THE ALGEBRAIC COMPLEXITY OF SHORTEST PATHS IN POLYHEDRAL SPACES

Chanderjit Bajaj

CSD-TR-523
June 1985

The Algebraic Complexity of Shortest Paths in Polyhedral Spaces

Chanderjit Bajaj

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

ABSTRACT

In this paper we show that the problem of finding the shortest path between two points in Euclidean 3-space, bounded by a finite collection of polyhedral obstacles, is in general not solvable by radicals over the field of rationals. The problem is shown to be not solvable even for the case when only two obstacle edges are encountered in the shortest path in 3-space. One direct consequence of the non-solvability by radicals is that for the shortest path problem there cannot exist an *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 primarily a function of the algebraic degree of the optimum solution.

For special relative orientations of the polyhedral obstacles however the shortest path is shown to be straight-edge and compass constructible. Simple polynomial time exact algorithms are known for such cases.

The Algebraic Complexity of Shortest Paths in Polyhedral Spaces

Chanderjit Bajaj

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

1. Introduction

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 long known 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 that the problem of finding the shortest path between two points in Euclidean 3-space, bounded by a finite collection of polyhedral obstacles, is in general not solvable by *radicals*† over Q. We generate the minimal polynomial whose root over the field of rational numbers is the solution of the shortest path problem. We show the generated polynomial to be minimal by proving it irreducible over Q and use Galois theory to prove the polynomial to be *not* solvable by examining the structure of its Galois group. For special relative orientations of the polyhedral obstacles however we show the shortest path to be straight-edge and compass *constructible*‡.

A number of immediate consequences arise from the non-solvability of the shortest path problem. First, for this problem in general there cannot exist *exact* algorithms 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 numerical or symbolic approximations to the optimum solution. In order to use numerical 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

---

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

‡ Henceforth by constructible we shall mean straight-edge and compass constructible.

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 shortest path problem one can 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 numericalal 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.

2. Shortest Path Problem

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. In Euclidean 2-space (the Euclidean plane) the problem is easy to solve and the shortest path is polynomial time computable, [LW79].

The problem for Euclidean 3-space is much harder and known shortest path computations require exponential time, [SS84]. In Euclidean 3-space the shortest path between two given points, in the presence of polyhedral obstacles, can be again shown to be piecewise straight lines (*polygonal* lines), as for the planar 2-dimensional problem, with break points that lie on the edges of the given polyhedral obstacles. Since the edges of the polyhedral obstacles are arbitrary lines in Euclidean 3-space, the problem of determining the points of contact of the shortest path with these edges can without loss of generality be versed also as follows.

> *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.*

We identify three different cases of the relative positions of the lines. All the various configurations of the n lines in 3-space consist of combinations of these basic orientations between pairs of lines.

(a) Lines are parallel to each other.

(b) Lines are not parallel but intersect.

(c) Lines are skew and do not intersect.

In § 3, we show that when the lines are oriented as a combination of the cases (a) and (b), then the shortest path problem in Euclidean 3-space is constructible. Simple polynomial time exact algorithms are known for such cases, [BM85]. However in § 4, we show that for the case (c) of even two skew lines the solution is not constructible and furthermore not solvable by radicals. This leaves only numericalal or symbolic approximations to the shortest path, [SS84] and [BM85].

3. The Constructible Cases

The complexity of straight-edge and compass constructions has been long known to be equivalent to the geometric solution being expressible in terms of $(+,-,*,/,\sqrt{})$ over Q, the field of rationals [CR41],[vdW53]. We now show that when the lines are oriented as a combination of the cases (a) and (b), then the solution to the shortest path problem is always expressible in terms of $(+,-,*,/,\sqrt{})$ over Q.

