1984

The Algebraic Degree of Geometric Optimization Problems

Chanderjit Bajaj

Report Number:
84-496

THE ALGEBRAIC DEGREE OF GEOMETRIC OPTIMIZATION PROBLEMS

Chanderjit Bajaj

CSD-TR-496
October 1984

The Algebraic Degree of Geometric Optimization Problems

Chanderjit Bajaj

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

ABSTRACT

In this paper we apply Galois theoretic algebraic methods to certain fundamental *geometric optimization* problems whose recognition versions are not even known to be in the class NP. In particular we show that the classic Weber problem, the *Line−restricted* Weber problem and the 3−*Dimension* version of this problem are in general not solvable by radicals over the field of rationals. One direct consequence of these results is that for these geometric optimization problems there exists *no exact* algorithm under models of computation where the root of an algebraic equation is obtained using arithmetic operations and the extraction of k^{th} roots. This leaves only numeric or symbolic approximations to the solutions, where the complexity of the approximations is shown to be primarily a function of the algebraic degree of the optimum solution point.

The Algebraic Degree of Geometric Optimization Problems

Chanderjit Bajaj

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

1. Introduction

Geometric optimization problems are inherently not pure combinatorial problems since the optimal solution often belongs to an infinite feasible set, the entire real (Euclidean) plane. Such problems frequently arise in computer application areas such as robotics and cad/cam. It has thus become increasingly important to devise appropriate methods to analyze the complexity of problems where combinatorial analysis methods seem to fail. Here we take a step in this direction by applying Galois theoretic algebraic methods to certain fundamental *geometric optimization* problems. These problems are non-combinatorial and have no known polynomial time solutions. Neither have these problems shown to be intractable (*NP*-hard, etc.,). In fact the recognition versions of these optimization problems are not even known to be in the class *NP* [Gr84].

The use of algebraic methods for analyzing the complexity of geometric problems has been popular since the time of Descartes, Gauss, Abel and Galois. The complexity of straight-edge and compass constructions has been shown to be equivalent to the geometric solution being expressible in terms of $(+,-,*,/,\sqrt{})$ over Q, the field of rationals [CR41],[vdW53]. In this paper we show how necessary and sufficient conditions for the existence of minima in certain geometric optimization problems are tied to the question of solvability of an algebraic equation over Q. We illustrate a method of generating the minimal polynomial, whose root over the field of rational numbers is the solution of the geometric optimization problem on the real (Euclidean) plane. Having shown the derived polynomial to be minimal by proving it irreducible over Q we use Galois theory to answer questions about the impossibility of straight-edge and compass constructions and furthermore the non-solvability (or non-expressibility) of the optimizing solution by *radicals*†.

† A real number α is expressible in terms of *radicals* if there is a sequence of expressions $\beta_1, \ldots, \beta_n$, where $\beta_1 \in Q$, and each β_i is either a rational or the sum, difference, product,

For the geometric optimization problems whose minimal algebraic polynomials we show to be *not* solvable by radicals, there are a number of immediate consequences. First, for these problems there exists *no exact* algorithm under models of computation where the root of an algebraic equation is obtained using arithmetic operations and the extraction of k^{th} roots. Second, this leaves only numeric or symbolic approximations to the optimum solution. In order to use numeric or symbolic approximation techniques one first needs to compute a sequence of disjoint intervals with rational endpoints, each containing exactly one real root of the minimal polynomial and together containing all the real roots, (root isolation). Given an isolating interval with rational endpoints one can use symbolic bisection and sign calculation methods [CL82] or Newton's iterations [Li76] to rapidly approximate the solution to any desired degree of accuracy. The complexity of the algorithms which isolate the roots of a polynomial P of degree d with integer coefficients is bounded below by a power of $log\,(1/sep\,(P))$ where $sep\,(P)$ is the minimum distance between distinct real roots of P. A lower bound for $sep\,(P)$ given by [Ru79] satisfies $sep\,(P) > 1/(2d^{d/2}(|P|+1)^d)$. Hence from the minimal polynomial of the non-solvable geometric optimization problem we in effect derive a complexity bound for approximations which primarily depends on the algebraic degree of the optimum solution point, (the degree of the minimal polynomial).

A similar complexity bound may also be derived for the order of convergence of a sequence of numerical approximations of the optimum solution point. [Ku75] relates the order of convergence of approximations of an algebraic number with the algebraic degree of the number, provided the approximation sequence is of bounded order of convergence.

The main geometric optimization problem we consider is one of fundamental importance and has an equally long and interesting history in mathematical literature [Ku67]. Simply stated one wishes to obtain the optimum solution 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

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

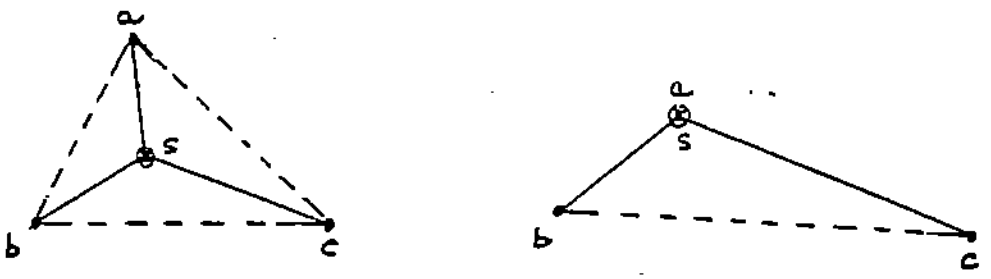
quotient or the k^{th} *root* of preceding β's and the last β_n is α.

