Finding the distance between two circles in three-dimensional space

by C. A. Neff

In this paper we investigate, from an algebraic point of view, the problem of finding the distance between two circles located in $\mathbb{R}^3$. We show, by combining a theorem about solvable permutation groups and some explicit calculations with a computer algebra system*, that, in general, the distance between two circles is an algebraic function of the parameters defining them, but that this function is *not* solvable in terms of radicals. Although this result implies that one cannot find a "closed-form" solution for the distance between an arbitrary pair of circles in $\mathbb{R}^3$, we discuss how such an algebraic quantity can still be manipulated symbolically by combining standard polynomial operations with an algorithm for isolating the real roots of a polynomial in a convenient data structure for real algebraic numbers. This data structure and its operations have been implemented.

* All computer algebra calculations in this paper were performed with SCRATCHPAD [1].

1. Introduction

The problem of finding the distance between two circles in three-dimensional space, or $\mathbb{R}^3$, and the related problem of finding the intersection of two tori in $\mathbb{R}^3$ both occur surprisingly often in computer-aided geometric design systems that strive for a combination of generality and robustness. We study the torus because it is a common and esthetically pleasing shape and occurs in several important applications: in producing rounds and fillets for objects with sharp edges, in delineating the workspace of multiply jointed robots, and in the shape of cutter heads of numerically controlled machine tools. It is easy to see that the problem of intersecting two tori is related to the problem of finding the distance between two circles, because a torus T can be represented as the set of points in $\mathbb{R}^3$ that are at some fixed distance r (the minor radius) from a central circle C. Thus, two tori T_1 and T_2 will intersect if and only if the distance d between their central circles, C_1 and C_2, is less than or equal to the sum of their two minor radii, $r_1 + r_2$.

Focusing on the circle–circle distance problem, because it is a common one, we would like to have a formula or "closed-form solution" for the distance in terms of the parameters that define the problem, for at least two reasons. First, such a solution offers ease and speed of evaluation (the operations involved in a closed-form expression are common to all computers and can be computed quickly). Second, a closed-form solution allows the distance quantity to be calculated and manipulated *robustly*, that is, with any specified accuracy.

For example, take the simpler problem of finding the distance between a point p with coordinates (x_0, y_0, z_0) and a plane W defined by the equation $ax + by + cz + d = 0$, in $\mathbb{R}^3$. In this case, the parameters are x_0, y_0, z_0, a, b, c, and d. The distance between p and W is given by the expression

$$\frac{|ax_0 + by_0 + cz_0 + d|}{\sqrt{a^2 + b^2 + c^2}}.$$

Another example of a closed-form solution comes from the problem of finding the distance between two circles in $\mathbb{R}^2$. Suppose that two circles C_i $(i = 1, 2)$ have centers (x_i, y_i) and radii $r_1 \geq r_2$. We define the quantities

$$D_c = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2},$$

$$\Delta_1 = r_1 - r_2 - D_c,$$

and

$$\Delta_2 = D_c - r_1 - r_2.$$

Then the distance between C_1 and C_2 is given by

$$\text{dist}(C_1, C_2) = \begin{cases} \Delta_1 & \text{if } \Delta_1 > 0 \quad (C_2 \text{ lies inside } C_1), \\ \Delta_2 & \text{if } \Delta_2 > 0 \quad (\text{the circles are separate}), \\ 0 & \text{otherwise.} \end{cases}$$

The simple form of this expression motivates, at least partially, the search for a corresponding one in three dimensions. Although this problem is very specialized in nature, it comes up frequently enough to make worthwhile the task of deciding whether it can be solved. One may easily conjecture that there is no such expression in three dimensions, but to show this definitively requires a good deal of work and a lot of algebraic manipulation, which we do in this paper. Fortunately, the use of a computer algebra system allows us to ignore most of the tedious calculations and to concentrate instead on the interesting mathematical ideas behind the problem.

2. Group theory and algebraic solvability

We now define more precisely what we mean by a closed-form solution.

