Discrete Comput Geom 3:177-191 (1988)

Discrete & Computational
Geometry
© 1988 Springer-Verlag New York Inc.

The Algebraic Degree of Geometric Optimization Problems

Chanderjit Bajaj

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

Abstract. In this paper we apply Galois methods to certain fundamental *geometric optimization* problems whose exact computational complexity has been an open problem for a long time. In particular we show that the classic Weber problem, along with the *line-restricted* Weber problem and its *three-dimensional* version 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 numerical 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.

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 space. Such problems frequently arise in computer-aided design and robotics. 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 algebraic methods to certain fundamental *geometric optimization* problems. These problems are noncombinatorial 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 [10].

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 known to be equivalent to the geometric solution being expressible in terms of $(+, -, *, /, \sqrt{})$ over Q, the field of rationals [6], [25]. In this paper we show that certain geometric optimization problems are not solvable by *radicals*[1] over Q, (i.e., not expressible in terms of $(+, -, *, /, \sqrt[k]{})$ over Q).

We show how necessary and sufficient conditions for the existence of minima in these 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 in real Euclidean space. 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 expressing the optimizing solution by radicals.

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 kth roots. Second, this leaves only numerical or symbolic approximation to the optimum solution. In order to use numerical or symbolic approximation techniques one first needs to compute a sequence of disjoint intervais 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 [5] or Newton's iterations [16] to approximate the solution rapidly 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 $\log(1/\text{sep}(P))$ where $\text{sep}(P)$ is the minimum distance between distinct real roots of P. A lower bound for $\text{sep}(P)$ given by [22], and corrected by [23], satisfies $\text{sep}(P) > 1/(2ed^{(d+3)/2}(|P|+1)^d)$. Hence from the minimal polynomial of the nonsolvable 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. Kung [14] 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 [13]. Simply stated one wishes to obtain the optimum solution of a single *source* point in the real plane, so that the sum of the Euclidean distances to n fixed *destination* points is a minimum.

[1] 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, quotient, or the kth *root* of preceding β's and the last β_n is α.

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*

$$\text{minimize}_{x,y} f(x, y) = \sum_{i=1,\ldots,n} \sqrt{(x-a_i)^2+(y-b_i)^2}. \tag{1}$$

Weber [26] 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, whether $\sum_{i=1,\ldots,n} \sqrt{(x-a_i)^2+(y-b_i)^2} \leq L$? This problem is not even known to be in NP. Since on guessing a solution one then attempts to verify whether $\sum_{i=1,\ldots,n} \sqrt{c_i} \leq L$, in time polynomial in the number of bits needed to express certain rational numbers $c_1, \ldots, c_n$ and L. However, no such polynomial time algorithm is known [9], [10], [20]. Baker [2] 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 from 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 *three-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 [18], however, nothing was known about the nonexpressibility 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 the 1600s [13]. Cavalieri in 1647 considered the problem for this case, in particular, when the three points, say a, b, c, 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, s. Heinen in 1834 noted that in a triangle which has an angle of $\geq 120°$, the vertex of this angle itself is the minimum point (Fig. 1).

Fagnano in 1775 showed that for the case $n=4$ when the four client points, say a, b, c, d, form a convex quadrilateral the minimum solution point, s, is the

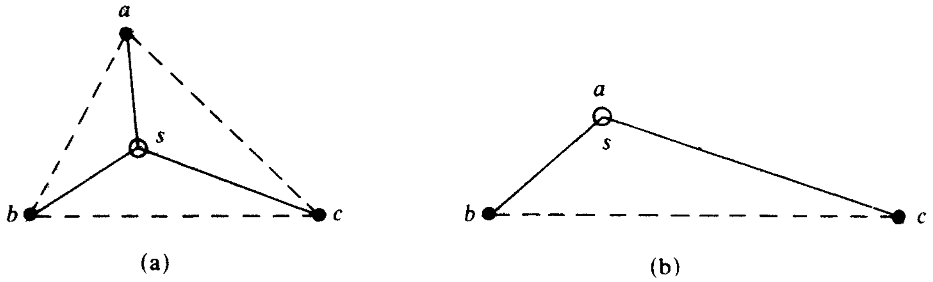


Fig. 1. Triangle with angles (a) <120° and (b) ≥120°.

