Simple unit vectors orthogonal to a given vector

by Michael A. O'Connor
Graziano Gentili

In geometrical computations it is often necessary to find two unit vectors such that they and a given vector form an orthogonal basis. Computationally simple forms for the two unit vectors are clearly useful. We show that they cannot always be chosen to have rational coordinates, but that in general the simplest possible vectors can be chosen to involve only one square root. We develop number-theoretic criteria for the existence of a rational vector and an effective algorithm for calculation of one if it exists. We also discuss storage and time requirements of the algorithm.

1. Introduction

In calculations in descriptive geometry a seemingly innocuous subproblem often occurs: Given a nonzero vector $\mathbf{v}$ in $\mathbb{R}^3$, find two vectors $\mathbf{u}$ and $\mathbf{u}'$, such that $\mathbf{u}$ and $\mathbf{u}'$ are unit vectors and $\mathbf{v}$, $\mathbf{u}$, and $\mathbf{u}'$ are mutually orthogonal. For example, if one must intersect two quadric surfaces, by using Levin's method [1] the problem is frequently reduced to intersecting a cone or cylinder with one of the original surfaces. To accomplish this, one treats the cone or cylinder as a ruled surface parameterized by a conic on the surface and in a plane orthogonal to the axis of the cone or cylinder.

The conic is then usually parameterized in terms of two vectors $\mathbf{u}$ and $\mathbf{u}'$ as above. In graphics the same problem of parameterizing a conic arises in the production of a wire frame drawing of a sphere, cylinder, cone, or torus. In geometrical modeling a standard feature of many systems is the ability to design in a plane in 3-space by using a local two-dimensional coordinate system, which again reduces to choosing $\mathbf{u}$ and $\mathbf{u}'$.

We previously described the problem of finding $\mathbf{u}$ and $\mathbf{u}'$ as seemingly innocuous. In fact, if we impose no further constraints, it is completely innocuous. For if we choose $\mathbf{w}$ to be any vector not parallel to $\mathbf{v}$ [at least one of $\mathbf{w} = {}^t(1, 0, 0)$ or $\mathbf{w} = {}^t(0, 0, 1)$ will do], then

$$\mathbf{u} = \frac{\mathbf{v} \times \mathbf{w}}{\|\mathbf{v} \times \mathbf{w}\|} = \frac{\mathbf{v} \times \mathbf{w}}{\|\mathbf{v}\|\|\mathbf{w}\| \sqrt{1 - \left(\frac{{}^t\mathbf{v}\mathbf{w}}{\|\mathbf{v}\|\|\mathbf{w}\|}\right)^2}}$$

$$= \frac{\mathbf{v} \times \mathbf{w}}{\sqrt{\|\mathbf{v}\|^2\|\mathbf{w}\|^2 - ({}^t\mathbf{v}\mathbf{w})^2}},$$

$$\mathbf{u}' = \frac{(\mathbf{v} \times \mathbf{w}) \times \mathbf{v}}{\|\mathbf{v} \times \mathbf{w}\|\|\mathbf{v}\|} = \frac{(\mathbf{v} \times \mathbf{w}) \times \mathbf{v}}{\|\mathbf{v}\| \sqrt{\|\mathbf{v}\|^2\|\mathbf{w}\|^2 - ({}^t\mathbf{v}\mathbf{w})^2}} \quad (1)$$

clearly satisfy all the requirements on $\mathbf{u}$ and $\mathbf{u}'$. However, if we add the constraint that we wish to use these vectors in computer calculations, the problem becomes much more interesting, since all vectors are not created equal. In a standard computational environment, where irrationalities can only be approximated, the two square roots in $\mathbf{u}$ and $\mathbf{u}'$ imply a necessary loss of accuracy and require time to approximate them. Even if we assume access to a symbol manipulator, since the complexity tends to be exponential in

the number of symbols, the two irrationalities come at a price. In symbol manipulation storage size and the length of calculation increase with the size of the integers involved, so that vectors with few rational numbers with small numerators and denominators are preferable. Such vectors can also increase the precision of floating-point calculations. With these observations in mind we will say that a vector $\mathbf{u}$ is simpler than a vector $\mathbf{v}$ in these three cases: first, if $\mathbf{u}$ involves fewer algebraically independent square roots than $\mathbf{v}$; second, if $\mathbf{u}$ and $\mathbf{v}$ involve the same number of algebraically independent square roots, but $\mathbf{u}$ has fewer occurrences of them; and third, if $\mathbf{u}$ and $\mathbf{v}$ involve the same number of algebraically independent square roots and occurrences of them, but it requires less storage to represent all of the rational numbers occurring in $\mathbf{u}$ than in $\mathbf{v}$. (A more precise definition can be found in the appendix of this paper.) Most often in applications $\mathbf{v}$ itself has rational coordinates, that is, $\mathbf{v} \in \mathbb{Q}^3$. Thus we are led to the main question of this article: How simple can we choose $\mathbf{u}$ and $\mathbf{u}'$ when $\mathbf{v} \in \mathbb{Q}^3$?