Weber [We37], was probably the first who formulated this problem in light of the location of a plant, with the objective of minimizing the sum of transportation costs from the plant to sources of raw materials and to market centers. Hence this problem for n points has also come to be known as the *Generalized Weber* problem. In the recognition version of this problem we ask if there exists (x,y) such that for given integer L, if $\sum_{i=1..n}\sqrt{(x-a_i)^2+(y-b_i)^2} \leq L$? 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 certain rational numbers $c_1, \cdots c_n$ and L. However no such polynomial time algorithm is known [GGJ76],[Gr84]. [Ba75] also explains some of the difficulty involved with the approximations to sums of square roots.

The solution to the Generalized Weber problem is simple to obtain for the special cases when the n points lie on a straight line or form a regular n-gon. However in general, straight edge and compass constructions are only known for the cases of $n=3$ and $n=4$. We show that for the case of $n=5$ points the solution is the root of an irreducible polynomial of high degree. Further we prove that the *Galois* group associated with the irreducible polynomial is the symmetric permutation group. Hence we are able to show that the Generalized Weber problem, is not solvable by radicals over Q for $n \geq 5$. For the *Line−restricted* Weber problem, where the optimum solution is constrained to lie on a certain given *line*, a much stronger result holds. We show that the Line-restricted Weber problem, in general, is not solvable by radicals over Q for $n \geq 3$. A similar result is also shown to apply to the *3−Dimension* version of this problem, for $n \geq 4$. A proof of the impossibility of straight-edge and compass constructions for the Generalized Weber problem (but not the Line-restricted case) appears in [Me73], however nothing was known about the non-expressibility of the solution by radicals.

2. The Weber Problem

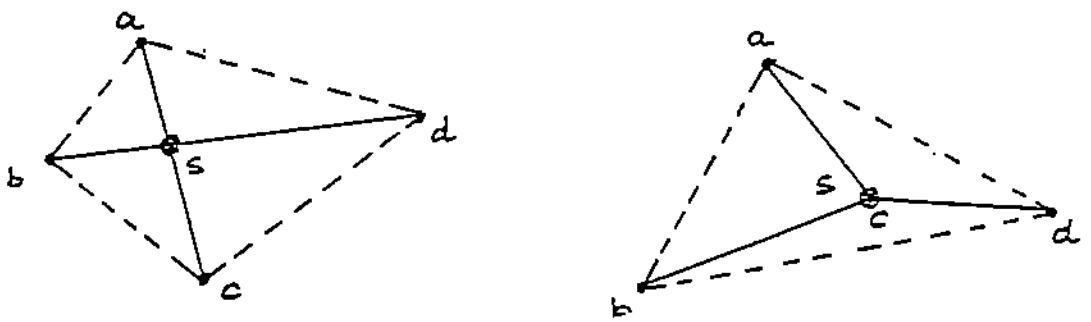
The Weber problem has a long and interesting history. The problem for the case of $n=3$ was first formulated and thrown out as a challenge by Fermat as early as in the 1600's [Ku67]. Cavalieri in 1647 considered the problem for this case, in particular, when the three points form the vertices of a triangle and showed that each side of the triangle must make an angle of 120° with the given minimum point. Heinen in 1834 noted that in a triangle which has an angle of $\geq 120^\circ$, the vertex of this angle itself is the minimum point (Fig. 1).



(a) Triangle with angles $< 120°$ (b) Triangle with an angle $\geq 120°$

Fig. 1

Fagnano in 1775 showed that for the case $n=4$ when the four client points form a convex quadrilateral the minimum solution point is the intersection of the diagonals of the quadrilateral. For a non-convex quadrilateral the fourth point which is inside the triangle formed by the three other points, is itself the minimum point (Fig. 2).



(c) Convex quadrilateral (d) Non-convex quadrilateral

Fig. 2

Tedenat in 1810 found that for the case of n points the necessary condition for the minimum solution point is that the sum of cosines of the angles between any arbitrary line in the plane and the set of lines connecting the n given points with the minimum point must be zero. Later, Steiner in 1837 proved that the necessary and sufficient conditions for the minimum solution are that the sum of the cosines and

sines of the above mentioned angles must be zero.

The constructions for the solution points for the case of 3 points is also worthy of note. The solution is variously obtained by the Steiner construction or the Simpson construction (Fig. 3).

(i) Steiner point (ii) Simpson point

Fig. 3

3. Algebraic Reduction

The function $f(x,y)$ specified in (1) of Section 1, can be shown to be strictly convex. A sufficient set of conditions for the function $f(x,y)$ to be convex is

$$(i)\ p=(d^2f/dx^2)_{x=x_0}>0 \qquad (ii)\ q=(d^2f/dy^2)_{y=y_0}>0$$

$$(iii)\ pq-r^2>0 \qquad \textit{where} \quad r=(d^2f/dxdy)_{x=x_0,y=y_0}$$

and (x_0,y_0) is the solution of the equations $df/dx=0$ and $df/dy=0$. The above conditions are quite easily met for the function $f(x,y)$ of (1). 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

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

$$df/dy=\sum_{i=1..n}(y-b_i)/\sqrt{(x-a_i)^2+(y-b_i)^2}=0 \quad (3)$$

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 (2) and (3) respectively. This is done by rationalizing and by the elimination of square-roots. By a process of

repeated squaring one can eliminate all the square-roots from the expressions (2) and (3) above. Starting with say a sum of n different square-roots, sqrt(i), i=1..n, equated to a constant, the technique is to take all terms of sqrt(i), for a certain i, to one side of the equation and the remaining terms on the other side, squaring both sides and thereby eliminating sqrt(i). Repeating this process by again isolating one of the remaining square-roots and squaring, one is able to eliminate all square-roots from the original equation in a maximum of n steps. Note that by this step we do not change the root of our original problem since repeated squaring preserves the root of the polynomial.