Between pairs of lines in 3-space which are parallel to each other there exists a unique plane which contains both of them. The same applies to pairs of lines in 3-space which intersect. Also a point and a line in 3-space define a unique plane between them. The problem of finding the shortest path between X and Y in 3-space for cases (a) and (b), then reduces to a constrained 2-1/2 dimensional space problem as follows. Let the point X and line l_1 define the plane P_1, the lines l_i and l_{i+1} define the planes P_{i+1}, $i=1..n-1$, and the line l_n and the point Y define the plane P_{n+1}. The original problem is now reduced to finding the shortest path between two points X and Y in 3-space with the path constrained to the planes P_i, $i=1..n$, (Figure 1). On unfolding all the planes P_i to a common plane P_1, the straight line connecting X and the corresponding transformed point, Y' is clearly the shortest path and one that subtends equal angles, at each of the lines l_i'. The length of the path as well as the subtended angles remain invariant under the above unfoldings and thus the shortest path from X to Y which passes through the given sequence of lines l_i enters and leaves l_i at equal angles. 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.

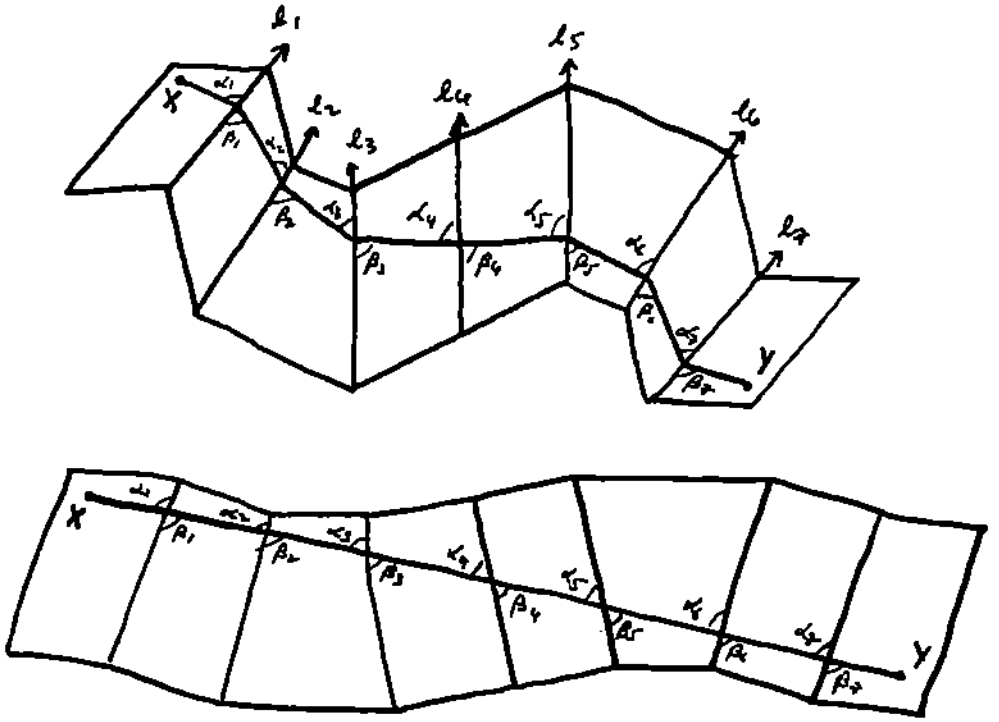

Figure 1: Lines which are Parallel or Intersect

For the case (a) of parallel lines, since 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. We are given the cartesian coordinates (a_1,a_2,a_3) and (b_1,b_2,b_3) of the points X and Y respectively and the line vectors l_i, all values over Q. Without loss of generality we can assume all lines l_i to be parallel to the x axis. The contact points on lincs l_i could then be taken to be x_i,y_i,z_i where we need to determine the unknowns x_i with the values of y_i and z_i being constant. The equation $\alpha_1=\beta_n$ or equivalently the equation $Cos\,\alpha_1 = Cos\,\beta_n$ (equality of the direction cosines) is then expressed as

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

Simplifying the equation 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.

For the case (b) of intersecting lines, since l_i intersects l_{i+1}, we have in addition to the set of equations (1) the set of equations

$$\alpha_{i+1} = \beta_i + c_i \ , \quad i=1..n-1 \qquad (3)$$

where c_i is the angle between l_i and l_{i+1} and is a constant value independent of the unknowns. This linear dependence amongst the angles is again sufficient to make each of the unknowns x_i, $i=1..n$ to be expressible in terms of $(+,-,*,/,\sqrt{})$ over constant values of Q and hence constructible.