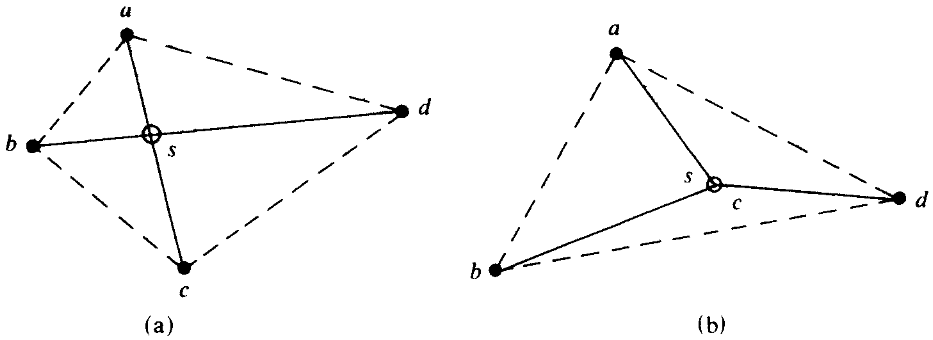


Fig. 2. (a) Convex quadrilateral and (b) nonconvex quadrilateral.

intersection of the diagonals of the quadrilateral. For a nonconvex quadrilateral the fourth point, *c*, which is inside the triangle formed by the three other points, is itself the minimum point (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, 1837, Steiner, 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.

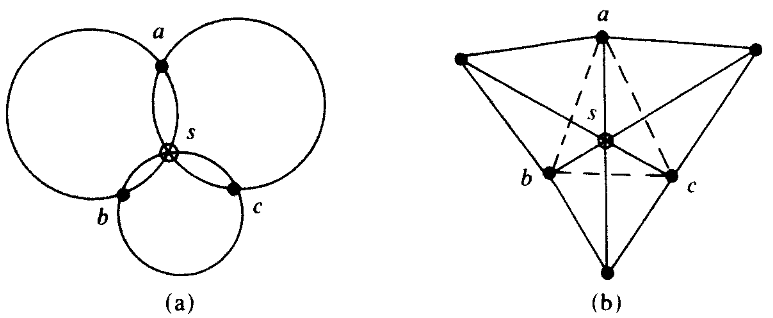


Fig. 3. (a) Steiner point and (b) Simpson point.

The constructions for the solution points for the case of three points is also worthy of note. The solution is variously obtained by the Steiner construction or the Simpson construction (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) $p=(d^2f/dx^2)_{x=x_0}>0$,
(ii) $q=(d^2f/dy^2)_{y=y_0}>0$,
(iii) $pq-r^2>0$, where $r=(d^2f/dx\,dy)_{x=x_0,y=y_0}$,

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 equations are:

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

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

Without loss of generality, we make an 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 expressions (2) and (3) above. Starting with, say, a sum of n different square roots, sqrt(i), $i=1, \ldots, n$, 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 in which 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) [25], 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 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 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 simple 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, one 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 $(a_1, b_1) = (3, 0)$, $(a_2, b_2) = (1, 3)$, $(a_3, b_3) = (0, c)$, $(a_4, b_4) = (-1, 3)$, and $(a_5, b_5) = (-3, 0)$ be the given points with integer coordinates. We choose the configuration of five points to be symmetric about the line $x = 0$. One of the points 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 we have the three possible symmetric configurations of five points (Fig. 4).

We need to find the solution $(0, y)$ satisfying the condition for minimally, $df/dy = 0$, giving us the following:

$$\text{minimize}_y f(y) = |y - c| + 2\sqrt{(y-3)^2 + 1} + 2\sqrt{y^2 + 9},$$
$$df/dy = \pm 1 + 2(y-3)/\sqrt{(y-3)^2 + 1} + 2y/\sqrt{y^2 + 9} = 0$$

according to as $y > c$ or $y < c$.[2]

Eliminating square roots by repeated squaring we obtain the polynomial $p(y)$

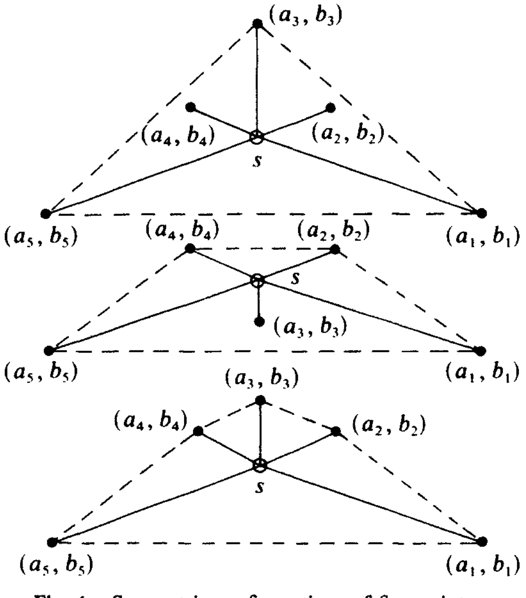


Fig. 4. Symmetric configurations of five points.