Simplest would be when we can find $\mathbf{u}$ and $\mathbf{u}'$ with rational coordinates. For $\mathbf{v} = {}^t(n_1, n_2, n_3) \in \mathbb{Z}^3$, that is, when $\mathbf{v}$ has integer coordinates, we obtain the Diophantine equation

$$(n_1^2 + n_2^2)x^2 - (n_1^2 + n_2^2 + n_3^2)y^2 - z^2 = 0 \tag{2}$$

and show that its solvability is a necessary and sufficient condition for the existence of a rational $\mathbf{u}$. Along the way we obtain several simple equations for possible choices of $\mathbf{u}$ and $\mathbf{u}'$, one of which shows that in general we can choose $\mathbf{u}$ and $\mathbf{u}'$ involving only one square root, $\|\mathbf{v}\|$, thus reducing the complexity of the obvious initial choice (Section 2). In order to obtain more explicit conditions on the existence of a rational $\mathbf{u}$ [2], we require several results from elementary number theory, which in the interest of making the paper self-contained we list in Section 3. Next we present several examples, one of which shows that in general the simplest unit vectors that always exist are the previously mentioned ones involving only $\|\mathbf{v}\|$. Now by utilizing a closer study of Equation (2) we obtain a number-theoretic condition on $\|\mathbf{v}\|^2$ which is a necessary and sufficient condition for the existence of a rational $\mathbf{u}$. Then we present a solution for $\mathbf{u}$ which is determined by a solution to (2) that requires only a decomposition of $\|\mathbf{v}\|^2$. We close the section with several applications to questions of rational rigid motions between lines and planes. Section 5 discusses requirements of the algorithm of the previous section in terms of assumed programming facilities, space, and time requirements, and the paper ends by recapitulating the main results and discussing several possible extensions.

2. Preliminary results

In the following $\mathbf{v} = {}^t(v_1, v_2, v_3)$ is a nonzero vector in $\mathbb{Q}^3$, and $\mathbf{u}$ and $\mathbf{u}'$ are a pair of vectors in $\mathbb{R}^3$ such that ${}^t\mathbf{u}\mathbf{v} = {}^t\mathbf{u}'\mathbf{v} = {}^t\mathbf{u}\mathbf{u}' = 0$ and $\|\mathbf{u}\| = \|\mathbf{u}'\| = 1$.

The simplest case would obviously have $\mathbf{u}$ and $\mathbf{u}'$ expressed in rational coordinates, so we begin with this. The following is no more than the recognition that the calculation in (1) imposes constraints.

Proposition 1
Assume that $\mathbf{u} \in \mathbb{Q}^3$ exists. $\mathbf{u}' \in \mathbb{Q}^3$ exists if and only if $\|\mathbf{v}\| \in \mathbb{Q}$.

Proof

$$\mathbf{u}' = \pm \frac{\mathbf{v} \times \mathbf{u}}{\|\mathbf{v} \times \mathbf{u}\|} = \pm \frac{\mathbf{v} \times \mathbf{u}}{\|\mathbf{v}\|}. \quad \square$$

We could now search for a $\mathbf{u} \in \mathbb{Q}^3$, given that $\|\mathbf{v}\| \in \mathbb{Q}$, but the trivial calculation in the proof shows that if $\mathbf{u} \in \mathbb{Q}^3$ exists, we can find $\mathbf{u}' \in \|\mathbf{v}\|\,\mathbb{Q}^3 = \{\|\mathbf{v}\|\mathbf{w} : \mathbf{w} \in \mathbb{Q}^3\}$ in any case. Since this is simpler than (1), we instead investigate when $\mathbf{u} \in \mathbb{Q}^3$ can exist in general.

Clearly, if $v_1 = 0$, then ${}^t(1, 0, 0)$ is a trivial solution to the problem, so we would lose little by assuming that $v_1 \neq 0$. For the ease it affords in stating subsequent results and formulas, we hereafter make this assumption. Multiplying $\mathbf{v}$ by any nonzero integer cannot affect the existence of $\mathbf{u}$, so without loss of generality we assume hereafter that $\mathbf{v} = {}^t(n_1, n_2, n_3) \in \mathbb{Z}^3$. With these reductions we are ready to state the following proposition.