4. The Non-Solvable Case

Even for skew lines the piecewise straight line shortest path enters and leaves each line l_i at equal angles [SS84]. However when any two adjacent lines l_i and l_{i+1} are skew to one another there exists no common plane containing both of them. Hence simplifications of the previous section are no longer possible. In fact we show that even for the case of two skew lines the solution is not constructible and furthermore not constructible by radicals. Consider the configuration of two skew lines as shown in Figure 2. We wish to obtain the shortest path between points X and Y which pass through interior points of lines l_1 and l_2 in that order. Stating it algebraically we wish to minimize the length of the path $XC + CD + DY$ where C and D are interior points of the lines l_1, l_2.

$$minimize_{x,z} \ f(x,z) = \sqrt{(z-3)^2+5} + \sqrt{z^2+x^2+4} + \sqrt{(x-3)^2+1}$$

From the fact that in the shortest path, the path segments CD and DY subtend equal angles with the line l_2 we obtain

$$x/\sqrt{x^2+z^2+4} = (x-3)/\sqrt{(x-3)^2+1}$$

and thereby

$$x = 3 + 3/(\sqrt{z^2+4}-1)$$

Substituting for x in $f(x,z)$ we reduce the shortest path problem for the above configuration to a minimization problem in a single variable.

$$minimize_z \ g(z) = \sqrt{(z-3)^2+5} + (1/(\sqrt{z^2+4}-1))$$
$$(\sqrt{(z^2+4)(z^2+14-2\sqrt{z^2+4}} + \sqrt{z^2+14-2\sqrt{z^2+4}})$$

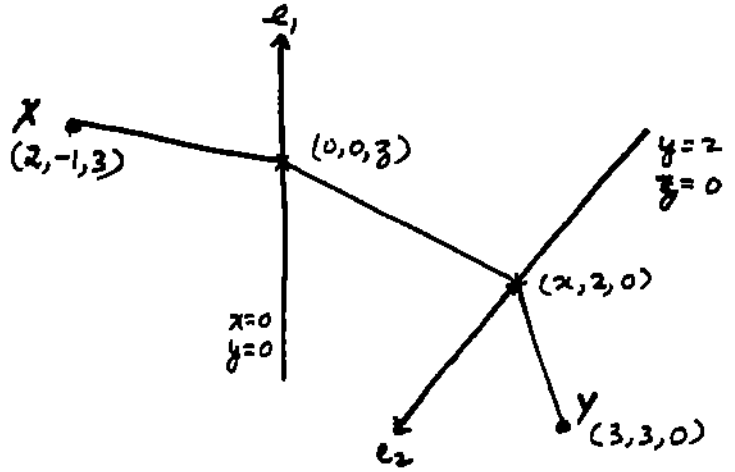

Figure 2: Skew Lines

The shortest path problem in Euclidean 3-space has a unique minimum, Sharir, Schorr [4]. The above function $g(z)$ can also shown to be strictly convex. Hence for the unique minimum solution the necessary and sufficient condition is $dg/dz = 0$. The corresponding rational equation is

$$dg/dz = (z-3)/\sqrt{(z-3)^2+5} + z(\sqrt{z^2+4}+1)/\sqrt{z^2+4}(\sqrt{(\sqrt{z^2+4}-1)^2+9}$$
$$-2z(\sqrt{z^2+4}+1)^2\sqrt{(\sqrt{z^2+4}-1)^2+9}/(z^2+3)^2\sqrt{z^2+4} = 0$$

By a process of repeated squaring one can eliminate all the square-roots from the rational equation 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 independent 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. Eliminating square-roots we obtain the polynomial,$h(z)$, with the following factorization over Q, (*Table* 1). Since the first two factors of $h(z)$ have only complex roots we obtain $q(z)$, (*Table* 1) as the polynomial whose real root is the solution to our problem. Our first step is to prove it irreducible, over Q.