[2] The case $y = c$ occurs when the point $(0, c)$, 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. Factorizations obtained with the use of MACSYMA (actually Vaxima on Unix).

Q:	$p(y)=15y^8-180y^7+1030y^6-4128y^5+11907y^4-15876y^3-17928y^2+75816y-54756$
disc$(p(y))$:	$2^{52}3^{25}5^8 13^5 17^2 13063$
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:	$p(y)=(y+5)(y^7-17y^6+18y^5-10y^4+15y^3-16y^2+17y+4)$

(Table 1), and note that this polynomial $p(y)$ is the polynomial for each of the three configurations in Fig. 4. Equation $df/dy=0$ is the same regardless of $c=5$, 1, or 4.

We now use algebraic methods to prove the properties of interest.

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 of David Musser (see p. 434 of [12]) is a much more efficient means of proving irreducibility than merely searching for a prime q for which $p(y)$ is irreducible mod q. 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 q relative to $p(y)$ (primes q that are not divisors of disc$(p(y))$) one computes the degree set $d_q=$ set of degrees of all factors of $p(y)$ mod q. 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 a straight-edge and compass, but before that we need a few definitions. (Henceforth when we refer to constructions we mean constructions with a 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 $\alpha\in F$. Using the notation of [11], 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 nonzero polynomial of degree n but no nonzero 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 nonconstructibility.

Lemma 2 [11]. *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 $p(y) \in Q[y]$, 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 $\mathrm{Gal}(p(y))$, 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 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 nonconstructibility by straight-edge and compass constructions similar to Lemma 2 above.

Lemma 3. *If E is the splitting field over Q of an irreducible polynomial $p(y)$, and if the order of its Galois group, $o[\mathrm{Gal}(p(y))] = [E:Q]$, 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 [8] and [11].

Lemma 4 [8]. *For a finite field F, $|F| = q^n$ and $p(y) \in F[y]$ factors over F into k different irreducible factors, and if $p(y) = q_1(y) \cdots q_k(y)$, where degree $q_i(y) = n_i$, then* $\mathrm{Gal}(p(y))$ *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 q also induces a partition, namely, the partition of the degree of $p(y)$ formed by the degree of the factors. Lemma 4 above states that the degree partition of the factors of $p(y)$ modulo q is the shape of the generating permutation of the group, $\mathrm{Gal}(p(y))$, which is, furthermore, cyclic.

Lemma 5 [8]. *Let $p(y) \in Z[y]$ and let $p^*(y) \in Z_q[y]$ be the polynomial $p(y)$* mod q *where q is a* good[3] *prime for $p(y)$. Then* $\mathrm{Gal}(p^*(y))$ *is* isomorphic *to a subgroup of* $\mathrm{Gal}(p(y))$.

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

[3] A good prime for a polynomial $p(y)$ is one which does not divide the discriminant of the polynomial $\mathrm{disc}(p(y))$.

Proof. Restating the assertion, we have to show that the roots of the polynomial $p(y)$ of Table 1 are not constructible by a straight-edge and compass. We know that $p(y)$ is irreducible over Q from Lemma 1. Let $p^*(y)$ be the polynomial $p(y)$ mod q for a good prime $q=37$ 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}, $o[\mathrm{Gal}(p(y))]=7$ and, from Lemma 5, it is a divisor of $o[\mathrm{Gal}(p(y))]$, which clearly is not a power of 2 and hence Lemma 3 proves our assertion. □

To prove the *nonexpressibility* of the roots of $p(y)$ over Q by radicals we use the Cebotarev-Van der Waerden sampling method to determine the Galois group of $p(y)$ [17], [27]. From the density theorem of Cebotarev 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 q_i $(i=1,\dots,s)$, tends to the proportion of permutations in $\mathrm{Gal}(p(y))$ whose shape is π.*

Then in order to 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 [4], [24]. The degree of concern for the polynomial $p(y)$ of Table 1 is 8. From [19] we know that there are exactly 200 permutation groups of degree 8. However all is not lost. We also know that polynomial $p(y)\in Q$ is irreducible iff the Galois group $\mathrm{Gal}(p(y))$ is *transitive*[4] [25], and there are only 50 transitive groups of degree 8.

