer questions about the impossibility of exact algorithms for problems under various models of computation. In particular we show that there exist applied computational problems for which there are no closed form solutions over models such as $Q(+, -, *, /, \sqrt{})$, $Q(+, -, *, /, k\sqrt{})$, and $Q(+, -, *, /, k\sqrt{}, q(x))$, where Q is the field of rationals and $q(x)$ are polynomials with non-solvable Galois groups. In § 2 we briefly review some standard models of computation and their relation to the models we discuss in subsequent sections. In § 3 we consider the restricted Quadrature computation models $Q(+, -, *, /, \sqrt{})$, and show the existence of two applied problems one which is solvable and the other non-solvable, by Quadrature. The results in this section are quite straightforward however are important in that the minimal polynomials derived therein are used in the following sections.

---

† A real number α is expressible in terms of *radicals* if there is a sequence of expressions $\beta_1, \ldots, \beta_n$, where $\beta_1 \varepsilon Q$, and each β_i is either a rational or the sum, difference, product, quotient or the k^{th} *root* of preceding β's and the last β_n is α.

In § 4 we consider the much stronger Solvable computation models $Q(+, -, *, /, k\sqrt{})$, and prove that certain applied problems are not solvable by radicals over Q. These results were first obtained in [B1], [B2]. In § 5 we consider the even more powerful Algebraic Computation models $Q(+, -, *, /, k\sqrt{}, q(x))$, where even roots of non-solvable polynomials $q(x)$ are allowed. We again prove for the problems of § 4, the impossibility of having exact algorithms which give closed form solutions over these general Algebraic models. These results arise from a series of observations about the structure of the Galois groups. Extensions to higher models and directions for further research are discussed in § 6.

2. Standard Models of Computation

The standard model of computation has been the *real* RAM [AHU], a random access machine with infinite precision, real number arithmetic. It performs addition, subtraction, multiplication, division, comparison and square-roots on real numbers in constant time. To develop fast algorithms we use this *real* RAM, since most of the above operations are available on modern day computers and moreover all of them take approximately the same unit time. Furthermore the size of the parameters and more importantly the size of the intermediate results of the various problems considered, often do not play a critical role in any of these algorithms. Where the size of the intermediate results of the problem does become important a RAM model with *logarithmic* cost criterion is used. The standard *integer* RAM or the *rational* RAM models are similar to the real RAM with constants, variables and operations now defined over Z or Q. At times the RAM models are more complicated than needed and thus a number of models are defined which abstract certain features of the RAM and ignore others. Examples of such models are Straight-line (loop-free) Programs, Bitwise Computations which reflect the logarithmic cost function, Bit Vector Operations and Decision Trees which include the branching instructions.

The model of computation that has been used to prove worst-case lower bounds has been the *decision tree* model. Although this model is less interesting from the computation point of view, many worst-case lower bounds have been proved for it. In this model, algorithms are presented as trees, in which every vertex of the tree has the form of a comparison $f(inputs) : 0$, where f is some function from a class of allowed functions. For *linear* and d^{th} order decision trees, where functions allowed are polynomials of degree at most d (d=1 for linear), several powerful techniques are known [DL],[SY]. These models are similar to the Quadrature models of § 3 as long as d is a power of 2 and furthermore the order of the Galois groups of the d degree polynomials are a power of 2. [G] proves that there exist irreducible polynomials over Q of

degree d which are solvable by Quadrature and for which $d-1$ square root extractions are required to obtain all the roots. Earlier [E] had illustrated a technique using method of logic, to obtain lower bounds of complexity $\Omega(logd)$ for polynomials of degree n over the Solvable Computation models of § 4. The lower bounds obtained for the linear and d^{th} order decision tree models were significantly improved for the powerful *Algebraic Computation Tree* (*ACT*) model [BO]. Our Algebraic models of § 5 are closely related to the *ACT* though not as general. The basic limitation of the *ACT* is that given a polynomial of degree d in n variables, the best lower bound complexity that can be derived for evaluating the polynomial is $\Omega(n \log d)$.