At this point we have a choice of two ways to proceed. 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), [vdW53], leading to a single polynomial equation $p(y)=0$ in a single variable. Alternatively the resulting polynomial equation for the optimization problem can be taken to be $p(x,y) = f_1(x,y)^2 + f_2(x,y)^2 = 0$, since it simultaneously satisfies both of the above equations $f_1(x,y) = 0$ and $f_2(x,y) = 0$.

Having obtained, say, the polynomial $p(x,y)$ for the problem the first step is to prove it irreducible, over Q. We show this by substituting constants for x, $x=a$ and showing that $p(a,y)$ is *irreducible*. If $p(x,y)$ is reducible then the corresponding $p(a,y)$ is also reducible. Hence if $p(a,y)$ is irreducible for some constant $x=a$ it implies that $p(x,y)$ is irreducible. However the fact that that the minimal polynomial $p(a,y)$ is irreducible is important to us only if the line determined by $x=a$ passes through the solution point of our optimization problem. Using a clever trick, we choose symmetric configurations of the points, symmetric about a line $x=a$, for then we know that the solution lies somewhere on $x=a$. Then for a set of n points distributed equally and symmetrically about the chosen axis $x=a$, (when n is odd, 1 point lies on this axis), we obtain the polynomial $p(y)$ of a single variable, for the problem. Proving it to be irreducible over Q gives us the minimal polynomial for the optimization problem.

For the problem in hand we now restrict ourselves to the case of n=5 points. Let (a_i,b_i), i = 1..5 be the given points with integer coordinates. We choose the configuration of 5 points to be symmetric about the line x=0. One of the points p lies on the line and has coordinates (0,c) on the x=0 axis. The value of c changes the configuration of points in that for c=5,1 and 4. This gives the three possible symmetric configurations of 5 points, (Fig. 4).

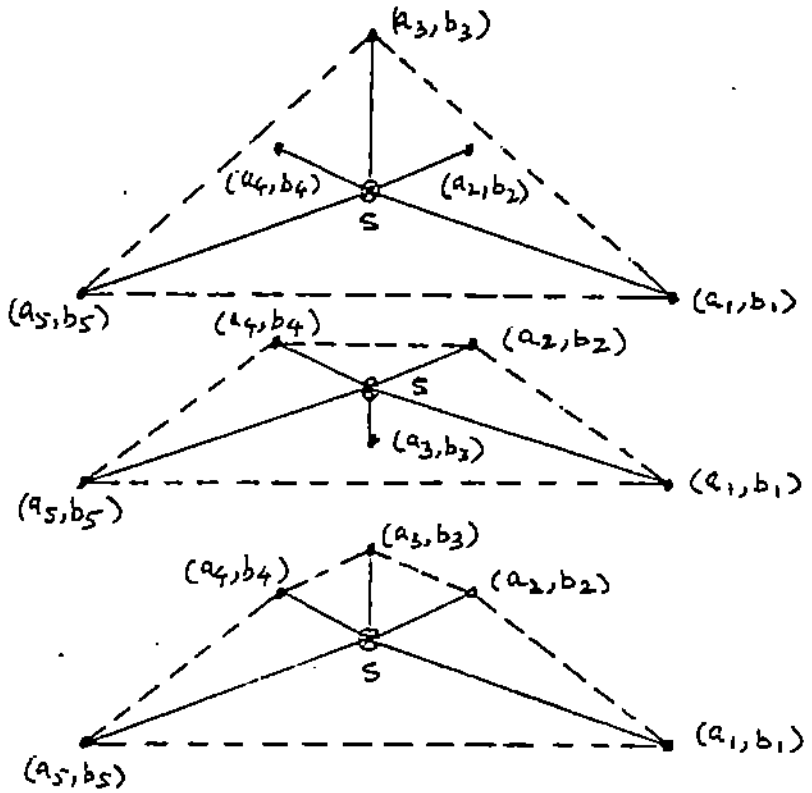


Fig. 4 Symmetric configurations of 5 points

Let $(a_1,b_1)=(3,0)$, $(a_2,b_2)=(1,3)$, $(a_3,b_3)=(0,c)$, $(a_4,b_4)=(-1,3)$ and $(a_5,b_5)=(-3,0)$. We need to find the solution $(0,y)$ satisfying the condition for minimality, $df/dy=0$, giving us the following,

$$\textit{minimize}_y \quad f(y)=|y-c| + 2\sqrt{(y-3)^2+1} + 2\sqrt{y^2+9}$$

$$df/dy = 1 + 2(y-3)/\sqrt{(y-3)^2+1} + 2y/\sqrt{y^2+9} = 0 \quad (y \neq c)$$

Eliminating square-roots we obtain the polynomial, $p(y)$, (*Table* 1). We note that this polynomial $p(y)$ is the polynomial for each of the 3 configurations above, since as long as $y \neq c$†, the equation $df/dy=0$ is the same regardless of $c=5,1$ or 4.

† The case $y=c$ occurs when the point $p=(0,c)$, coincides with the intersection of the lines between (a_1,b_1),(a_4,b_4) and (a_2,b_2),(a_5,b_5), which is also the solution for the case of those four points, (a_i,b_i), $i=1,2,4$ and 5.

Table 1

$$Q : p(y)=15y^8-180y^7+1030y^6-4128y^5+11907y^4$$
$$-15876y^3-17928y^2+75816y-54756$$
$$Disc(p(y)): \quad 2^{52}3^{25}5^8 13^5 17^2 13063$$
$$Mod\ 19 : p(y)=(y+7)(y^2-9y-4)(y^5+9y^4+8y^3+7y^2-4y-1)$$
$$Mod\ 31 : p(y)=(y^8-12y^7-14y^6+10y^5-6y^4+8y^3-11y^2-11y-11)$$
$$Mod\ 37 : p(y)=(y+5)(y^7-17y^6+18y^5-10y^4+15y^3-16y^2+17y+4)$$

Factorizations obtained with use of
MACSYMA, (actually Vaxima on Unix).