Proposition 2
Let $\mathbf{v} = {}^t(n_1, n_2, n_3) \in \mathbb{Z}^3$. Set $p = n_1^2 + n_2^2$, and $q = n_1^2 + n_2^2 + n_3^2$. A vector $\mathbf{u} \in \mathbb{Q}^3$ exists if and only if the Diophantine equation

$$px^2 - qy^2 - z^2 = 0 \tag{3}$$

has a solution $(x_0, y_0, z_0) \in \mathbb{Z}^3 \setminus {}^t(0, 0, 0)$.

Proof $\mathbf{u} = {}^t(u_1, u_2, u_3)$ by definition is orthogonal to $\mathbf{v}$, that is,

$$u_1 = -\frac{n_2u_2 + n_3u_3}{n_1}, \tag{4}$$

and is a unit vector, that is,

$$u_1^2 + u_2^2 + u_3^2 = 1.$$

By substituting the first equation in the second,

$$n_2^2u_2^2 + 2n_2n_3u_2u_3 + n_3^2u_3^2 + n_1^2u_2^2 + n_1^2u_3^2 = n_1^2,$$

and then

$$(n_1^2 + n_2^2)u_2^2 + 2n_2n_3u_3u_2 + ((n_1^2 + n_3^2)u_3^2 - n_1^2) = 0,$$

and solving for u_2,

$$u_2 = \frac{-n_2n_3u_3 \pm \sqrt{(n_2n_3u_3)^2 - (n_1^2 + n_2^2)\,((n_1^2 + n_3^2)u_3^2 - n_1^2)}}{n_1^2 + n_2^2}$$

$$= \frac{-n_2n_3u_3 + n_1\sqrt{(n_1^2 + n_2^2) - (n_1^2 + n_2^2 + n_3^2)u_3^2}}{n_1^2 + n_2^2}. \tag{5}$$

Hence, if $u_3 \in \mathbb{Q}$, then $u_2 \in \mathbb{Q}$, if and only if $p - qu_3^2 = r^2$ for some $r \in \mathbb{Q}$. Multiplication by the denominators squared of u_3 and r establishes the claim. □

Corollary 1
If (x_0, y_0, z_0) is a nontrivial solution of $px^2 - qy^2 - z^2 = 0$, then

$$\mathbf{u} = {}^t\left(-\frac{n_1 n_3 y_0 \pm n_2 z_0}{(n_1^2 + n_2^2)x_0}, \quad \frac{-n_2 n_3 y_0 \pm n_1 z_0}{(n_1^2 + n_2^2)x_0}, \quad \frac{y_0}{x_0}\right)$$

solves ${}^t\mathbf{u}\mathbf{v} = 0$ and $\|\mathbf{u}\| = 1$.

Proof Proposition 2, substitution, and simplification suffice. □

As a simple corollary we can now complete discussion of the existence of rational $\mathbf{u}$ and $\mathbf{u}'$.

Corollary 2
Vectors $\mathbf{u}$ and $\mathbf{u}' \in \mathbb{Q}^3$ exist if and only if $\|\mathbf{v}\| \in \mathbb{Q}$.

Proof Necessity is implied by Proposition 1. Since $\sqrt{q} = \|\mathbf{v}\| \in \mathbb{Q}$ and $p1^2 - q(n_1/\sqrt{q})^2 - n_2^2 = 0$, then $\mathbf{u} \in \mathbb{Q}^3$ exists, and Proposition 1 implies the existence of $\mathbf{u}' \in \mathbb{Q}^3$. □

When Corollary 1 is used, the solution in the proof yields

$$\mathbf{u} = \frac{n_1}{p\sqrt{q}}\,{}^t(-n_1 n_3, -n_2 n_3, p) \pm \frac{n_2}{p}\,{}^t(n_2, -n_1, 0),$$

$$\mathbf{u}' = \frac{n_1}{p}\,{}^t(n_2, -n_1, 0) \mp \frac{n_2}{p\sqrt{q}}\,{}^t(-n_1 n_3, -n_2 n_3, p). \tag{6}$$

Clearly, if $\sqrt{q} \in \mathbb{Q}$, $\mathbf{u}$ and $\mathbf{u}'$ are rational, but even if $\sqrt{q} \notin \mathbb{Q}$, we have found a simpler expression than (1). If we extend the field $\mathbb{Q}$ to contain $\|\mathbf{v}\|$, and denote it as $\mathbb{Q}(\|\mathbf{v}\|)$, then we can formalize this as the following corollary.

Corollary 3
Vectors $\mathbf{u}$ and $\mathbf{u}'$ always exist in $\mathbb{Q}(\|\mathbf{v}\|)^3$.