Furthermore, if the Galois group of the polynomial $p(y)$ of degree n is the symmetric group S_n (the group of all permutations of $[1,\dots,n]$), we have:

Lemma 8. *If $n\equiv 0 \pmod 2$ and $n>2$ then the occurrence of an $(n-1)$-cycle and an n-cycle and a permutation of the type $2+(n-3)$ on factoring the polynomial $p(y)$ modulo "good" primes establishes that $\mathrm{Gal}(p(y))$ over Q is the symmetric group S_n. If $n\equiv 1 \pmod 2$ then an $(n-1)$ cycle and an n cycle and a permutation of the type $2+(n-2)$ is enough.*

Proof. Since for $n\equiv 0 \pmod 2$, $n-3$ 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, generates the symmetric group S_n as follows. Let $(12,\dots,n-1)$ be the $(n-1)$-cycle. By virtue of transitivty, 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 $(12,\dots,n-1)$ and its powers yield all cycles $(1n)(2n)\cdots(n-1n)$ and these cycles together generate the symmetric group S_n [25]. For $n\equiv 1 \pmod 2$, 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 and the n-cycle generates the symmetric group as above. □

[4] A permutation group on $1,\dots,n$ is called transitive if for any k, $1\le k\le n$, it contains a permutation π which sends 1 to k.

Zassenhaus [27] observes that using the Cebotarev-Van der Waerden method for the symmetric S_n group, sampling about $n+1$ good primes are sufficient. Usually the decision that $\mathrm{Gal}(p(y)) = S_n$ is reached even after much less than $n+1$ trials as a consequence of the evolving pattern of permutations occurring in $\mathrm{Gal}(p(y))$ and the application of known theorems of permutation groups.

We are now ready to prove our main theorem, but first let us indulge (for the last time) in some definitions. A polynomial $p(y) \in Q[y]$ 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 $\alpha_i^{n_i} \in F_i$ 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 [11]. *$p(y) \in Q[y]$ is solvable by radicals over Q* iff *the Galois group over Q of $p(y)$,* $\mathrm{Gal}(p(y))$*, is a solvable group.*

Lemma 10 [11]. *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 $q = 19$, 31, and 37, the degrees of the irreducible factors of $p(y) \bmod q$ 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 $\mathrm{Gal}(p(y)) = S_8$, 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 real plane with coordinates (a_i, b_i), we need to determine the location (x, y) of a single *source* point, restricted to lie on a 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 nontrivial case of three 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(a)) *or* passing through the convex-hull (Fig. 5(b)).

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

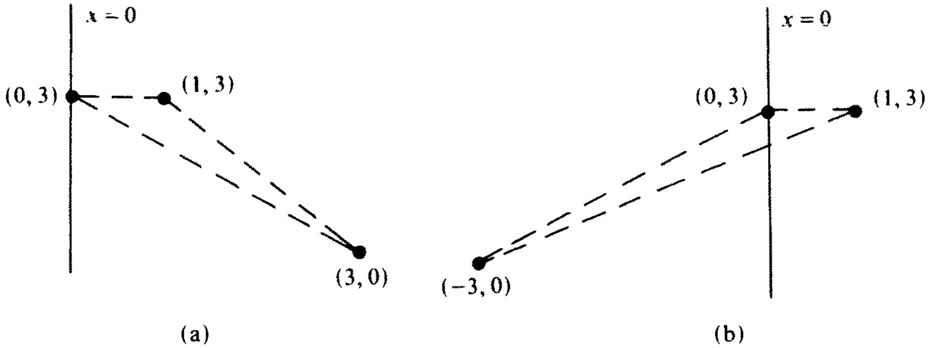


Fig. 5

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

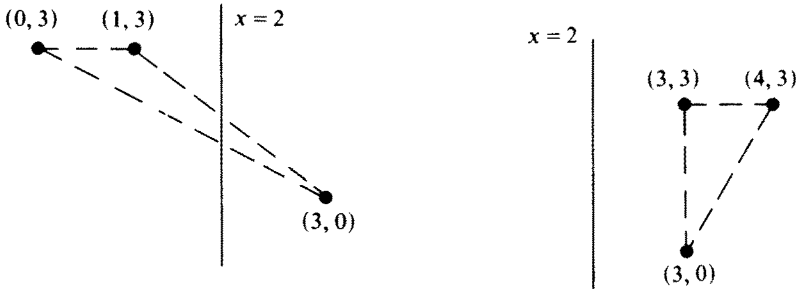
As before, for the case of $n=3$ destination points consider the solution restricted to a line, however, not passing through any of the three points and *either* not intersecting the convex-hull (of the destination points) (Fig. 6(a)) *or* passing through the convex-hull (Fig. 6(b)).