We now use Galois theoretic methods to prove the properties of interest. For a definition of the terms used here see [He75],[Ga71].

Lemma 1: The polynomial $p(y)$, [*Table* 1], is irreducible over Q.

Proof : Since $p(y)$ is irreducible mod 31 and the prime 31 is not a divisor of 15 the leading coefficient of the polynomial, it follows that $p(y)$ is irreducible over Q and is our minimal polynomial. □

The degree testing algorithm, see [Kn81], is a much more efficient means of proving irreducibility than merely searching for a prime p for which $p(y)$ is irreducible mod p. By performing the factorization of the polynomial $p(y)$ modulo several primes, and considering the possible degrees of the factors, one can obtain important information about the degree of the true factors. For good primes p relative to $p(y)$, {primes p that are not divisors of disc($p(y)$)}, one computes the degree set d_p=set of degrees of all factors of $p(y)$ mod p. The degree set of $p(y)$ must be contained in $d_{p_1} \cap \cdots \cap d_{p_m}$, where $p_1,\ldots,p_m$ are the primes tried. If $p(y)$ is irreducible over Q, often $d_{p_1} \cap d_{p_2} \cap \cdots = (0,n)$ after only a few primes have been tried.

As our next step we show the impossibility of constructions with straight-edge and compass, but before that we need a few definitions. (Henceforth when we refer

to constructions we mean constructions with straight-edge and compass.) A field F is said to be an *extension* of Q if F contains Q and a *simple extension* if $F=Q(\alpha)$ for some $\alpha \epsilon F$. Every finite extension of Q is a simple extension. Using the notation of [He75], we denote $[F:Q]$=degree of F over Q, (the dimension of F as a vector space over Q).

Consider all the points (x,y) in the real Euclidean plane, both of whose coordinates x, y are in Q. This set of points is called the plane of Q. A point is *constructible* from Q *iff* we can find a finite number of real numbers $\alpha_1, \ldots, \alpha_n$ such that (i) $[Q(\alpha_1):Q]=1$ or 2 and (ii) $[Q(\alpha_1, \ldots, \alpha_i):Q(\alpha_1, \ldots, \alpha_{i-1})]= 1$ or 2, and such that our point lies in the plane of $Q(\alpha_1, \ldots, \alpha_n)$. It follows that if α is *constructible* then α lies in some extension of Q, of degree a power of 2. We know that a real number α is algebraic over Q *iff* $Q(\alpha)$ is a finite extension of Q. Further α is said to be *algebraic* of *degree* n over Q if it satisfies a non-zero polynomial of degree n but no non-zero polynomial of lower degree. Also if α is algebraic of degree n over Q, then $[Q(\alpha):Q] =n$. This together with our discussion of constructibility above gives the following important criterion for non-constructibility.

Lemma 2 : [*He75*] If the real number α satisfies an irreducible polynomial over Q of degree n and if n is not a power of 2, then α is not constructible.

If $p(y) \epsilon Q[y]$, a finite extension E of Q is said to be a *splitting field* over Q for $p(y)$ if over E but not over any proper subfield of E, $p(y)$ can be factored as a product of linear factors. Alternatively, E is a *splitting field* of $p(y)$ over Q if E is a *minimal* extension of Q in which $p(y)$ has n roots, where n=degree of $p(y)$. Given a polynomial $p(y)$ in $Q[y]$, the polynomial ring in y over Q, we shall associate with $p(y)$ a group, $Gal(p(y))$, the Galois group of $p(y)$. The Galois group turns out to be a certain permutation group of the roots of the polynomial. It is actually defined as a certain group of automorphisms of the *splitting field* of $p(y)$ over Q. From the duality, expressed in the fundamental theorem of Galois Theory, between the subgroups of the Galois group and the subfields of the splitting field one can derive a condition for the solvability by means of radicals of the roots of a polynomial in terms of the algebraic structure of its Galois group. As a special case one can give a criterion for non-constructibility by straight-edge and compass constructions similar to the above *Lemma* 2.

Lemma 3: If E is the splitting field over Q of an irreducible polynomial $p(y)$, and if the order of its Galois group, $o[Gal(p(y))] = [E:Q]$, is not a power of 2, then the roots of $p(y)$ are not *constructible*.

We now state a few additional theorems from Galois theory of use to us here. The following are well known and proofs may be found in [He75],[Ga71].

Lemma 4: [*Ga71*] For a finite field F, $|F|=p^n$ and $p(y)\epsilon F[y]$ factors over F into k different irreducible factors, $p(y)=q_1(y)...q_k(y)$, where degree $q_i(y)=n_i$, then $Gal(p(y))$ is *cyclic* and is *generated* by a permutation containing k cycles with orders $n_1, \ldots, n_k$.

The *shape* of a permutation of degree n is the partition of n induced by the lengths of the disjoint cycles of the permutation. The factorization of a polynomial modulo any prime p also induces a partition, namely the partition of the degree of $p(y)$ formed by the degree of the factors. The above *Lemma* 4 states that the degree partition of the factors of $p(y)$ modulo p is the shape of the generating permutation of the group, $Gal(p(y))$, which is furthermore cyclic.

Lemma 5: [*Ga71*] Let $p(y)\epsilon Z[y]$ have roots $\alpha_1, \ldots, \alpha_n$ and let $p^*(y)\epsilon Z_p[y]$, be the polynomial $p(y)$ mod p. If the roots of $p^*(y)$ are $\alpha_1^*, \ldots, \alpha_n^*$, then the $Gal(p^*(y))$, {as a permutation group of its roots} is isomorphic to a subgroup of $Gal(p(y))$.