Proof See (6). □

The discussion following Proposition 1 and the last two corollaries limit our search to investigating when $\mathbf{u} \in \mathbb{Q}^3$ exists, so that $\mathbf{u}' \in \|\mathbf{v}\|\,\mathbb{Q}^3$, that is, when (3) has a solution. Two obvious special cases are when $\sqrt{p} \in \mathbb{Q}$, so that $(1, 0, \sqrt{p})$ solves (3) and yields

$$\mathbf{u} = \frac{1}{\sqrt{p}}\,{}^t(n_2, -n_1, 0), \qquad \mathbf{u}' = \frac{1}{\sqrt{pq}}\,{}^t(-n_1 n_3, -n_2 n_3, p), \tag{7}$$

which corresponds to choosing $\mathbf{w} = {}^t(0, 0, 1)$ in (1), or when $\sqrt{p/q} \in \mathbb{Q}$, so that $(1, \sqrt{p/q}, 0)$ solves (3) and yields

$$\mathbf{u} = \frac{1}{\sqrt{pq}}\,{}^t(-n_1 n_3, -n_2 n_3, p), \qquad \mathbf{u}' = \frac{1}{\sqrt{p}}\,{}^t(n_2, -n_1, 0).$$

Thus solutions exist when $\sqrt{q} \notin \mathbb{Q}$. To show that (6) is often the simplest possible choice, that is, (3) may not have a solution, and to determine precise conditions for the solvability of (3), we require certain number-theoretic results of the next section.

3. A little number theory

We make use of several results from elementary number theory which can be found in most introductory texts, but to keep this article self-contained we list these results with references in this section.

The first result, due to Legendre, and the second, due to Holzer [3], can be found in pages 46 and 47 of [4].

Definition 1
For integers m and n, n is said to be a quadratic residue of m if an integer solution of $x^2 = n \bmod(m)$ exists, and a quadratic nonresidue otherwise. □

Result 1
If integers a, b, c are square-free, pairwise relatively prime, and not all of the same sign, then $ax^2 + by^2 + cz^2 = 0$ has nontrivial integer solutions, if and only if $-bc$ is a quadratic residue of each prime factor of a, $-ac$ is a quadratic residue of each prime factor of b, and $-ab$ is a quadratic residue of each prime factor of c. □

Result 2
If $ax^2 + by^2 + cz^2 = 0$ has a nontrivial integer solution for square-free and pairwise relatively prime integers a, b, c, then it has a nontrivial integer solution satisfying $|x| \le \sqrt{|bc|}$, $|y| \le \sqrt{|ac|}$, and $|z| \le \sqrt{|ab|}$, with equality occurring only if two of a, b, and c equal ± 1. □

All of the following results can be found in [5]. The first group is the body of Part One, Chapter VI, and the last result that of Part Three, Chapter III. In order to clearly phrase this first group, we define a limited version of the Legendre symbol that will suffice for our purposes and then present the results as facts about the symbol.

Definition 2
If p is an odd prime and p is not a divisor of n, define the Legendre symbol, $\left(\frac{n}{p}\right)$, as

$$\left(\frac{n}{p}\right) = \begin{cases} 1 \text{ if } n \text{ is a quadratic residue of } p, \\ -1 \text{ if } n \text{ is a quadratic nonresidue of } p. \end{cases}$$

Thus, by the definition of a quadratic residue, the Legendre symbol is ± 1, depending on whether $x^2 = n \bmod(p)$ can be solved. A short study shows that the positive integers less than p form a cyclic group under multiplication mod(p), and that the Legendre symbol is in fact a group homomorphism from this group to the group ± 1. These two observations in fact prove most of the following results.

Result 3
If p and p' are odd primes and p does not divide integers n, a, or b, then

$$\left(\frac{n+kp}{p}\right) = \left(\frac{n}{p}\right),$$

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right),$$

$$\left(\frac{a^2}{p}\right) = 1,$$

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 \text{ if } p = 1 \bmod(4), \\ -1 \text{ if } p = 3 \bmod(4), \end{cases}$$

$$\left(\frac{2}{p}\right) = \begin{cases} 1 \text{ if } p = \pm 1 \bmod(8), \\ -1 \text{ if } p = \pm 3 \bmod(8), \end{cases}$$

$$\left(\frac{p'}{p}\right) = \begin{cases} \left(\frac{p}{p'}\right) \text{ if either } p \text{ or } p' = 1 \bmod(4), \\ -\left(\frac{p}{p'}\right) \text{ if both } p \text{ and } p' = 3 \bmod(4), \end{cases}$$

(quadratic reciprocity). □

The final result we require deals with the possibility of decomposing a number in a sum of two squares.