3. $Q(+, -, *, /, \sqrt{})$ Quadrature Computation Models

The complexity of straight-edge and compass constructions has for long known to be equivalent to the geometric solution being expressible in terms of $(+,-,*,/,\sqrt{})$ over Q, the field of rationals, [vdW]. The impossibility of straight-edge and compass constructions for the problems of trisecting an angle, duplicating the cube, and construction of a regular heptagon, imply the non-solvability of these problems by quadrature. Here we discuss two applied computational problems and sketch simple Galois methods by which we show solvability and non-solvability by quadrature.

Consider the following fundamental geometric problem. It has a long and interesting history and has come to be known as the Weber problem [B1]. Simply stated one wishes to obtain the optimum location of a single *source* point in the plane, so that the sum of the Euclidean distances to n fixed *destination* points is a minimum.

Given n fixed destination points in the plane with integer coordinates (a_i, b_i), determine the optimum location (x, y) of a single source point, that is

$$minimize_{x,y} \quad f(x,y) = \sum_{i=1..n} \sqrt{(x-a_i)^2+(y-b_i)^2}$$

In the decision version of this problem we ask if there exists (x,y) such that for given integer L, $\sum_{i=1..n} \sqrt{(x-a_i)^2+(y-b_i)^2} \leq L$? This problem is not even known to be in NP. Since on guessing a solution one then attempts to verify *if* $\sum_{i=1..n} \sqrt{c_i} \leq L$ *?*, in time polynomial in the number of bits needed to express the rational numbers $c_1, \cdots c_n$ and L. However no such polynomial time algorithm is known [Gr],[O]. Such a decision problem is fundamental in that it also occurs in numerous other geometric optimization problems such as in finding the minimum length Euclidean Traveling Salesman Tour and the minimum length Euclidean Steiner Tree.

We obtain our results by first deriving for each of the above geometric problems their minimal polynomial, whose root over the field of rational numbers is the solution of the problem in Euclidean space. The function $f(x,y)$ of the Weber problem to be minimized can be shown to be strictly convex. Hence there exists a *unique* minimum solution for which the necessary and sufficient conditions are $df/dx = 0$ and $df/dy = 0$. The corresponding rational equations are

$$df/dx = \sum_{i=1..n} (x-a_i)/\sqrt{(x-a_i)^2+(y-b_i)^2} = 0$$

$$df/dy = \sum_{i=1..n} (y-b_i)/\sqrt{(x-a_i)^2+(y-b_i)^2} = 0$$

We make a *wlg*, (without loss of generality), assumption that the solution does not coincide with any of the destination points and obtain the corresponding polynomial equations $f_1(x,y) = 0$ and $f_2(x,y) = 0$ from the above two rational equations, respectively. This is done by rationalizing and by the elimination of square-roots by a process of repeated squaring. Note that by this step we do not change the root of our original problem since repeated squaring preserves the root of the polynomial. The system of two polynomial equations $f_1(x,y) = 0$ and $f_2(x,y) = 0$ can be solved by elimination techniques (using resultants), [vdW], leading to a single polynomial equation $p(y)=0$ in a single variable.

For this problem consider a case of 5 points in the plane. On applying the above technique we obtain the single variate polynomial $p(y)$ for the problem. This polynomial $p(y)$ is the same for each of the three possible configurations of five points in the plane, namely having three, four or five points on the convex hull. All the process steps of rationalizing and eliminating square roots were done using MACSYMA giving us the final polynomial equation below. For details see [B1].

$$Q : p(y) = 15y^8 - 180y^7 + 1030y^6 - 4128y^5 + 11907y^4$$

$$- 15876y^3 - 17928y^2 + 75816y - 54756$$

We show that $p(y)$ is the minimal polynomial of our problem by noting that $p(y)$ is irreducible mod 31, (where the prime 31 is not a divisor of 15 the leading coefficient of the polynomial), and hence irreducible over Q. On factoring this polynomial modulo 37, (where the prime 37 does not divide the discriminant of the polynomial), we obtain a factor of degree 7. From Galois theory we know that 7 must be a divisor of $o[Gal(p(y))]$, which clearly is not a power of 2 and hence the roots of the polynomial $p(y)$ are not constructible by straight-edge and compass.

Lemma 3.1 : For the Weber problem, in general for $n \geq 5$, there is no algorithm which would give a closed form solution over the Quadrature Computation Model.

To see an example of an applied problem expressible by Quadrature, (constructible by straight-edge and compass) consider the following shortest path problem.