Theorem 6 : The solution of the *Generalized−Weber* problem, in general, is not *constructible* by straight-edge and compass for $n \geq 5$.

Proof : Restating the assertion, we have to show that the roots of the polynomial $p(y)$ of *Table* 1 are not constructible by straight-edge and compass. We know that $p(y)$ is irreducible over Q from *Lemma* 1. Consider $p^*(y)$ as the polynomial $p(y)$ mod p for a *good*† prime $p=37$ relative to $p(y)$. From *Table* 1 the irreducible factors of $p^*(y)$ have degrees 1 and 7. On application of *Lemma* 4 we know that for the finite field Z_{37}, the $o[Gal(p(y))] = 7$ and from *Lemma* 5, it is a divisor of $o[Gal(p(y))]$, which clearly is not a power of 2 and hence *Lemma* 3 proves our assertion. □

To prove the *non−expressibility* of the roots of $p(y)$ over Q by radicals we use the *Ceboratev−Van der Waerden* sampling method to determine the Galois group of $p(y)$, [Mc79],[Za71]. From the density theorem of Ceboratev one obtains,

Lemma 7: As $s \to \infty$, the proportion of occurrences of a partition π as the degree partition of the factorization of $p(y) mod\ p_i$, $(i=1..s)$, tends to the proportion of

† A good prime for a polynomial $p(y)$ is one which does not divide the discriminant of the polynomial $disc(p(y))$.

permutations in $Gal(p(y))$ whose shape is π. (The *shape* of a permutation of degree n is the partition of n induced by the lengths of the disjoint cycles of the permutation).

In order to then apply this method of obtaining the group of the polynomial over Q one needs a table of permutation groups of the desired degree, along with a distribution of its permutations, [St73]. The degree of concern for the polynomial $p(y)$ of *Table* 1 is 8. From [Mi99] we know that there are exactly 200 permutation groups of degree 8. However all is not lost. We also know that polynomial $p(y) \epsilon Q$ is irreducible *iff* the Galois group, $Gal(p(y))$ is *transitive*‡, [vdW53], and there are only 50 transitive groups of degree 8.

If the Galois group of the polynomial is the symmetric group, S_n, (the group of all permutations of $[1..n]$), the Ceboratev-Van der Waerden method realizes the fact quickly. Indeed,

Lemma 8: [Za71] If $n \equiv 0(mod\ 2)$ and $n > 2$ then after sampling about $(n+1)$ good primes we run across an $(n-1)$-cycle and an n-cycle and a permutation of the type $2+(n-3)$ and that will be enough to establish that $Gal(p(y))$ over Q is the symmetric group S_n. If $n \equiv 1(mod\ 2)$ then one will run across an $(n-1)$ cycle and a permutation of the type $2+(n-2)$ in about the same time and that will be enough.

Proof : We prove why, if we run across cycle permutations of the above kind, it is enough for the Galois group to be the symmetric permutation group. Since for $n \equiv 0(mod\ 2)$, $n-3$ is odd, the permutation type $2+(n-3)$ when raised to a power (n-3) yields a 2-cycle. This together with the $n-1$ cycle and the n cycle generate the symmetric group S_n as follows. Let $(12...n-1)$ be the $n-1$ cycle. By virtue of transitivity, the 2-cycle (ij) can be transformed into (kn), where k is one of the digits between 1 and $(n-1)$. The transformation of (kn) by $(12...n-1)$ and its powers yield all cycles $(1n)(2n)...(n-1n)$ and these cycles together generate the symmetric group, S_n [vdW53].

For $n \equiv 1(mod\ 2)$, again as $n-2$ is odd, the permutation type $2+(n-2)$ when raised to a power $(n-2)$ yields a 2-cycle, which together with the $n-1$ cycle generates the symmetric group as above. □

‡ A permutation group on $1..n$ is called *transitive* if for any k, $1 \leq k \leq n$, it contains a permutation π which sends 1 to k.

Usually the decision that $Gal(p(y))=S_n$ is reached even after much less than $n+1$ trials as a consequence of the evolving pattern of permutations occurring in $Gal(p(y))$ and the application of known theorems of permutation groups.

We are now ready to prove our main theorem, but first let us indulge in some definitions. A polynomial $p(y)\epsilon Q[y]$ is called *solvable* over Q if there is a finite sequence of fields $Q=F_0<F_1<\cdots<F_k$, (where $F_{i-1}<F_i$ implies that F_{i-1} is a subfield of F_i) and a finite sequence of integers $n_0,\ldots,n_{k-1}$ such that $F_{i+1}=F_i(\alpha_i)$ with $\alpha_i^{n_i}\epsilon F_i$ and if all the roots of $p(y)$ lie in F_k, that is , $E\subseteq F_k$, where E is the splitting field of $p(y)$. F_k is called a *radical extension* of Q. Furthermore, we know from Galois theory that

Lemma 9 : [*He75*] $p(y)\epsilon Q[y]$ is solvable by radicals over Q *iff* the Galois group over Q of $p(y)$, $Gal(p(y))$ is a solvable group.

Lemma 10 : [*He75*] The symmetric group S_n is not solvable for $n\geq 5$.

Theorem 11: The *Generalized −Weber* problem, in general, is not solvable by radicals over Q for $n\geq 5$.