Result 4

For any integer n, there exist integers a and b such that $n = a^2 + b^2$, if and only if

$$n = 2^{\alpha} m^2 \prod_{i=1}^{j} p_i,$$

with p_i's being distinct primes equal to 1 mod(4), m an integer, and $\alpha = 0$ or 1. □

4. The main results

Integers p and q of the Diophantine equation (3) in general do not satisfy the hypothesis of Result 1, but we can easily produce an equivalent equation that does. Let $p = ta^2r$ and $q = tb^2s$ where r, s, and t are square-free and pairwise relatively prime. Then the solvability in nontrivial integers of

$$px^2 - qy^2 - z^2 = rt(ax)^2 - st(by^2) - z^2 = 0 \tag{8}$$

clearly implies that of

$$rtu^2 - stv^2 - z^2 = 0 \tag{9}$$

if we define $u = ax$ and $v = by$, and the solvability of (9) upon multiplication by a^2b^2 clearly implies the solvability of (8). If (9) is solvable, then z must equal tw, since the other two terms are divisible by t, which upon dividing by t shows the equivalence of the solvability of

$$ru^2 - sv^2 - tw^2 = 0. \tag{10}$$

This equation satisfies the hypothesis of Result 1. Working backwards, one finds that if

$$ru^2 - sv^2 - tw^2 = 0, \tag{11}$$

then

$$p(bu)^2 - q(au)^2 - (abtw)^2 = 0. \tag{12}$$

We now consider several examples.

Example 1

If $\mathbf{v} = (1, 1, 1)$, then $\mathbf{u} \in \mathbb{Q}^3$ exists, if and only if $2x^2 - 3y^2 - z^2 = 0$ is solvable in nontrivial integers. Since $\left(\frac{2}{3}\right) = -1$ by Result 3, then no solution exists by Result 1. Thus no $\mathbf{u} \in \mathbb{Q}^3$ exists. This example implies that in general radicals may be required, so that (6) is the simplest choice for $\mathbf{u}$. □

Example 2

If $\mathbf{v} = (1, 2, 6)$, then $\mathbf{u} \in \mathbb{Q}^3$ exists, if and only if $5x^2 - 41y^2 - z^2 = 0$ is solvable in nontrivial integers. Since $\left(\frac{5}{41}\right) = \left(\frac{41}{5}\right) = \left(\frac{1}{5}\right) = 1$ and $\left(\frac{-41}{5}\right) = \left(\frac{-1}{5}\right) = 1$ by Result 3, then by Result 1 a solution exists. Using Result 2 by trial and error, one finds that $(3, 1, 2)$ solves the equation, and so $\mathbf{u} = 1/3\ {}^t(-2, -2, 1)$ or $\mathbf{u} = 1/15\ {}^t(-2, -14, 5)$ by Corollary 1. □

Example 3

If $\mathbf{v} = (3, 9, 2)$, then $\mathbf{u} \in \mathbb{Q}^3$ exists, if and only if $90x^2 - 94y^2 - z^2 = 0$ is solvable in nontrivial integers. Since $90 = 3^2 \cdot 2 \cdot 5$ and $94 = 2 \cdot 47$, then by the reductions described earlier the solvability of this equation is equivalent to that of $5x^2 - 47y^2 - 2z^2 = 0$. Since by Result 3 $\left(\frac{10}{47}\right) = \left(\frac{2}{47}\right)\left(\frac{5}{47}\right) = 1 \cdot \left(\frac{2}{5}\right) = -1$, no solution exists by Result 1. □

Since $\sqrt{p} \notin \mathbb{Q}$, $\sqrt{q} \notin \mathbb{Q}$, and $\sqrt{p/q} \notin \mathbb{Q}$ in Example 2, we see that there exist vectors with rational $\mathbf{u}$ which possess no obvious properties for sufficiency and in particular are not among the special cases of Section 2. We use the following lemma in the proof of a proposition yielding an explicit and necessary condition for the existence of $\mathbf{u} \in \mathbb{Q}^3$.

Lemma 1

If p and q are integers that can be written as the sum of squares of two integers, then $px^2 - qy^2 - z^2 = 0$ has a nontrivial integral solution, if and only if one exists for $qx^2 - py^2 - z^2 = 0$.