Given a sequence $L=(l_1,l_2,\cdots,l_n)$ of lines in 3-dimensional space , find the shortest path from a source point X to a destination point Y constrained to pass through interior points of each of the lines $l_1,l_2,\cdots,l_n$ in this order.

The problem of finding the shortest path between two points in Euclidean 3-space, bounded by a finite collection of polyhedral obstacles is a special case of the more general problem of planning optimal collision-free paths for a given robot system. The lines of the above problem arise from the edges of these polyhedral obstacles where the breakpoints of the shortest path ocurr. The necessary and sufficient conditions for the shortest path can be expressed algebraically by the set of n equations

$$\alpha_i = \beta_i \ , \quad i=1..n \qquad (1)$$

where α_i and β_i are the angles subtended at line l_i by the incoming and outgoing segments of the shortest path respectively. For the case of adjacent parallel lines, l_i is parallel to l_{i+1}, we furthermore have

$$\beta_i = \alpha_{i+1} \ , \quad i=1..n-1 \qquad (2)$$

Using the equations of (1) and (2) we obtain the equation $\alpha_1=\beta_n$ where α_1 is the angle subtended at line l_1 by the incoming shortest path segment from point X and β_i is the angle subtended at the line l_n by the outgoing shortest path segment to point Y. On simplifying the equation $\alpha_1=\beta_n$ or equivalently the equation $Cos\,\alpha_1 = Cos\,\beta_n$ we obtain,

$$x_n = b_1+(x_1-a_1)\sqrt{((y_n-b_2)^2+(z_n-b_3)^2)/((y_1-a_2)^2+(z_1-a_3)^2)}$$

The above equation has x_n expressed in terms of $(+,-,*,/,\sqrt{})$ over constant values of Q and x_1. Using sets of equations (1) and (2) it is straightforward to see that each of the unknowns x_i, $i=2..n$, can similarly be expressed in terms of $(+,-,*,/,\sqrt{})$ over constant values of Q and x_1. Next solving an equation of (1), say, $\alpha_n = \beta_n$ we obtain x_1 expressed in terms of $(+,-,*,/,\sqrt{})$ over constant values of Q. It follows that each of the x_i, $i=1..n$ is expressible in terms of $(+,-,*,/,\sqrt{})$ over constant values of Q and hence constructible. A similar result can be shown for the case when adjacent lines intersect. Hence we have the following lemma

Lemma 3.2 : When the adjacent lines are parallel or intersect, then the solution to the shortest path problem is always expressible in terms of $(+,-,*,/,\sqrt{})$ over Q.

4. $Q(+,-,*,/,k\sqrt{})$ Solvable Computation Models

Again consider the Weber problem of § 3. Since the minimal polynomial $p(y)$ of degree 8 of the problem considered there is irreducible we know that its Galois group is transitive. Further we shall now show that its Galois group is in fact the non-solvable symmetric group S_8. We find that for suitable primes q=19,31 and 37, the degrees of the irreducible factors of $p(y)$ mod q gives us a 2 + 5 permutation, an 8 cycle and a 7 cycle. The 2 + 5 permutation when raised to the 5^{th} power yields a transposition. This together with the 7 cycle and the 8 cycle and the transitivity of the group generates the entire symmetric group S_8. This principle generalizes to an irreducible polynomial with degree n. On factoring this polynomial modulo suitable primes, occurrence of an $n-1$ cycle, an n cycle and a permutation of the type 2 + factors with odd degree when n is even, (and factors with even degree when n is odd), is enough to establish its Galois group to be S_n. See [B1] for further details. Carrying out the same algebraic reduction technique for variants of the Weber problem, as for the Weber problem in § 3, we obtain for the Line-restricted version a minimal polynomial of degree 12. This for the case of 3 points in the plane and a line L not passing through these points and the solution restricted to L.

$$Q : p(y)=3y^{12}-72y^{11}+780y^{10}-4992y^{9}+20772y^{8}-58500y^{7}+113610y^{6}$$

$$-155448y^{5}+156912y^{4}-119040y^{3}+51876y^{2}+972y-729=0$$

The non-solvability follows by showing that its Galois group is the non-solvable S_{12} group. For the 3-Dimension Weber problem we examine the simplest case of 4 points in Euclidean 3-space, forming a tetrahedron, and obtain a minimal polynomial of degree 10.

$$Q : p(y)=8y^{10}-112y^{9}+507y^{8}+492y^{7}-14448y^{6}$$

$$+64932y^{5}-143326y^{4}+160772y^{3}-71112y^{2}-324y+243=0$$

Again we are able to show, using factorizations modulo primes, that its Galois group is the non-solvable S_{10} group.