Proof : Restating the assertion, we need to show that the polynomial $p(y)$ of *Table* 1 is not solvable by radicals over Q. We note from *Table* 1 that for the 'good' primes $p=19,31$ and 37, the degrees of the irreducible factors of $p(y)$ mod p gives us a 2 + 5 permutation, an 8 cycle and a 7 cycle, which is enough to establish, from *Lemma* 8 for $n=8$, that $Gal(p(y))=S_8$, the symmetric group of degree 8. *Lemma* 10 tells us that this is not a solvable group and hence our assertion follows from *Lemma* 9. □

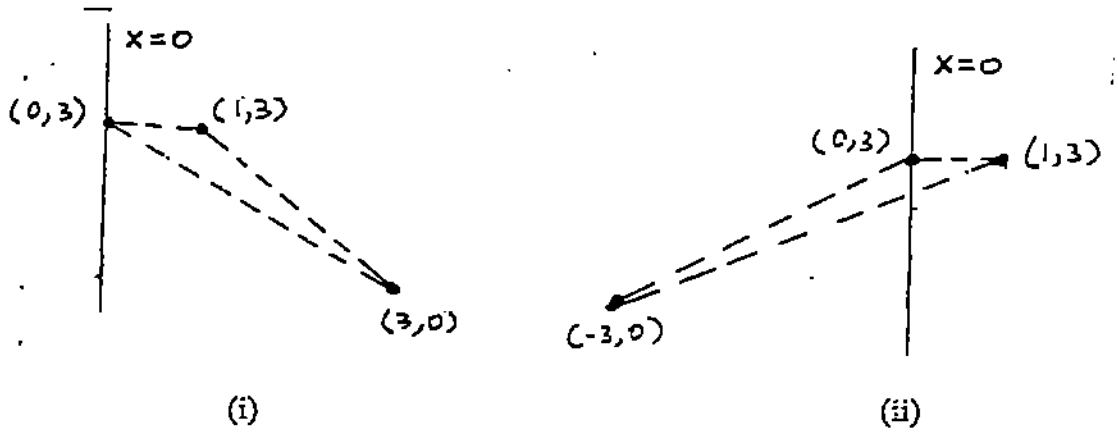
4. The Line-restricted Weber problem

Given n fixed *destination* points as before in the plane with coordinates (a_i,b_i), we need to determine the location (x,y) of a single *source* point, restricted to lie on certain given *line*, such that the sum of the Euclidean distances from this *source* to each of the *destinations* is minimized.

We consider two different positions (and orientations) of this line, since the algebraic degree of the solution point varies with the relative positions of the line and the fixed destination points.

For the non-trivial case of 3 destination points consider the solution restricted to a line passing through one of the points and *either* not intersecting the convex-hull

(of the destination points), Fig. 5 (i) *or* passing through the convex-hull, Fig.5 (ii).



(i) (ii)

Fig. 5

Table 2

$$minimize_y \quad f(y) = y - c + \sqrt{(y-3)^2+1} + \sqrt{y^2+9}$$

$$df/dy = 1 + (y-3)/\sqrt{(y-3)^2+1} + y/\sqrt{y^2+9} = 0$$

$$Q : p(y) = 3y^8 - 36y^7 + 202y^6 - 780y^5 + 2277y^4 - 4212y^3 + 3402y^2 - 81 = 0$$

$$disc(p(y)) : \quad 2^{28}3^{23}5^6 13^3 19687$$

$$Mod\ 7 : p(y) = (y^8 + 2y^7 + 2y^6 - y^5 + 3y^4 + 3y^3 + 1) = 0$$

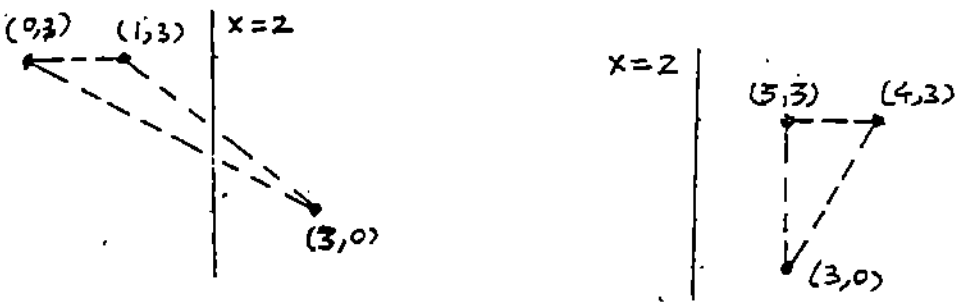
$$Mod\ 11 : p(y) = (y-5)(y^7 + 4y^6 + 3y^5 - 3y^4 - 4y^3 - 5y^2 - 2y + 1) = 0$$

$$Mod\ 29 : p(y) = (y+13)(y^2 + 5y - 11)(y^5 - y^4 + 12y^3 + 11y^2 + 2y + 1) = 0$$

Lemma 12: For the above cases of Fig.5 (i) and (ii), the minimal polynomial $p(y)$ (*Table* 2) of degree 8 is irreducible over Q. Furthermore, this polynomial is not solvable by radicals over Q.

Proof : Since $p(y)$ is irreducible mod 7, for a 'good' prime 7, it follows that $p(y)$ is irreducible over Q. To show non-solvability by radicals we apply *Lemma* 8 for $n=8$ and note from *Table* 2 that for the 'good' primes $p=7,11$ and 29 the degrees of the irreducible factors of $p(y)$ mod p gives us an 8 cycle, a 7 cycle and a 2 + 5 permutation which is enough to establish that $Gal(p(y))=S_8$. Again, *Lemma* 10 tells us that this is not a solvable group and hence our assertion follows from *Lemma* 9. □

As before, for the case of $n=3$ destination points consider the solution restricted to a line however, not passing through any of the 3 points and *either* not intersecting the convex-hull (of the destination points), Fig. 6 (iii), *or* passing through the convex-hull, Fig. 6 (iv).



(iii) (iv)

Fig. 6

Lemma 13: For the above cases of Fig. 6 (iii) and (iv), the minimal polynomial $p(y)$ (table 3) of degree 12 is irreducible over Q. Furthermore, this polynomial is not solvable by radicals over Q.