Table 1

$$Q\ : h(z)=(z^2+3)^2(z^2+4)^2(z^{20}-12z^{19}+99z^{18}-648z^{17}+3334z^{16}$$
$$-14976z^{15}+56370z^{14}-183360z^{13}+512669z^{12}-1255452z^{11}+2578119z^{10}$$
$$-5006952z^9+7175196z^8-9864504z^7+3160836z^6+26727408z^5$$
$$-71592336z^4+185698656z^3-167588352z^2-25194240z+18895680)$$
$$Q\ : q(z)=z^{20}-12z^{19}+99z^{18}-648z^{17}+3334z^{16}-14976z^{15}+56370z^{14}$$
$$-183360z^{13}+512669z^{12}-1255452z^{11}+2578119z^{10}-5006952z^9$$
$$+7175196z^8-9864504z^7+3160836z^6+26727408z^5-71592336z^4$$
$$+185698656z^3-167588352z^2-25194240z+18895680$$
$$Disc\,(q(z)):\qquad 2^i 3^j 5^k 61^l\, largeprime\ (>100)$$
$$Mod\ 37:\ q(z)=(z-10)(z^{19}-2z^{18}+5z^{17}-6z^{16}+18z^{15}+4z^{14}-15z^{13}+10z^{12}$$
$$-14z^{11}+3z^{10}-11z^9+8z^7-2z^6+17z^5-z^4-10z^3-4z^2-15)$$
$$Mod\ 47:\ q(z)=(z^{20}-12z^{19}+5z^{18}+10z^{17}-3z^{16}+17z^{14}-13z^{13}-7z^{12}$$
$$+12z^{11}-19z^{10}+5z^9-12z^8-3z^7-8z^6+12z^5-9z^4+11z^3+18z^2+16z-12)$$
$$Mod\ 79:\ q(z)=(z+20)(z^2-6z-15)(z^{17}-26z^{16}-34z^{15}+15z^{14}-23z^{13}$$
$$+2z^{12}-12z^{11}+15z^{10}-7z^9-39z^8+26z^7+2z^6+19z^5-28z^4$$
$$-31z^3+33z^2-20z+9)$$

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

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

Proof : Since the monic polynomial $q(z)$ is irreducible mod the prime 47 it follows that $q(z)$ is irreducible over Q and is our minimal polynomial. □

As our next step we show the impossibility of constructions with straight-edge and compass. The following important criterion for non-constructibility suffices.

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.

Theorem 3 : The solution of the shortest path problem, in general, is not *constructible* by straight-edge and compass for $n \geq 2$, where n is the number of

obstacle

edges encountered in the shortest path.

Proof : Through the foregoing algebraic reduction, we only need to show that the roots of the polynomial $q(z)$ of *Table* 1 are not constructible by straight-edge and compass. We know that $q(z)$ is irreducible over Q from *Lemma* 1 and direct use of *Lemma* 2 proves our assertion. □

We now state a few facts from Galois theory to explain the method we use to prove the non-solvability of the roots of $q(z)$ over Q by radicals. The following are well known and proofs and details may be found in [vdW53],[He75],[Ga71].

A polynomial $q(z) \in Q[y]$ 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 $q(z)$ lie in F_k, that is , $E \subseteq F_k$, where E is the *splitting field* of $q(z)$. F_k is called a *radical extension* of Q. If $q(z) \in Q[y]$, a finite extension E of Q is said to be a *splitting field* over Q for $q(z)$ if over E but not over any proper subfield of E, $q(z)$ can be factored as a product of linear factors. Alternatively, E is a *splitting field* of $q(z)$ over Q if E is a *minimal* extension of Q in which $q(z)$ has n roots, where n =degree of $q(z)$. Given a polynomial $q(z)$ in $Q[y]$, the polynomial ring in y over Q, we shall associate with $q(z)$ a group, $Gal(q(z))$, the Galois group of $q(z)$. 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 $q(z)$ 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.