Lemma 4.1 For the Weber problem, the Line-restricted version and the 3-Dimension Weber problem, there is in general no algorithm which would give a closed form solution over solvable computation models.

Also again consider the shortest path problem of § 3. This time consider the case where the adjacent lines are skew to each other. We show in [B2] that for the case of even two skew lines the solution is not expressible by radicals over Q. We again reduce the geometric problem to an algebraic one and with the use of MACYSMA simplify and obtain the minimal polynomial $p(y)$ over Q.

$$Q : p(y)=y^{12}-12y^{11}+87y^{10}-504y^{9}+2244y^{8}-8136y^{7}+24948y^{6}$$

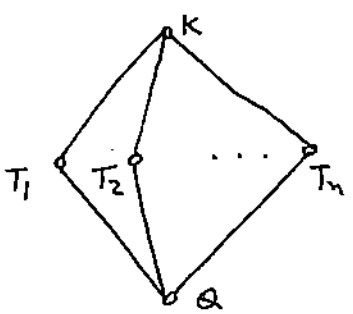
$$-62160y^{5}+128880y^{4}-224928y^{3}+297216y^{2}-311040y+233280$$

The polynomial is irreducible modulo 23, gives an 11 cycle modulo 31 and a $2+3+7$ cycle modulo 43. Again this enough to establish its transitive Galois group to be the non-solvable symmetric group S_{12}.

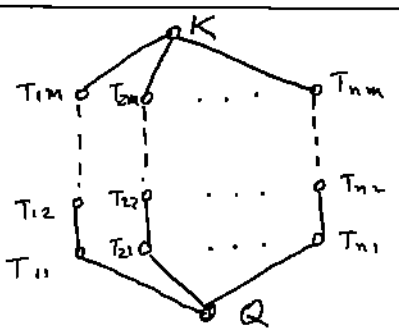
Lemma 4.2 For the shortest path problem with skew adjacent lines there is in general no algorithm which would give a closed form solution over solvable computation models.

5. $Q(+, -, *, /, k\sqrt{}, q(x))$ Algebraic Computation Models

Now consider solving the minimal non-solvable polynomials of § 4, on the more powerful algebraic computation models $Q(+, -, *, /, k\sqrt{}, q(x))$ where $q(x)$ are irreducible polynomials with rational coefficients having non-solvable Galois groups. For example $q(x)$ could be 'general' polynomial equations of degree n, $n \geq 5$, over Q. Then multiple use of the roots of the polynomial $q(x) \varepsilon Q$ to obtain the solution can be depicted by the following field diagram (a). Here K corresponds to the splitting field of the minimal polynomial $p(y)$ and T_i corresponds to the splitting field of the polynomial $q(x)$ over Q. The field diagram (b) corresponds to also the use of polynomials $q(x)$ with coefficients over arbitrary fields, not just rationals.



(a)



(b)

For what follows we need a part of the fundamental theorem of Galois theory [vdW], which simply stated is,

> *Galois' Theorem :* Let $f(x)$ be a polynomial in $F[x]$, K its splitting field over F and $G(K,F)$ its Galois Group. For any subfield T of K which contains F let $G(K,T) = \{\sigma \in G(K,F) \mid \sigma(t)=t, \forall t \in T\}$. Then T is a normal extension of F iff $G(K,T)$ is a normal subgroup of $G(K,F)$ and when T is a normal extension of F, then $G(T,F)$ is isomorphic to $G(K,F) / G(K,T)$