Definition 1 Let $\{c_1, \cdots, c_k\}$ be a finite set of parameters. A *closed-form expression* in $c_1, \cdots, c_k$ is

1. Any rational number α.
2. One of the parameters c_i.
3. Any expression of the form $C_1 + C_2$, $C_1 - C_2$, $C_1 \times C_2$, or C_1/C_2, where C_1 and C_2 are closed-form expressions in $c_1, \cdots, c_k$. In the case C_1/C_2, we also insist that $C_2 \neq 0$.
4. An expression of the form $\sqrt[n]{C}$, where C is a closed-form expression in $c_1, \cdots, c_k$ and n is any positive integer.

A closely related concept is the following.

Definition 2 A complex number ζ is called *algebraically solvable* if ζ can be written as a closed-form expression involving no parameters (i.e., just rational numbers).

It is easy to see that if the solution of a problem involving parameters $c_1, \cdots, c_k$ can be written as a closed-form expression in the parameters c_i, and if z is the solution of the same problem for a particular set of rational values $r_1, \cdots, r_k$ of the c_i, then z must be algebraically solvable. In the rest of this section and the next, we construct two particular circles in $\mathbb{R}^3$ and prove that the distance between them is not an algebraically solvable number, from which we conclude that the general problem of finding the distance between two circles in $\mathbb{R}^3$ does not have a closed-form solution.

In order to prove that a certain number is not algebraically solvable, we make use of several concepts from group theory and Galois theory, which we now quickly review.

Definition 3 A *group* G is a set, together with a binary operation (usually written as multiplication or addition) and a special element of $e \in G$ such that

1. $(ab)c = a(bc)$ $\quad \forall a, b, c \in G.$
2. $ea = a$ $\quad \forall a \in G.$
3. For each $a \in G$ there exists a $b \in G$ with $ba = e$. (We write $b = a^{-1}$.)

Remark It is not immediately obvious, but one can show that the conditions in Definition 3 are enough to conclude that $ae = a$ and that $ba = e \Rightarrow ab = e$ $\forall a, b \in G$.

Definition A subset $H \subset G$ is a *subgroup* of G if

1. $ab \in H$ whenever $a \in H$ and $b \in H$.
2. $a^{-1} \in H$ whenever $a \in H$.

Example The set of integers with the binary operation addition forms a group. The even integers are a subgroup.

The group of integers, with addition as the binary operation, is an example of a group with an infinite number of elements, but many important groups are finite. One of the most important families of such groups is given in the following definition.

Definition Given an ordered set of n elements $S = \{s_1, s_2, \cdots, s_n\}$, the set of permutations of these elements forms a group, usually denoted by Σ_n, with binary operation given by composition. The group Σ_n is known as the *symmetric group* on n *letters.*

A permutation $\phi \in \Sigma_n$ is called a k-cycle if there are k elements of the set S, say $t_1, \cdots, t_k$, such that $\phi(t_i) = t_{i+1}$ for $i = 1, \cdots, k-1$, and $\phi(t_k) = t_1$. A compact notation for such a permutation is $\phi = (t_1 t_2 \cdots t_k)$.

For any positive integer n, a subgroup G of Σ_n is known as a *permutation group.* Historically, the study of these groups provided much of the motivation for the general theory of finite groups; in fact, every finite group has a concrete representation as a subgroup of one of the symmetric groups. Finite groups have applications in many diverse fields, ranging from crystallography to quantum mechanics. Their application to the theory of algebraic solvability is outlined in the following sequence of definitions and lemmas.

Definition For the purposes of this paper, a *field* is a subset of the complex numbers that contains $\{0, 1\}$ and is closed under the elementary operations $+, -, \times, /$ (except for division by 0). The field of rational numbers is written as $\mathbb{Q}$.

Definition Given a set of complex numbers $\{r_1, \cdots, r_k\}$, the *field generated* by $r_1, \cdots, r_k$ is written $\mathbb{Q}(r_1, \cdots, r_k)$ and is the smallest field that contains all of the r_i.

Definition 4 An automorphism of a field K is a function from K to itself that respects all of the arithmetic operations.

Example $\mathbb{Q}(\sqrt{2})$ consists of all real numbers of the form $a + b\sqrt{2}$, where a and b are rational. The function $\phi(a + b\sqrt{2}) = a - b\sqrt{2}$ is an automorphism of this field; the function $\phi(t) = 1/t$ is not.