Lemma 4: [*Ga71*] For a finite field F, $|F| = p^n$ and $q(z) \in F[y]$ factors over F into k different irreducible factors, $q(z) = q_1(y)\ldots q_k(y)$, where degree $q_i(y) = n_i$, then $Gal(q(z))$ 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 $q(z)$ formed by the degree of the factors. The above *Lemma* 4 states that the degree

partition of the factors of $q(z)$ modulo p is the shape of the generating permutation of the group, $Gal\,(q(z))$, which is furthermore cyclic. To prove the non-solvability of $q(z)$ over Q by radicals we use the *Ceboratev−Van der Waerden* sampling method to determine the Galois group of $q(z)$, [Mc79],[Za71]. From the density theorem of Ceboratev one obtains,

> *Lemma 5:* As $s \to \infty$, the proportion of occurrences of a partition π as the degree partition of the factorization of $q(z) mod\ p_i$, $(i = 1..s)$, tends to the proportion of permutations in $Gal\,(q(z))$ 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]. We could restrict our attention to *transitive*† permutation groups since we know that polynomial $q(z) \in Q$ is irreducible *iff* the Galois group, $Gal\,(q(z))$ is transitive, [vdW53]. 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 in fact realizes this very quickly. Indeed,

> *Lemma 6:* [*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 $Gal\,(q(z))$ 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

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

‡ A good prime for a polynomial $q(z)$ is one which does not divide the discriminant of the polynomial, $disc\,(q(z))$.

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. □

We are now ready to prove our main theorem. From Galois theory we know that

Lemma 7 : [*He75*] $q(z) \epsilon Q[y]$ is solvable by radicals over Q *iff* the Galois group over Q of $q(z)$, $Gal(q(z))$ is a solvable group.

Lemma 8 : [*He75*] The symmetric group S_n is not solvable for $n \geq 5$.

Theorem 9: The shortest path problem, in general, is not solvable by radicals over Q for $n \geq 2$, where n is the number of obstacle edges encountered in the shortest path.

Proof : Restating the assertion, we need to show that the polynomial $q(z)$ of *Table* 1 is not solvable by radicals over Q. We note from *Table* 1 that for the 'good' primes p =37,47 and 79, the degrees of the irreducible factors of $q(z)$ mod p gives us a 2 + 17 permutation, a 20 cycle and a 19 cycle, which is enough to establish, from *Lemma* 6 for n =20, that $Gal(q(z)) = S_{20}$, the symmetric group of degree 20. *Lemma* 8 tells us that this is not a solvable group and hence our assertion follows from *Lemma* 7. □

5. Discussion & Further Research

We have used an algebraic reduction procedure to obtain the minimal polynomial, whose root over the field of rational numbers is the solution of the shortest path problem in Euclidean 3-space. This may be applied to a number of other optimization problems as well [Ba84]. Other methods of computing minimal polynomials could also be used [PR85]. Having obtained the minimal polynomial one uses 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.

6. References

[Ba75]
Baker, A., *Transcendental Number Theory*, Cambridge University Press,1975.

[Ba84]
Bajaj, C., *The Algebraic Degree of Geometric Optimization Problems*, Computer Science Tech. Report, Purdue University, TR84-496, 1984.

[BM85]
Bajaj, C., and Moh, T., *Generalized Unfoldings for Shortest Paths in Euclidean 3-Space*, Computer Science Tech. Report, Purdue University, TR85-526, 1985.

[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.

[He75]
Herstein, I.N., *Topics in Algebra*, 2^{nd} edition, John Wiley & sons, New York, 1975.

[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

[LW79]
Lozano-Perez, T., and Wesley, M.A., *An algorithm for planning collision free paths among polyhedral obstacles*, CACM 22, p560-570, 1979.

[Mc79]
McKay, J., *Some Remarks on Computing Galois Groups*, Siam J. of Comp., vol 8, no 3, p344-347, 1979.

[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.

[SS84]
Sharir, M., and Schorr, A., *On shortest paths in polyhedral spaces*, Proceedings 16th STOC, p144-153, 1984.

[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.

[Za71]
Zassenhaus, H., *On the Group of an Equation* Computers in Algebra and Number Theory, SIAM and AMS proceedings, p69-88, 1971.