Let us again return to the Weber problem of § 3. Let $p(y)$ be the minimal polynomial of the Weber problem, K its splitting field over Q and $G(K,Q)$ its Galois Group. Let the non-solvable roots of the general fifth degree polynomial equation lie in their splitting field T, a normal extension of Q. The Galois group $G(T,Q)$ is, the symmetric group S_5, whose order is 5 !. From Galois' Theorem we obtain that $G(K,T)$ is a normal subgroup and $G(T,Q)$ is isomorphic to $G(K,Q) / G(K,T)$. However from § 4, we know $G(K,Q)$ for the polynomial is S_8, of order 8 !. Further the only normal subgroups of S_8 are the singleton set containing the identity, the Alternating group of order 8 !/2, and the symmetric group S_8, itself. Thus, $G(T,Q)$ cannot be isomorphic to $G(K,Q) / G(K,T)$, which goes to say that the normal extension T cannot exist. Hence the Weber problem is not solvable over this algebraic computation model which allows use of the non-solvable roots of the general fifth degree polynomial equation. Similar algorithmic limitations apply for other general polynomial equations $q(x)$, $n>5$. For the line-restricted Weber problem and the shortest path problem both with Galois groups S_{12}, algorithmic limitations apply for algebraic models with non-solvable roots of general polynomial equations of degree n upto 12. We thus have

> *Lemma 5.1* For the Weber problem with its variants and the shortest path problem, there is in general no algorithm which would give a closed form solution over a variety of algebraic computation models.

The above method of proving algorithmic limitations generalizes to various other non-solvable Galois groups other than the symmetric group. Additional possible non-solvable Galois groups are the alternating groups A_n and other non-abelian finite simple groups. From the classification of finite simple groups we know that non-abelian finite simple groups are either the alternating groups, groups of Lie type or the finitely many sporadic groups [C]. For irreducible minimal polynomials possible non-abelian simple Galois groups are furthermore transitive. The question of whether for any finite group G there exists a polynomial equation over Q whose Galois group

is isomorphic to G, has for long been an extremely difficult problem [J]. The question of whether for any non-solvable finite group G there exists a polynomial equation over Q whose Galois group is isomorphic to G, is equally difficult. The earliest general results on this problem are that the answer is affirmative if G is S_n or A_n for any n. Safarewic, using deep arithmetic results, had earlier proved that the answer is affirmative for every solvable finite group G.

When the Galois group of the minimum polynomial of our problems is the Symmetric group we have already seen above some of the consequences of limitations to algorithm solvability. If the Galois group is a finite simple group then directly the weakest algebraic computation model which permits a solvable algorithm is one where $q(x)$ is the minimal polynomial of the problem, since the splitting field of the polynomial has no normal sub-fields. Hence all 'exact' algorithms for this problem would finally need to approximate the roots of this minimal polynomial by numerical or symbolic procedures [BCL]. Complexity lower bounds of $\Omega(nlogd)$ of the *ACT* model for evaluating the polynomial can be used directly.

6. Discussion and Extensions

One of the main shortcomings of the analysis of algorithmic limitations as discussed in the above sections, is the efficent computation of Galois groups of the problems. Though various ways of computing Galois groups of polynomials are known such as straightforward resolvent techniques, the numerical techniques of Artin [St], and the van der Waerden Sampling methods [vdw], the drawback is that the computations are worst case exponential time. Extremely large space requirements is also a bottleneck. These become insurmountable for larger sized problems.

Nevertheless there are some very heartening features. Some polynomial time algorithms exist for computing Galois groups of polynomials when the group is either S_n or A_n [L]. The method of sampling of § 4 also proves quite effective for establishing the Symmetric Galois group [Z]. Further, the Galois group of a polynomial $p(y)$ is the Alternating group if and only if the discriminant of $p(y)$ is a perfect square of an element of Q. Also quite often we need only obtain the order of the Galois group to answer questions about algorithmic limitations over certain models. For example the order of the Galois group not being a power of 2 implies impossibility over the *Quadrature* models of § 3 and being n ! for polynomials of degree n implies impossibility over Solvable models of § 4. The order of the Galois group not being n ! implies the simplicity of the non-solvable Galois group and thus impossiblity of exact algorithms over various algebraic models of § 5.