It is not hard to see that an automorphism of a field leaves all rational numbers fixed. Moreover, if ϕ is any automorphism of a field K, and $r \in K$ is a root of a polynomial $x^n + c_{n-1}x^{n-1} + \cdots + c_0$ with rational coefficients, then $\phi(r)$ must also be a root of this polynomial, since

$$\begin{aligned} 0 = \phi(0) &= \phi(r^n + \cdots + c_0) \\ &= \phi(r)^n + \phi(c_{n-1})\phi(r)^{n-1} + \cdots + \phi(c_0) \\ &= \phi(r)^n + c_{n-1}\phi(r)^{n-1} + \cdots + c_0. \end{aligned}$$

Thus we have the following lemma.

Lemma Let $p(x)$ be a polynomial with rational coefficients and roots $r_1, \cdots, r_n$. If $K = \mathbb{Q}(r_1, \cdots, r_n)$, then any automorphism of K induces a permutation of the roots of p.

If π_i $(i = 1, 2)$ are permutations of $r_1, \cdots, r_n$ that are induced by automorphisms ϕ_i of K, then the product permutation $\pi_1\pi_2$ is induced by the composition automorphism $\phi_1 \circ \phi_2$ $[\phi_1 \circ \phi_2(z) = \phi_1(\phi_2(z))]$, and the inverse permutation π_1^{-1} is induced by the automorphism ϕ_1^{-1}. Thus the permutations of $r_1, \cdots, r_n$ that are induced by automorphisms of K form a subgroup of Σ_n, and this leads to the following.

Definition With the notation of the above lemma, the *Galois group* of p, G_p, is the group of all permutations of the r_i that are induced by automorphisms of the field K. If $L \subseteq K$ is a subfield, the *Galois group of* p *over* L, $G_{p/L}$, is the subgroup of G_p consisting of all permutations that are induced by automorphisms that are the identity on L.

Example 5 Let $p(x)$ be the polynomial $x^3 - 7x^2 + 3x + 1$. It has three real roots, which we denote by r_1, r_2, r_3. In this case, G_p is Σ_3, the entire set of permutations of the three roots.

Example 6 Let $p(x)$ be the polynomial $x^3 - 6x^2 + 3x + 1$. Again, $p(x)$ has three real roots, which we denote by $\alpha_1, \alpha_2, \alpha_3$. This time G_p is just the three-element group consisting of the identity permutation and the two 3-cycles (r_1, r_2, r_3) and (r_1, r_3, r_2).

We see below how to deduce these two examples. Intuitively, G_p measures the nature of the set of algebraic relations among the roots of p. The more relations there are, the fewer permutations G_p will contain. In fact, there is also a necessary and sufficient condition on G_p for the roots of p to be algebraically solvable. In order to understand this condition, we need to make one last set of definitions.

Definition A subgroup H of a group G is called a *normal* subgroup of G, denoted $H \lhd G$, if $gHg^{-1} \subseteq H$ for all $g \in G$. (This is equivalent to $gHg^{-1} = H$ for all $g \in G$ and to $g^{-1}Hg = H$ for all $g \in G$.)

Example $\{e, (1\ 2\ 3), (1\ 3\ 2)\}$ is a normal subgroup of Σ_3; $\{e, (1\ 2)\}$ is a subgroup, but is not normal, since $(1\ 3)(1\ 2)(1\ 3)^{-1} = (2\ 3)$.

If H is a normal subgroup of G, then the set of all subsets of G of the form gH, where $g \in G$, forms a group with the multiplication rule $(g_1H)(g_2H) = (g_1g_2)H$, for $g_1, g_2 \in G$.

This is called the *quotient group* of G with respect to H and is written G/H.

Definition A group G is called *solvable* if there is a tower of subgroups

$$\{e\} = H_0 \lhd H_1 \lhd \cdots \lhd H_{k-1} \lhd H_k = G,$$

with the property that each quotient group H_i/H_{i-1} is a commutative group.

The fundamental theorem of Galois theory [2] is the following.

Theorem 7 Suppose that $p(x)$ is a polynomial with rational coefficients that has no nontrivial polynomial factors with rational coefficients (p is called *irreducible* over $\mathbb{Q}$). For any root r of p, r is algebraically solvable if and only if G_p is a solvable group.