Lemma 13. *For the cases of Fig.* 6(a) *and* (b), *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 nonsolvability by radicals, we again apply Lemma 8 for $n=8$ and note from Table 2 that for the "good" primes

Table 2

	minimize, $f(y)=3-y+\sqrt{(y-3)^2+1}+\sqrt{y^2+9}$
	$df/dy=-1+(y-3)/\sqrt{(y-3)^2+1}+y/\sqrt{y^2+9}=0$
Q:	$p(y)=3y^8-36y^7+202y^6-780y^5+2277y^4-4212y^3+3402y^2-81=0$
disc($p(y)$):	$2^{38}3^{23}5^{6}13^{3}19687$
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:	$p(y)=(y+13)(y^2+5y-11)(y^5-y^4+12y^3+11y^2+2y+1)=0$



(a) (b)

Fig. 6

$q = 7$, 19, and 61 the degrees of the irreducible factors of $p(y) \bmod q$ give us a 12-cycle, an 11-cycle and a $2+9$ permutation which is enough to establish that $\mathrm{Gal}(p(y)) = S_{12}$, 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. □

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 two of the three given destination points, the solution 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.

Table 3

	minimize, $f(y) = \sqrt{(y-3)^2+4} + \sqrt{(y-3)^2+1} + \sqrt{y^2+1}$ $df/dy = (y-3)/\sqrt{(y-3)^2+4} + (y-3)/\sqrt{(y-3)^2+1} + y/\sqrt{y^2+1} = 0$
Q:	$p(y) = 3y^{12} - 72y^{11} + 780y^{10} - 4002y^9 + 20772y^8 - 58500y^7 + 113610y^6$ $- 155448y^5 + 156912y^4 - 119040y^3 + 51786y^2 + 972y - 729 = 0$
disc($p(y)$):	$2^a 3^b 5^c 13^d p$
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:	$p(y) = (y+13)(y^2 - 3y + 10)(y^9 + 27y^8 + 19y^6 - 7y^5 + y^4 - 10y^3 - 25y^2 - 21y + 23) = 0$

5. Euclidean Three-Dimension Space

The Weber problems that we have considered can also be generalized to the case of noncoplanar points in real Euclidean three-dimension space. The simplest case here corresponds to four noncoplanar points forming a tetrahedron. The solution point which minimizes the sum of the Euclidean distances from these four 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 (namely, pairs of lines subtending equal angles at the solution point). The problem in three dimensions thus appears more difficult and as we suspect, in general, not solvable by radicals over Q. We show this to be true for the case of four noncoplanar points with the solution restricted to a line passing through one of the given points, as illustrated by Fig. 7.

Theorem 15. *The* three-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 four noncoplanar points corresponds to a case of four 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 (a) and (b) of Fig. 7. For $p_1(y)$ of degree 6, we note from Table 4 that for the "good" primes $q = 17$, 19, and 29, degrees of the irreducible factors of $p_1(y) \bmod q$ give us a 5-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 $q = 19$, 31, and 37, the degrees of the irreducible factors of $p_2(y) \bmod q$ give us a 10-cycle, a 9-cycle, and a 2+7 permutation, which is again enough to establish our assertion. □

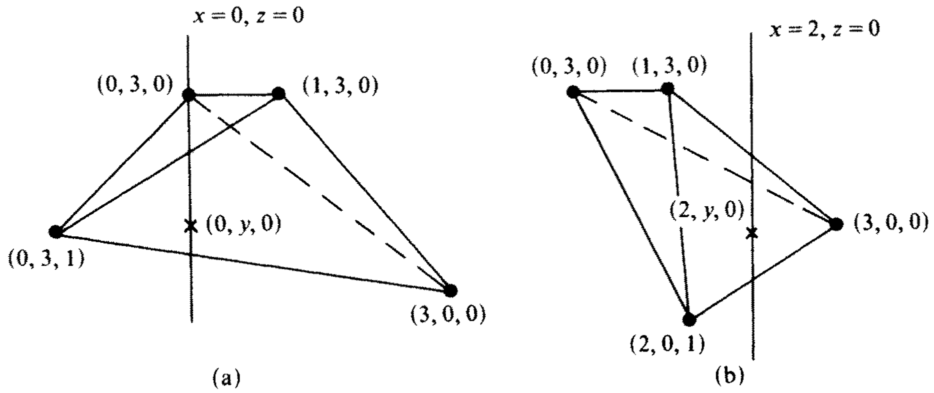


Fig. 7

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 permutation
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 permutation

6. Discussion and 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 [21]. 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 [15]. From the minimal polynomial of the nonsolvable 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 [7]. 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.