Proof Result 4 allows us to factor p and q as $p = 2^{\alpha'} a^2 \prod_{i=1}^{j} p_i'$ and $q = 2^{\beta'} b^2 \prod_{i=1}^{k'} q_i'$ where α', a, p_i', β', b, and q_i' are as in Result 4. If we define $t = \gcd(2^{\alpha'} \prod_{i=1}^{j'} p_i', 2^{\beta'} \prod_{i=1}^{k'} q_i')$ then we can further factor p and q as $p = t2^{\alpha} a^2 \prod_{i=1}^{j} p_i$ and $q = t2^{\beta} b^2 \prod_{i=1}^{k} q_i$, where α and β are equal to 0 or 1, but not both 1, and $\{p_i\}_{i=1}^{j} \subset \{p_i'\}_{i=1}^{j'}$ and $\{q_i\}_{i=1}^{k} \subset \{q_i'\}_{i=1}^{k'}$. For simplicity we write $r = 2^{\alpha} \prod_{i=1}^{j} p_i$ and $s = 2^{\beta} \prod_{i=1}^{k} q_i$. Now, by the discussion at the beginning of the section, the solvability in nontrivial integers of

$$rx^2 - sy^2 - tz^2 = 0 \tag{13}$$

is equivalent to that of (3), and this equation satisfies the assumptions of Result 1. By Result 1 (13) is solvable in

nontrivial integers, if and only if $-st$ is a quadratic residue of 2^{α}, $-st$ is a quadratic residue of p_i for $1 \le i \le j$, rt is a quadratic residue of 2^{β}, rt is a quadratic residue of q_i for $1 \le i \le k$, and rs is a quadratic residue of t. By Result 3, since each p_i and $q_i = 1 \bmod(4)$, and since any integer is a quadratic residue of 2, these statements about quadratic residues are true if we change the signs of st and $-rt$; that is, st is a quadratic residue of 2^{α}, st is a quadratic residue of p_i for $1 \le i \le j$, $-rt$ is a quadratic residue of 2^{β}, $-rt$ is a quadratic residue of q_i for $1 \le i \le k$. Now by Result 1 again, these statements are true if and only if $-rx^2 + sy^2 - tz^2 = 0$ is solvable in nontrivial integers. But the solvability of this equation is equivalent to that of $-px^2 + qy^2 - z^2 = 0$ by the reductions at the beginning of the proof [6]. □

Theorem 1
$\mathbf{u} \in \mathbb{Q}^3$ exists if and only if $\|\mathbf{v}\|^2 = m^2 + n^2$ for some integers m and n.

Proof *Necessity.* Since $\|\mathbf{u}\| = 1$, then by Corollary 2 there exist $\mathbf{w}$ and $\mathbf{w}'$ in $\mathbb{Q}^3$ with $\|\mathbf{w}\| = \|\mathbf{w}'\| = 1$ and ${}^t\mathbf{w}\mathbf{u} = {}^t\mathbf{w}'\mathbf{u} = {}^t\mathbf{w}\mathbf{w}' = 0$. $\mathbf{v}$ is orthogonal to $\mathbf{u}$, and so belongs to the span of $\mathbf{w}$ and $\mathbf{w}'$, so that $\|\mathbf{v}\|^2 = ({}^t\mathbf{w}\mathbf{v})^2 + ({}^t\mathbf{w}'\mathbf{v})^2$. If α is the product of the denominators of ${}^t\mathbf{w}\mathbf{v}$ and ${}^t\mathbf{w}'\mathbf{v}$, then $\alpha^2\|\mathbf{v}\|^2$ is the sum of the squares of two integers, and so by Result 4 $\|\mathbf{v}\|^2$ itself is the sum of the squares of two integers as claimed.

Sufficiency. By Proposition 2 we need only show that (3) has a nontrivial solution in the integers. By assumption q is the sum of the squares of two integers and by definition p is, so that by Lemma 1, the solvability of (3) in nontrivial integers is equivalent to that of $qx^2 - py^2 - z^2 = 0$ in nontrivial integers, but $(1, 1, n_3)$ clearly solves this equation. □

In fact we could have avoided use of the lemma by use of the following proposition, which has the advantage of yielding an almost-closed-form solution of (3). The proposition's statement agrees with Theorem 1 due to the following simple lemma [7].

Lemma 2
If a and b are the sums of two squares, so is ab. If a and ab are the sums of two squares, so is b.

Proof Result 4 makes the claims obvious. □

Proposition 3
If $pq = r^2 + s^2$, then $(q + r, p + r, n_3 s)$ solves (3).

Proof $p(q + r)^2 - q(p + r)^2 = pq^2 + pr^2 - qp^2 - qr^2 = q(pq - r^2) - p(pq - r^2) = n_3^2 s^2$, which verifies the claim [8]. □

We can express this in terms more similar to those of Theorem 1 by applying the well-known identity

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2. \qquad (14)$$

Corollary 4
If $\|\mathbf{v}\|^2 = a^2 + b^2$, then $(q - an_1 - bn_2, p - an_1 - bn_2, n_3(an_2 - bn_1))$ solves (3).