In order to gather information about the Galois group of a particular polynomial, we make use of the following definition and lemma.

Definition A group G of permutations on the set $S = \{s_1, \cdots, s_k\}$ is called *transitive* if for every pair of elements s_i, s_j of S there is a $g \in G$ such that $g(s_i) = s_j$. Equivalently, G is transitive if for every $s_i \in S$ there is a $g \in G$ such that $g(s_1) = s_i$.

Lemma 8 Let $p(x)$ be a polynomial and K a field. If p is *irreducible* over K (does not factor into smaller polynomials with coefficients in K), then $G_{p/K}$ is transitive.

Example 9 (Example 5 continued) Consider again the polynomial $p(x) = x^3 - 7x^2 + 3x + 1$. If we use a computer algebra system to factor $p(x)$ over $\mathbb{Q}$, the field of rational numbers, we find that $p(x)$ is irreducible. Applying Lemma 8, with $K = \mathbb{Q}$, we see that G_p is transitive. Next we construct the field $K_1 = \mathbb{Q}(r_1)$, where r_1 is a root of $p(x)$. When we then factor $p(x)$ over K_1, we find

$$\begin{aligned} p(x) &= (x - r_1)[x^2 + (r_1 - 7)x + r_1^2 - 7r_1 + 3] \\ &= (x - r_1)p_1(x). \end{aligned}$$

Let r_2 and r_3 be the other two roots of $p(x)$—that is, the two roots of the polynomial $p_1(x)$. If we appeal to Lemma 8 again, this time with $K = K_1$ and with p_1 in place of p, we see that the Galois group of p over $\mathbb{Q}(r_1)$ is transitive on the set $\{r_2, r_3\}$. That is, G_p contains a permutation of the form (r_2, r_3). From this it is easy to conclude that G_p is all of Σ_3.

Example 10 (Example 6 continued) Now consider instead $p(x) = x^3 - 6x^2 + 3x + 1$.

If we factor $p(x)$ over $\mathbb{Q}$, we again find that $p(x)$ is irreducible. So, as before, G_p is transitive. But this time when we try to factor over the field $\mathbb{Q}(r_1)$ we get

$$p(x) = (x - r_1)(x - r_1^2 + 6r_1 - 4)(x + r_1^2 - 5r_1 - 2).$$

In this case, if r_2 and r_3 are as in the previous example, we have

$$r_2 = r_1^2 - 6r_1 + 4 = q_1(r_1),$$

$$r_3 = -r_1^2 + 5r_1 + 2 = q_2(r_1).$$

This tells us that the Galois group of p over $\mathbb{Q}(r_1)$ is trivial (consists of only the identity permutation), because any automorphism with the property that $\phi(r_1) = r_1$ must also have the property that $\phi[q(r_1)] = q(r_1)$ for any polynomial q with rational coefficients. In other words, ϕ must satisfy $\phi(r_2) = r_2$ and $\phi(r_3) = r_3$. Thus, each element $g \in G_p$ is completely determined by $g(r_1)$, and we conclude that G_p contains only the identity permutation and the two 3-cycles mentioned in Example 6.

3. The circle–circle problem

Let us construct a particular instance of the circle–circle distance problem. We choose C_1 to be a unit circle, centered at the origin and located in the xy-plane. We take C_2 to be a unit circle, centered at (1, 0, 3) and located in the plane passing through this point and perpendicular to the vector $\langle 3, 2, 1 \rangle$. By using the method of Lagrange multipliers, we find that the distance between C_1 and C_2 is the minimum nonnegative real value of $\sqrt{D}$, where D is a value for which there is a solution to the following system of equations:

$$u^2 + v^2 - 1 = 0, \tag{1}$$

$$(x - 1)^2 + y^2 + (z - 3)^2 - 1 = 0, \tag{2}$$

$$3(x - 1) + 2y + (z - 3) = 0, \tag{3}$$

$$\mu_2(x - 1) + 3\mu_3 - (x - u) = 0, \tag{4}$$

$$\mu_2 y + 2\mu_3 - (y - v) = 0, \tag{5}$$

$$\mu_2(z - 3) + \mu_3 - z = 0, \tag{6}$$

$$\mu_1 u - (x - u) = 0, \tag{7}$$

$$\mu_1 v - (y - v) = 0, \tag{8}$$

$$(x - u)^2 + (y - v)^2 + z^2 - D = 0. \tag{9}$$

As noted in the previous section, if there is a closed-form solution to the general circle–circle distance problem in $\mathbb{R}^3$, then $\sqrt{D}$ must be algebraically solvable. It follows immediately from Definitions 1 and 2 that this is equivalent to the condition that D be algebraically solvable. We shall now see that it is not.