Acknowledgments

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

References

1. C. Bajaj, Geometric Optimization and Computational Complexity, Computer Science Technical Report TR84-629, Ph.D. thesis, Cornell University, Ithaca, NY, 1984.
2. A. Baker, *Transcendental Number Theory*, Cambridge University Press, Cambridge, 1975.
3. J. Burns, Abstract definition of groups of degree eight, *Amer. J. Math.* **37** (1915), 195-214.
4. C. Butler and J. McKay, The transitive groups of degree up to 11, *Comm. Algebra* **11** (1983), 863-911.

5. G. E. Collins and R. Loos, Real zeros of polynomials, in *Computing Supplementum*, vol. 4 (B. Buchberger *et al.*, eds.), 84–94, Springer-Verlag, Wien, New York, 1982.
6. R. Courant and H. Robbins, *What is Mathematics?*, Oxford University Press, Oxford, 1941.
7. E. Engeler, Lower bounds by Galois theory, *Astérisque* **38–39** (1976), 45-52.
8. L. Gaal, *Classical Galois Theory with Examples*, Markham, 1971.
9. M. R. Garey, R. L. Graham, and D. S. Johnson, Some NP-complete geometric problems, *Proceedings of the Eighth Symposium on the Theory of Computing*, 10–22, 1976.
10. R. L. Graham, Unsolved problem P73, problems and solutions, *Bull. EATCS* (1984), 205-206.
11. I. N. Herstein, *Topics in Algebra*, 2nd ed., Wiley, New York, 1975.
12. D. E. Knuth, *The Art of Computer Programming*, vol. 2, 2nd edn., Addison-Wesley, Reading, MA, 1981.
13. H. W. Kuhn, On a pair of dual non-linear programs, in *Non-Linear Programming* (J. Abadie, ed.), 37-54, North-Holland, Amsterdam, 1967.
14. H. T. Kung, The computational complexity of algebraic numbers, *SIAM J. Numer. Anal.* **12** (1975), 89-96.
15. S. Landau and G. L. Miller, Solvability by radicals in polynomial time, *Proceedings of the 15th Annual Symposium on the Theory of Computing*, 140-151, 1983.
16. J. D. Lipson, Newton's method: a great algebraic algorithm, *Proceedings of the 1976 ACM Symposium on Symbolic and Algebraic Computation (SYMSAC)*, 260-270, 1976.
17. J. McKay, Some remarks on computing Galois groups, *SIAM J. Comput.* **8** (1979), 344-347.
18. Z. A. Melzak, *Companion to Concrete Mathematics*, Wiley, New York, 1973.
19. G. A. Miller, Memoir on the substitution groups whose degree does not exceed eight, *Amer. J. Math.* **21** (1899), 287-337.
20. A. M. Odlyzko, Personal Communication, May 1985.
21. B. R. Peskin and D. R. Richman, A method to compute minimal polynomials, *SIAM J. Algebraic Discrete Methods* **6** (1985), 292-299.
22. S. M. Rump, Polynomial minimum root separation, *Math. Comp.* **33** (1979), 327-336.
23. J. T. Schwartz, Polynomial Minimum Root Separation (Note to a Paper of S. M. Rump), Robotics Research Technical Report No. 39, New York University, 1985.
24. R. P. Stauduhar, The determination of Galois groups, *Math. Comp.* **27** (1973), 981-996.
25. B. L. Van der Waerden, *Modern Algebra*, vol. 1, Ungar, New York, 1953.
26. A. Weber, *Theory of the Location of Industries* (translated by Carl J. Friedrich), The University of Chicago Press, Chicago, 1937.
27. H. Zassenhaus, On the group of an equation, *Computers in Algebra and Number Theory, SIAM and AMS Proceedings*, 69-88, 1971.

Received May 13, 1986, and in revised form October 3, 1986.