Proof (14) and Proposition 3 suffice. □

Example 4
If $\mathbf{v} = {}^t(11, 17, 24)$, then $p = 11^2 + 17^2 = 410$ and $\|\mathbf{v}\|^2 = q = p + 24^2 = 986$. Since $986 = 2 \cdot 17 \cdot 29$, then $\|\mathbf{v}\|^2$ is the sum of two squares by Result 4, so that by Theorem 1 $\mathbf{u} \in \mathbb{Q}^3$ exists. Since $25^2 + 19^2 = 986$, then (14) implies that $pq = qp = (25^2 + 19^2)(11^2 + 17^2) = 598^2 + 216^2$, so that by Proposition 3 we have that $(986 + 598, 410 + 598, 24 \cdot 216) = (1584, 1008, 5184) = 144(11, 7, 36)$ solves the equation, and by the homogeneity of the equation so does $(11, 7, 36)$. □

Although not the purpose of this investigation, the results lead immediately to information about rational maps between vectors. This in turn has implications regarding maps of many objects commonly occurring in modeling. Before stating them we need several terms.

Definition 3
Let $g(3, \mathbb{R})$ be the algebra of all 3 by 3 matrices with real components, and let $g(3, \mathbb{Q})$ be the subalgebra with components in $\mathbb{Q}$. Let $G(3, \mathbb{R})$ be the group of 3 by 3 invertible matrices with real components, and let $G(3, \mathbb{Q})$ be the subgroup with components in $\mathbb{Q}$. Let $O(3, \mathbb{R}) \subset G(3, \mathbb{R})$ be the subgroup of orthogonal matrices, and $O(3, \mathbb{Q})$ the corresponding subgroup with rational components. □

Lemma 3
$\mathbf{v} \in \mathbb{Q}^3$ admits unit $\mathbf{u}$ and $\mathbf{u}'$ in $\mathbb{Q}^3$ with $\{\mathbf{v}, \mathbf{u}, \mathbf{u}'\}$ forming an orthogonal basis if and only if there exists $O \in O(3, \mathbb{Q})$ such that $\{O^t(1, 0, 0), O^t(0, 1, 0), O^t(0, 0, 1)\} = \{\mathbf{v}/\|\mathbf{v}\|, \mathbf{u}, \mathbf{u}'\}$. $\mathbf{v} \in \mathbb{Q}^3$ has rational unit orthogonal $\mathbf{u}$ if and only if there exists ${}^t(a, b, 0) \in \mathbb{Q}^3$ with $\|\mathbf{v}\|^2 = a^2 + b^2$ and for each such ${}^t(a, b, 0)$ there exists $O \in O(3, \mathbb{Q})$ such that $O^t(a, b, 0) = \mathbf{v}$ and $O^t(0, 0, 1) = \mathbf{u}$.

Proof In each of the claims sufficiency is obvious.

In the first claim, since $\mathbf{u}$ and $\mathbf{u}'$ exist, then Proposition 1 implies that $\|\mathbf{v}\| \in \mathbb{Q}$. Matrix O with columns $\mathbf{v}/\|\mathbf{v}\|$, $\mathbf{u}$, $\mathbf{u}'$ is the matrix which establishes the necessity of the claim.

Now we turn to the necessity of the second claim. By Theorem 1 there exist rational a and b with $a^2 + b^2 = \|\mathbf{v}\|^2$. If we define O by extending linearly from the map which takes ${}^t(a, b, 0)$ to $\mathbf{v}$, ${}^t(0, 0, 1)$ to $\mathbf{u}$, and ${}^t(-b, a, 0)$ to $\mathbf{v} \times \mathbf{u}$, then we see quickly that $O \in G(3, \mathbb{R})$. Since $a^2 + b^2 = \|\mathbf{v} \times \mathbf{u}\|^2 = \|\mathbf{v}\|^2$, O maps an orthogonal basis to an orthogonal basis and preserves the lengths of the basis vectors, so that we also have that $O \in O(3, \mathbb{R})$. For

$$\phi_1 \colon \mathbf{w} \in \mathbb{R}^3 \to \left(\frac{1}{\sqrt{a^2 + b^2}} (a, b, 0)\mathbf{w} \right) \frac{\mathbf{v}}{\|\mathbf{v}\|},$$

ϕ_2: $\mathbf{w} \in \mathbb{R}^3 \rightarrow ((0, 0, 1)\mathbf{w})\mathbf{u}$,

$$\phi_3: \mathbf{w} \in \mathbb{R}^3 \rightarrow \left(\frac{1}{\sqrt{a^2 + b^2}}(-b, a, 0)\mathbf{w}\right)\frac{\mathbf{v} \times \mathbf{u}}{\|\mathbf{v} \times \mathbf{u}\|},$$

we have $\phi_1, \phi_2, \phi_3 \in g(3, \mathbb{Q})$. Now since $\phi_1 + \phi_2 + \phi_3 = O$, then $O \in O(3, \mathbb{Q})$ as claimed. □