We can eliminate all variables except D by doing a Gröbner basis calculation [3, 4], a method of eliminating variables from a system of equations, by using a computer algebra system. The result is a polynomial of degree 8 in D alone, with rational coefficients:

$$p(D) = D^8 + c_7 D^7 + \cdots + c_1 D + c_0. \tag{10}$$

Since the coefficients have large numerators and denominators, and since their exact values are not crucial to what follows, we do not list them here.

We now prove that the Galois group of $p(D)$ is not solvable, by using the following lemma and theorem in combination with some explicit computer algebra calculations.

Lemma 11 A subgroup of a solvable group is solvable.

Proof See [5, 6].

Theorem 12 If G is a transitive permutation group on a set S of q elements where q is a *prime* integer and G is solvable, then the only element of G that leaves two elements fixed is the identity permutation.

Before we prove this, let us see how it applies to the problem we are considering.

Let $p(D)$ be the polynomial in (10), and suppose that G_p is solvable. Pick a root ρ_1 of $p(D)$ and consider the Galois group G_1 of p of $\mathbb{Q}(\rho_1)$. By definition, this is a subgroup of G_p. Thus, by Lemma 11, since we are assuming that G_p is solvable, G_1 must also be solvable.

Now G_1 is a permutation group on a seven-element set $\{\rho_2, \cdots, \rho_8\}$. We can factor $p(D)$ over $\mathbb{Q}(\rho_1)$, and we obtain $p(D) = (D - \rho_1)p_7(D)$, where p_7 is a polynomial of degree 7 with coefficients in the field $K_1 = \mathbb{Q}(\rho_1)$, which is *irreducible* over K_1. Thus, Lemma 8 tells us that G_1 is transitive on $\{\rho_2, \cdots, \rho_8\}$.

Next we factor p_7 over the field $K_2 = \mathbb{Q}(\rho_1, \rho_2)$, obtaining $p_7(D) = (D - \rho_2)p_6(D)$, where p_6 is a polynomial of degree 6, which is *irreducible* over K_2.

If the only element of G_1 that fixes the two elements ρ_2, ρ_3 is the identity, then $p_6(D)$ must split completely into linear factors over the field $\mathbb{Q}(\rho_1, \rho_2, \rho_3)$. Otherwise, Lemma 8 would imply that the elements of G_1 that fix both ρ_2 and ρ_3 are actually transitive on some nontrivial subset of the elements $\rho_4, \cdots, \rho_8$. However, when we factor $p_6(D)$ (using a computer algebra system), we find that this is not the case; in fact, $p_6(D)$ has only one linear factor. Thus, by Theorem 12, G_1 cannot be a solvable group. But, by Lemma 11, this contradicts our assumption that G_p is solvable. Hence, by Theorem 7, no root of $p(D)$ is algebraically solvable. Thus, there is no closed-form solution to the general circle–circle distance problem in $\mathbb{R}^3$.

To complete this section we now give the proof of Theorem 12.

Proof of Theorem 12 Let H be a normal subgroup of G. We define our equivalence relation $\sim$ on the elements of S as follows:

$$s_i \sim s_j \Leftrightarrow \sigma(s_i) = s_j \quad \text{for some } \sigma \in H. \tag{11}$$

The equivalence relation $\sim$ splits S into *disjoint* equivalence classes. Let $\mathcal{C}_1 = \{s_1, \cdots, s_k\}$ and $\mathcal{C}_2 = \{s_i, \cdots, s_j\}$ be two such classes. Since G is transitive, we can choose $\sigma_i \in G$ with the property that $\sigma_i(s_1) = s_i$.