Proof : Since $p(y)$ is irreducible mod 7, for a 'good' prime 7, it follows that $p(y)$ is irreducible over Q. One notes that the impossibility of straight-edge and compass constructions follows immediately from *Lemma* 2, since the degree of $p(y)$ is 12 which is not a power of 2. To show the non-solvability by radicals, we again apply *Lemma* 8 for $n=8$ and note from table 2 that for the 'good' primes $p=7,19$ and 61 the degrees of the irreducible factors of $p(y)$ mod p gives us a 12 cycle, a 11 cycle and a 2 + 9 permutation which is enough to establish that $Gal(p(y))=S_{12}$, the symmetric group of degree 12. *Lemma* 10 tells us that this is not a solvable group and hence our assertion follows from *Lemma* 9. □

Table 3

$$minimize_y \quad f(y)=\sqrt{(y-3)^2+4}+\sqrt{(y-3)^2+1}+\sqrt{y^2+1}$$

$$df/dy=(y-3)/\sqrt{(y-3)^2+4}+(y-3)/\sqrt{(y-3)^2+1}+y/\sqrt{y^2+1}=0$$

$$Q: p(y)=3y^{12}-72y^{11}+780y^{10}-4992y^9+20772y^8-58500y^7+113610y^6$$
$$-155448y^5+156912y^4-119040y^3+51876y^2+972y-729=0$$

$$disc(p(y)): \qquad 2^a 3^b 5^c 13^d p$$

$$Mod\ 7: p(y)=(y^{12}-3y^{11}+y^{10}+2y^9+y^8+2y^7-2y^5+3y^3+2y^2+2y+2)=0$$

$$Mod\ 19: p(y)=(y-6)(y^{11}+y^{10}+8y^8-y^7+7y^6+7y^5+y^4+3y^3-9y^2+5y-7)=0$$

$$Mod\ 61: p(y)=(y+13)(y^2-3y+10)$$
$$(y^9+27y^8+19y^7+19y^6-7y^5+y^4-10y^3-25y^2-21y+23)=0$$

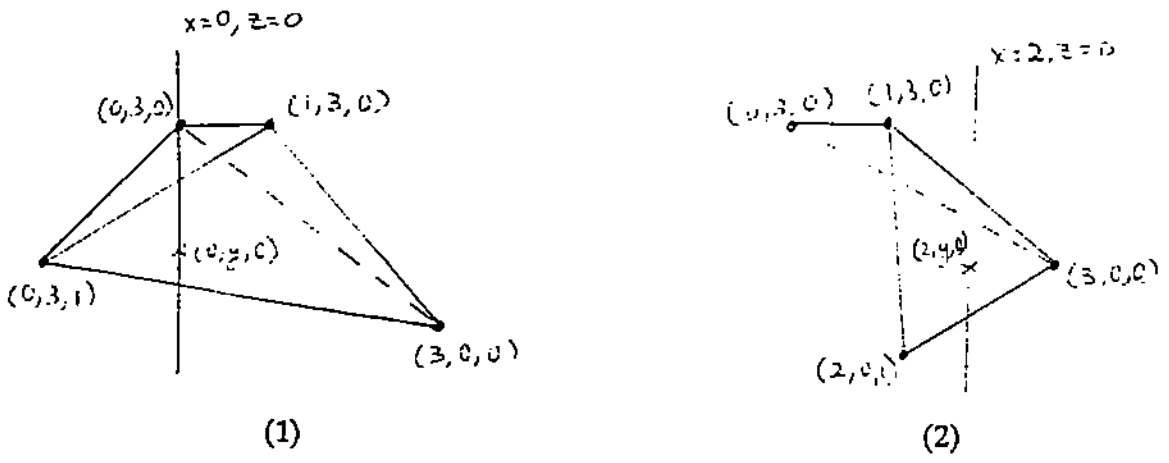
Theorem 14: The *Line−restricted Weber* problem, in general, is not solvable by radicals over Q for $n \geq 3$.

Proof : Follows from *Lemmas* 12 and 13. □

For the case of the line passing through 2 of the 3 given destination points, the soiution to the *Line−restricted Weber* problem coincides with projection of the 3rd point onto that line and so is *constructible*. Furthermore, the case of $n=5$ for the symmetric Generalized-Weber problem is equivalent to the (weighted) case, $n=3$, of the Line-restricted Weber problem, where the *line* is the axis of symmetry, which passes through one of the destination points. (and hence the algebraic degree of the solutions are the same). On the other hand the above case of $n=3$ of the Line-restricted Weber problem where the line does not pass through any of the destination points is equivalent to the case of $n=6$ for the symmetric Generalized-Weber problem, (the line becoming the axis of symmetry as before). The solutions of these cases are as expected, of higher algebraic degree.

5. Euclidean 3-Dimension Space

The Weber problems that we have considered can also be generalized to the case of noncoplanar points in Euclidean 3-Dimension space. The simplest case here corresponds to 4 noncoplanar points forming a tetrahedron. The solution point which minimizes the sum of the Euclidean distances from these 4 points clearly lies inside the tetrahedron, however for no point within the tetrahedron does there exist a *regular* configuration analogous to the corresponding planar Weber problem of Fig. 1, (viz., pairs of lines subtending equal angles at the solution point). The problem in 3-Dimensions thus appears more difficult and as we suspect, in general, not solvbale by radicals over Q. We show this to be true for the case of 4 noncoplanar points with the solution restricted to a line passing through one of the given points, as illustrated by *Fig* 7.



(1) (2)

Fig. 7

Theorem 15: The 3–*Dimension* version of the *Line–restricted Weber* problem, in general, is not solvable by radicals over Q for $n \geq 4$.