An important extension to our above analysis is the exploration of algorithmic power and limitations of Transcendental extensions. The problem of squaring the circle, like the duplication of the cube and the trisection of an angle, is impossible over Quadrature models. However the impossibility of squaring the circle as opposed to other problems, follows from the fact first established by Lindemann in 1882, that Π is a transcendental number that is not algebraic over Q. Hence exact algorithms for squaring the circle are impossible over all algebraic computation models. Transcendental extensions such as $Q(+,-,*,/, q(x), \Pi)$ suffice. From [BCL, p169] we learn that rational operations in a field extended by a transcendental element is equivalent to performing arithmetic in the field of rational functions over the field. However little else is known about its computational power or limitations. Meanwhile transcendental extension models of computation are being used in areas such as Computational Geometry where the model of computation is the real RAM extended with unit time computations of transcendental trignometric functions [Sh]. Exploring the limitations of models which permit the use of non-analytic functions such as the floor function, which cannot be computed by a constant number of arithmetics or comparisons [F], is yet in its early stages [S].

7. References

[AHU]Aho, A., Hopcroft, J., Ullman, J., *The Design and Analysis of Computer Algorithms*, Addison-Wesley, 1974.

[B1] Bajaj, C., *The Algebraic Degree of Geometric Optimization Problems*, Computer Science Technical Report, Purdue University, TR84-496, 1984.

[B2] Bajaj, C., *The Algebraic Complexity of Shortest Paths in Polyhedral Spaces*, Computer Science Technical Report, Purdue University, TR85-523, 1985.

[BCL]Buchberger, B., Collins, G., and Loos, R.,(editors) *Computer Algebra, Symbolic and Algebraic Computation*, Computing Supplementum 4, Springer Verlag, Wien New York, 1982. (edited by B. Buchberger, et. al.).

[BM] Borodin, A., Munro, I., *Computational Complexity of Algebraic and Numeric Problems*, American Elsevier Publishing Company, 1975.

[BO] Ben-Or, M. *Lower Bounds for Algebraic Computation Trees*, Proc. 15th Symposium on Theory of Computing, p80-86, 1983.

[C] Cameron, P.J., *Finite Permutation Groups and Finite Simple Groups*, Bulletin London Math. Society, vol. 13, p1-22, 1981.

[DL] Dobkin, D., Lipton, R., *On the Complexity of Computations under Varying Sets of Primitives*, J. of Computer and System Sciences, vol 18, p86-91, 1979.

[E] Engeler, E., *Generalized Galois Theory and its Application to Complexity*, Theoretical Computer Science, vol. 13, p271-293, 1981.

[F] Friedman, N., *Some Results on the Effect of Arithmetics on Comparison Problems*, Proc. 13th IEEE Symposium on Switching and Automata Theory, p139-143, 1972.

[G] Gati, G., *The Complexity of Solving Polynomial Equations by Quadrature* Journal of the ACM, vol. 30, no. 3, 1983.

[Gr] Graham, R.L., *Unsolved Problem P73*, Problems and Solutions, Bulletin of the EATCS, p205-206, 1984.

[J] Jacobson, N., *Basic Algebra I*, W.H. Freeman and Company, 1974.

[L] Landau, S., *Polynomial Time Algorithms for Galois Groups*, Lecture Notes in Computer Science, Springer Verlag 174, Proc. EUROSAM 84, p225-236, 1984.

[Mc] McKay, J., *Some Remarks on Computing Galois Groups*, Siam J. of Computing, vol 8, no 3, p344-347, 1979.

[O] Odlyzko, A.M., *Personal Communication, May 1985.*

[R] Rabin, M., *Proving Simultaneous Positivity of Linear Forms*, J. of Computer and System Sciences, vol 6, p639-650, 1972.

[S] Schmitt, A., *On the Computational Power of the Floor Function*, Information Processing Letters, vol 14, no. 1, p1-3, 1982.

[Sh] Shamos, M., *Computational Geometry*, Ph.D. Thesis, University Microfilms International, 1978.

[St] Stauduhar, R.P., *The Determination of Galois Groups*, Mathematics of Computation, vol 27, no 124, p981-996, 1973.

[SY] Steele, J., and Yao, A., *Lower Bounds for Algebraic Decision Trees*, Journal of Algorithms, vol 3, p1-8, 1982.

[vdW]van der Waerden, B.L., *Modern Algebra*, vol 1, Ungar, New York 1953.

[Z] Zassenhaus, H., *On the Group of an Equation* Computers in Algebra and Number Theory, SIAM and AMS proceedings, p69-88, 1971.