Consider the set $\sigma_i(\mathcal{C}_1) = \{\sigma_i(s_1), \cdots, \sigma_i(s_k)\}$, and let $\sigma_i(s_l) \in \sigma_i(\mathcal{C}_1)$. Then there is a $\sigma \in H$ such that $\sigma(s_1) = s_l$, and we have

$$\sigma_i(\sigma\{\sigma_i^{-1}[\sigma_i(s_1)]\}) = \sigma_i[\sigma(s_1)] = \sigma_i(s_l). \tag{12}$$

Thus $\sigma_i(\mathcal{C}_1)$ is exactly the equivalence class of $\sim$ that contains s_i. Since s_i was arbitrary, all equivalence classes contain the same number of elements. But, since q is prime, this number must be either 1 (q classes and $H = \{e\}$) or q (one class and H is also transitive on S).

Let

$$\{e\} = G_{k+1} \lhd G_k \lhd G_{k-1} \lhd \cdots \lhd G_1 \lhd G_0 = G \tag{13}$$

be a solvable series for G. Since every commutative group has a normal, cyclic subgroup, we may assume that the group G_k is generated by the q-cycle

$$\omega = (s_1 s_2 \cdots s_{q-1} s_q). \tag{14}$$

Suppose $\gamma \in G_{k-1}$. We know that $\gamma\omega\gamma^{-1} \in G_k$, so $\gamma\omega\gamma^{-1} = \omega^m$ for some m in $1, 2, \cdots, q-1$. In fact,

$$m = 1 \quad \text{if and only if} \quad \gamma \in G_k, \tag{15}$$

since the only permutations in Σ_q that commute with a q-cycle are the powers of that q-cycle.

If we suppose $\gamma(s_q) = s_j$, then

$$\gamma(s_1) = \gamma[\omega(s_q)] = \gamma\omega\gamma^{-1}[\gamma(s_q)] = \omega^m(s_j) = s_\nu, \tag{16}$$

where $\nu = (j + m) \bmod q$.

In general, $\gamma(s_i) = s_{\nu(i)}$, where $\nu(i) = (j + mi) \bmod q$. Thus, either $\gamma \in G_k$, or γ fixes exactly one element.

Now, suppose that $\theta \in G_{k-2}$. Since $G_{k-1} \lhd G_{k-2}$, and since $\omega \in G_k \subset G_{k-1}$, we know that $\theta\omega\theta^{-1} \in G_{k-1}$. But it is easy to see from Equation (14) that $\theta\omega\theta^{-1}$ does not fix any elements. By the previous paragraph, this can happen only if $\theta\omega\theta^{-1} \in G_k$, that is, $G_k \lhd G_{k-2}$. We can now simply replace G_{k-1} with G_{k-2} in the previous discussion, and the proof can be completed by induction.

4. Computing with real algebraic numbers

We can still capture some of the advantages of a closed-form solution by extending the idea of taking an nth root to the idea of taking real roots of arbitrary polynomials. To do this, we represent a real algebraic number α as a pair. The first element of the pair is a polynomial with rational coefficients, of which α is a root. We call this the defining polynomial for α. The second element of the pair is a rational *isolating interval* for α—that is, an interval of the real line that contains only one root of the defining polynomial for α, namely α itself.

Example $\sqrt{3}$ can be represented as the pair $(x^2 - 3, [1, 2])$.

The elementary operations $+, -, \times, /$ are actually much easier to perform with this representation than

with a representation that uses "towers" of radicals. The operations $+, -, \times$ are performed on real algebraic numbers almost as if they were polynomials. If α is defined by $(p(x), [a, b])$, $\beta = q_1(\alpha)$, and $\gamma = q_2(\alpha)$, then $\beta \cdot \gamma = q(\alpha)$, where

$$q(x) = q_1(x) \cdot q_2(x) \mod p(x). \tag{17}$$

Example 13 Suppose α is defined as $(x^3 - 6x^2 + 3x + 1, [0, 4])$ (Example 6). If $\beta = \alpha^2 + \alpha + 1$ and $\gamma = \alpha + 2$, then $\beta\gamma = \alpha^3 + 3\alpha^2 + 3\alpha + 2 = 9\alpha^2 + 1$.

