J. Symbolic Computation (1986) 2, 99–102

Proving Geometric Algorithm Non-solvability: An Application of Factoring Polynomials

CHANDERJIT BAJAJ

Department of Computer Science,
Purdue University, West Lafayette, IN 47907, U.S.A.

(*Received* 10 *September* 1985)

We explain how factoring polynomials modulo primes can be used in proving that for certain geometric optimisation 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. This leaves only numerical or symbolic approximations to the solution of these problems under these models. This letter describes work which is described in more detail in Bajaj (1984)—here we concentrate on the use of computer algebra, in particular factoring polynomials over the rationals using the MACSYMA system.

Consider the following geometric problem which is of fundamental importance with an equally long and interesting history. 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*
>
> $$\textit{minimise}_{x,y}\, f(x, y) = \sum_{i=1\ldots n} \sqrt{(x-a_i)^2+(y-b_i)^2}.$$

Weber (1937) was probably the first who formulated this problem in light of the location of a plant, with the objective of minimising the sum of transportation costs from the plant to two sources of raw materials and a market centre. Hence this problem for n points has also come to be known as the *Generalised Weber* problem. In the decision version of this problem we ask if there exists (x, y) such that for given integer L,

$$\sum_{i=1\ldots n} \sqrt{(x-a_i)^2+(y-b_i)^2} \leqslant L?$$

This problem is not even known to be in NP. Since on guessing a solution one then attempts to verify *if*

$$\sum_{i=1\ldots n} \sqrt{c_i} \leqslant L\,?,$$

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 (Graham, 1984; Odlyzko, 1985). Such a decision problem is fundamental in that it also occurs in numerous other geometric optimisation problems such as in finding the minimum length Euclidean Travelling Salesman Tour and the minimum length Euclidean Steiner Tree.

0747-7171/86/010099+04 $03.00/0

The solution to the Generalised 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 $n=4$. 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 (Kuhn, 1967). 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 $\geqslant 120°$, the vertex of this angle itself is the minimum point. 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. We show that for the case of $n=5$ points (and greater), in general the solution is the root of an irreducible polynomial of high degree which is not solvable by radicals over Q, the field of rationals. For variants of the problem, namely the *Line-restricted* Weber problem, where the optimum solution is constrained to lie on a certain given *line*, and for the problem in Euclidean 3-space, much stronger result hold. We show that the Line-restricted Weber problem, in general, is not solvable by radicals over Q for $n \geqslant 3$ points, and the same applies to the *3-Dimension* Weber problem, for $n \geqslant 4$ points. This in effect proves that for these geometric optimisation 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, and leaves only numerical or symbolic approximations to the solution of these problems (Collins & Loos, 1982).

We obtain these 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 minimised can be shown to be strictly convex. Hence there exists a *unique* minimum solution for which the necessary and sufficient conditions are $\mathrm{d}f/\mathrm{d}x=0$ and $\mathrm{d}f/\mathrm{d}y=0$. The corresponding rational equations are

$$\mathrm{d}f/\mathrm{d}x = \sum_{i=1\ldots n} (x-a_i)/\sqrt{(x-a_i)^2+(y-b_i)^2} = 0$$

$$\mathrm{d}f/\mathrm{d}y = \sum_{i=1\ldots n} (y-b_i)/\sqrt{(x-a_i)^2+(y-b_i)^2} = 0.$$

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 rationalising 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) (van der Waerden, 1953) leading to a single polynomial equation $p(y)=0$ in a single variable.

For the Weber problem we consider a case of 5 points in the plane and on applying the above technique obtain the single variate polynomial $p(y)$ for the problem. We note that 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 rationalising and eliminating square roots were done using MACSYMA giving us the final polynomial equation below

$$Q: p(y) = 15y^8 - 180y^7 + 1030y^6 - 4128y^5 + 11907y^4 \\ - 15876y^3 - 17928y^2 + 75816y - 54756.$$

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 $o[\mathrm{Gal}(p(y))]$, 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. Next, for the case where the Galois group of the polynomial $p(y)$ of degree n is the symmetric group, S_n (the group of all permutations of $[1 \ldots n]$), we note the following. If $n \equiv 0 (\mathrm{mod}\ 2)$ and $n > 2$ 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 suitable primes (that do not divide the discriminant of $p(y)$), establishes that $\mathrm{Gal}(p(y))$ over Q is the symmetric group S_n. If $n \equiv 1 (\mathrm{mod}\ 2)$, then an $(n-1)$-cycle and a permutation of the type $2+(n-2)$ is enough. This from primarily noting the fact that the Galois group of an irreducible polynomial $p(y) \in Q$, is transitive. 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, which is enough to establish for our polynomial of degree 8, that $\mathrm{Gal}(p(y)) = S_8$, the symmetric group of degree 8, which is not a solvable group and hence our assertion.

Such a method of using the degrees of the irreducible factors of polynomials modulo primes to determine the Galois group has come to be known as the *Ceboratev–van der Waerden* sampling method (Zassenhaus, 1971). 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. These tables can become very large, for example, we know that there are exactly 200 permutation groups of degree 8 (Miller, 1899). Group theory systems like CAYLEY could prove quite useful in this regard. To check whether the Galois group is the symmetric group, however, is much easier. As Zassenhaus (1971) observes and as we also noticed, using the degrees of factorisations modulo about $n+1$ suitable primes are sufficient in nearly all cases to confirm the S_n group. In fact in most cases 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 $\mathrm{Gal}(py))$ and the application of known theorems of permutation groups.

Carrying out the same algebraic reduction technique for variants of the Weber problem we obtained for the Line-restricted version a minimal polynomial of degree 12. This for the case of 3 points in the plane and a line not passing through these points

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

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 factorisations modulo primes, that its Galois group is the non-solvable S_{10} group. In conclusion we feel that the method outlined above should prove quite universal and may be applied to numerous other problems. As examples we have used this approach to show the limitations of algorithm solvability to problems in robotics such as obtaining shortest paths in the presence of polyhedral obstacles, additional location problems and object recognition problems. A note to mention here is that factoring polynomials into irreducible factors over the rationals and finite fields was possible due to the MACSYMA system, actually Vaxima on UNIX. However, such factorisations are both time and space inefficient and are practical only when the algebraic degree of the problem (of the minimal polynomial), is low. For the above problems we were fortunate in this regard.

References

Bajaj, C. (1984). *The Algebraic Degree of Geometric Optimization Problems*. Computer Science Tech. Report, Purdue University, TR84-496.

Collins, G. E., Loos, R. (1982). Real Zeros of Polynomials. In: (Buchberger, B., Collins, G., Loos, R., eds) *Computing Supplementum 4*, pp. 84–94, New York: Springer Verlag.

Graham, R. L. (1984). Unsolved Problem P73, Problems and Solutions. *Bull. EATCS:* 205–206.

Kuhn, H. W. (1967). On a pair of dual non-linear programs. In: (Abadie, J., ed.) *Non-Linear Programming*, pp. 37–54. Amsterdam: North-Holland.

Miller, G. A. (1899). Memoir on the substitution groups whose degree does not exceed eight. *Am. J. Math.* **21**, 287–337.

Odlyzko, A. M. (1985). Personal communication.

van der Waerden, B. L. (1953). *Modern Algebra*, vol. 1. New York: Ungar.

Weber, A. (1937). *Theory of the Location of Industries*. Translated by Carl J. Friedrich. Chicago: University of Chicago Press.

Zassenhaus, H. (1971). On the group of an equation. *Computer in Algebra and Number Theory*, SIAM and AMS proceedings, pp. 69–88.