Proof : This case of 4 noncoplanar points corresponds to a case of 4 planar points of the planar Line-restricted Weber problem with two of the points being symmetrical about the given line. Our proof thus follows from *Theorem* 14. Alternatively, and more directly, we derive the corresponding polynomial via the algebraic reduction, and prove our result similar to the proof of *Theorem* 11. The polynomials $p_1(y)$ and $p_2(y)$ of *Table* 4 correspond respectively to the point configurations (1) and (2) of Fig. 7. For $p_1(y)$ of degree 6, we note from *Table* 4 that for the 'good' primes p =17,19 and 29, the degrees of the irreducible factors of $p_1(y)$ mod p gives us a 5

Table 4

$$Q : p_1(y)=56y^6-768y^5+4257y^4-15228y^3+42768y^2-75816y^7+54756=0$$

Mod 17 : *a* 5 *cycle*

Mod 19 : *a* 6 *cycle*

Mod 29 : *a* 2 + 3 *cycle*

$$Q : p_2(y)=8y^{10}-112y^9+507y^8+492y^7-14448y^6$$
$$+64932y^5-143326y^4+160772y^3-71112y^2-324y+243=0$$

Mod 19 : *a* 10 *cycle*

Mod 31 : *a* 9 *cycle*

Mod 37 : *a* 2 + 7 *cycle*

cycle, a 6 cycle and a 2 + 3 permutation, which is enough to establish our assertion, (from *Lemmas* 8 , 9 and 10). Similarly, for $p_2(y)$ of degree 10, we note from *Table* 4 that for the 'good' primes p =19,31 and 37, the degrees of the irreducible factors of $p_2(y)$ mod p gives us a 10 cycle, a 9 cycle and a 2 + 7 permutation, which is again enough to establish our assertion. □

6. Discussion & Further Research

We have outlined above a method of obtaining the minimal polynomial, whose root over the field of rational numbers is the solution of the geometric optimization problem on the real (Euclidean) plane. This may be applied to a number of other optimization problems as well. Other methods of computing minimal polynomials could also be used [PR85]. Having obtained the minimal polynomial one can apply Galois theoretic methods to check for solvability as sketched above. Alternatively one can use the computational procedure of [LM83]. From the minimal polynomial of the non-solvable optimization problems one can derive a complexity bound for approximations which primarily depends on the algebraic degree of the optimum

solution point, (the degree of the minimal polynomial). For the case when the polynomial is solvable computational lower bounds for obtaining the solution based on the order of the solvable Galois group, may be derived using methods of logic, [En76]. It seems that the domain of relations between the algebraic degree, the order of the Galois group of the minimal polynomials and the complexity of obtaining the solution point of optimization problems is an exciting area to explore.

Acknowledgements : Sincere thanks to John Hopcroft for his inspirations and suggestions in the use of algebraic methods and to Walter Schnyder for his explanations on methods of logic.

7. References

[Ba75]

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

[Ba84]

Bajaj, C., *Geometric Optimization and Computational Complexity*, Computer Science Tech. Report, Cornell University, Ph.D. Thesis, TR84-629, 1984.

[Bu15]

Burns, J.E., *Abstract Definition of Groups of Degree Eight*, Amer. Journal of Math. 37, p195-214, 1915.

[CL82]

Collins, G.E., and Loos, R., *Real Zeros of Polynomials*, Computing Supplementum 4, Springer Verlag, p84-94, 1982.

[CR41]

Courant R., and Robbins, H., *What is Mathematics ?* Oxford University Press, 1941

[En76]

Engeler, E., *Lower Bounds by Galois Theory*, Societe' Mathematique de France, Asterisque 38-39, p45-52, 1976.

[Ga71]

Gaal, L., *Classical Galois Theory with Examples*, Markham Publishing Company, 1971.

[GGJ76]

Garey, M.R., Graham, R.L. and Johnson, D.S., *Some NP-Complete Geometric Problems*, Proceedings 8th Symposium on the Theory of Computing, p10-22,

1976.

[Gr84]

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

[He75]

Herstein, I.N., *Topics in Algebra*, 2^{nd} edition, John Wiley & sons, New York, 1975.

[Kn81]

Knuth, D.E., *The Art of Computer Programming*, vol 2, 2nd ed., Addison Wesley, Reading, MA, 1981.

[Ku67]

Kuhn, H.W., *On a pair of dual non-linear programs*, Non-Linear Programming, J. Abadie ed., p37-54, North Holland, 1967.

[Ku75]

Kung , H.T., *The Computational Complexity of Algebraic Numbers*, Siam J. of Numerical Analysis, vol 12, no1, p89-96, 1975.

[Li76]

Lipson, J.D., *Newton's Method: A Great Algebraic Algorithm*, Proceedings of the 1976 ACM Sympsoium on Symbolic and Algebraic Computation, (SYMSAC), p260-270, 1976.

[LM83]

Landau, S., and Miller, G.L., *Solvability by Radicals in Polynomial Time*, Proceedings of the 15th Annual STOC, p140-151, 1983

[Mc79]

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

[Me73]

Melzak, Z.A., *Companion to Concrete Mathematics* John Wiley & sons, New York 1973.

[Mi99]

Miller, G.A., *Memoir on the substitution groups whose degree does not exceed eight*, Amer. Journal of Math., 21, p287-337, 1899.

[PR85]

Peskin, B.R. and Richman, D.R., *A Method to Compute Minimal Polynomials*, Siam

J. Algebraic and Discrete Methods, vol 6, no. 2, p292-299, 1985.

[Ru79]

Rump, S.M., *Polynomial Minimum Root Separation* Mathematics of Computation, vol 33, no 145, p327-336, 1979.

[St73]

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

[vdW53]

van der Waerden, B.L., Modern Algebra, vol 1, Ungar, New York 1953.

[We37]

Weber, A., *Theory of the Location of Industries*, Translated by Carl J. Friedrich, The University of Chicago press, 1937.

[Za71]

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