Division is implemented using the Euclidean algorithm; $r(\alpha) = 1/q(\alpha)$ if and only if there is a polynomial $A(x)$ such that

$$q(x)r(x) + A(x)p(x) = 1. \tag{18}$$

Example Using α defined above, we have

$$1/\alpha = -\alpha^2 + 6\alpha - 3, \tag{19}$$

$$1/(\alpha^2 - 1) = (1/71)(51\alpha^2 - 19\alpha - 41). \tag{20}$$

In order to take full advantage of this notion of a real algebraic number, however, one must be able to build them in "towers" and to use them in geometric calculations. Both of these require that numbers be *ordered*. For example, if we take the β and γ of Example 13, it is not easy to tell whether $\beta < \gamma$. A relatively simple algorithm for doing this does exist, though, and has been implemented recently.

Example Suppose we are given the equations of two tori T_1 and T_2 and want to know if they intersect. The equations for their central circles, C_1 and C_2, are easily obtained from the equations for T_1 and T_2, so we can find the polynomial $p(D)$ in Section 3. By doing successive binary subdivision, we can find a rational number r such that $p(D)$ has exactly one distinct root in the interval $[0, r]$. We now define D_1 symbolically by $D_1 = (p(D), [0, r])$. Let r_1 and r_2 be the radii of C_1 and C_2 respectively, and let $R_1 = r_1^2$, $R_2 = r_2^2$. Quantities R_1 and R_2 are easily obtained from the equations for T_1 and T_2, so we can define r_1 and r_2 symbolically as the quantities

$$r_1 = (r^2 - R_1, [0, R_1]),$$

$$r_2 = (r^2 - R_2, [0, R_2]).$$

Using the fact that we can order real algebraic numbers represented in this way, we can now simply determine whether T_1 and T_2 intersect by determining whether the inequality $D_1 \le (r_1 + r_2)^2$ holds. Or, using the fact that we can build real algebraic numbers in towers, we can define the distance between the two circles C_1 and C_2 as the quantity $d_1 = (d^2 - D_1, [0, D_1])$, and then determine whether T_1 and T_2 intersect, even more directly, by determining whether $d_1 \le r_1 + r_2$.

The point is that, from the point of view of the person doing the calculation, working symbolically with a root of the complicated polynomial $p(D)$ is no more difficult than working symbolically with a root of the simple polynomial $x^2 - 3$, namely $\sqrt{3}$. More emphatically, in the context of symbolic calculations (in geometric applications and elsewhere) the question of whether a particular real algebraic number can be expressed in closed form becomes unimportant.

Acknowledgment

This problem was originally posed by Michael O'Connor.

References

1. R. D. Jenks, R. S. Sutor, and S. M. Watt, "Scratchpad II: An Abstract Datatype System for Mathematical Computation," *Research Report RC-12327*, IBM Thomas J. Watson Research Center, Yorktown Heights, NY, 1986.
2. I. Kaplansky, *Fields and Rings*, second edition, University of Chicago Press, Chicago, 1972.
3. B. Buchberger, "A Theoretical Basis for the Reduction of Polynomials to Canonical Forms," *ACM SIGSAM Bull.* **39,** 19–29 (1976).
4. B. Buchberger, "Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory," *Multidimensional System Theory: Progress, Directions, and Open Problems in Multidimensional Systems*, N. K. Bose, Ed., D. Reidel, Boston, 1985, Ch. 6.
5. I. N. Herstein, *Topics in Algebra*, Blaisdell, New York, 1953.
6. J. J. Rotman, *The Theory of Groups*, second edition, Allyn and Bacon, Inc., Boston, 1973.

Received December 22, 1989; accepted for publication July 30, 1990

C. Andrew Neff *IBM Thomas J. Watson Research Center, P.O. Box 218, Yorktown Heights, New York 10598.* Dr. Neff received a B.S. degree from the University of Chicago in 1981 and a Ph.D. in mathematics from Princeton University in 1986. Since that time he has been a Research Staff Member at the IBM Thomas J. Watson Research Center, joining the Manufacturing Research Department in 1987. His research interests include algebraic and numerical methods in geometric computation and, more recently, simulation of IC fabrication processes.