Definition 4
For $\mathbf{v}, \mathbf{p} \in \mathbb{R}^3$ let $P(\mathbf{v}, \mathbf{p}) = \{\mathbf{x} \in \mathbb{R}^3 : {}^t\mathbf{v}(\mathbf{x} - \mathbf{p}) = 0\}$, that is, the plane orthogonal to $\mathbf{v}$ and containing $\mathbf{p}$. Let $L(\mathbf{v}, \mathbf{p}) = \{t\mathbf{v} + \mathbf{p} : t \in \mathbb{R}\}$, that is, the line parallel to $\mathbf{v}$ and containing $\mathbf{p}$. We say that $P(\mathbf{v}, \mathbf{p})$ [or $L(\mathbf{v}, \mathbf{p})$] is rational if $\mathbf{v}, \mathbf{p} \in \mathbb{Q}^3$. □

Corollary 5
Let $P = P(\mathbf{v}, \mathbf{0})$ and $P' = P(\mathbf{v}', \mathbf{0})$ be rational, and further let $\|\mathbf{v}\|^2 = r^2 + s^2$ for $r, s \in \mathbb{Q}$. There exists $O \in O(3, \mathbb{Q})$ such that $O(P) = P'$ if and only if $\|\mathbf{v}'\| = q\|\mathbf{v}\|$ for some $q \in \mathbb{Q}$.

Proof If O exists, then $O\mathbf{v} = q\mathbf{v}'$ for some $q \in \mathbb{Q}$, since $O\mathbf{v}, \mathbf{v}' \in \mathbb{Q}^3$ and are parallel. On the other hand, if $\|\mathbf{v}'\|^2 = (qr)^2 + (qs)^2$, then Lemma 3 implies the existence of orthogonal O_1 mapping ${}^t(r, s, 0)$ to $\mathbf{v}$ and orthogonal O_2 mapping ${}^t(qr, qs, 0)$ to $\mathbf{v}'$, so that $O_2O_1^{-1}(P) = P'$. □

Since a rigid motion is decomposable into an orthogonal motion and a translation, the above implies that not all rational planes can be mapped to one another by rigid motions. The obvious generalization to lines implies that the same is true for lines. The implications of these simple observations are far-reaching. In the common robotics problem of putting a block on a table, they mean that the rigid motion required may not be able to be represented in Cartesian coordinates with rational numbers. For example, if the table is assumed to lie in the x-y plane and the block has a face in a plane orthogonal to (1, 1, 1), then the rigid motion is of this type. In geometrical modeling one would like to believe that a rigid motion moving a cylinder to an identical cylinder can always be provided, but again this may not be so in the world of rational rigid motions. It seems, then, that extensions of the rationals, leading to symbol manipulation, or approximations, or a severe limitation of the domain of applicability, are the only recourses.

5. Discussion of the algorithm

At this point we have reduced the problem of determining whether a rational orthonormal vector exists to factoring an integer and calculating the factors mod(4), and the problem of finding a vector when a solution exists to decomposing an integer as sum of the squares of two integers. Since the problems arise in a computational setting, any estimation of the usefulness of the reductions must be determined by the difficulty of implementation and space and time requirements of an implementation.

Implementation of the technique presents little difficulty for a symbol manipulator. Infinite-precision integer arithmetic in a language would suffice, while the availability of arithmetic mod(4), greatest common divisor, factorization, and an implementation of decomposition into a sum of squares would clearly ease the programming task [9].

For ease of exposition let us make the following definition.

Definition 5
For $n \in \mathbb{Z}$ let bit(n) denote the minimal $m \in \mathbb{Z}$ with $|n| < 2^m$, that is, the number of bits needed to represent n, and for $s/t \in \mathbb{Q}$ let bit(s/t) = bit(s) + bit(t). □

Now, in order to discuss the space requirements for representing a solution vector $\mathbf{u} \in \mathbb{Q}^3$, we consider an estimate. The vector is found by applying the solution to (3) given in Proposition 3 to the formula in Corollary 1.

Proposition 4
If $\mathbf{v} = {}^t(n_1, n_2, n_3) \in \mathbb{Z}^3$ and $\|\mathbf{v}\|^2 = a^2 + b^2$ for $a, b \in \mathbb{Z}$, then for

$$\mathbf{u} = {}^t(u_1, u_2, u_3) = \frac{1}{q - r}\,{}^t(n_3(a - n_1), n_3(b - n_2), p - r)$$

with

$$p = n_1^2 + n_2^2,\ q = \|\mathbf{v}\|^2, \text{ and } r = n_1a + n_2b,$$

we have that $\mathbf{u}$ is a rational unit vector orthogonal to $\mathbf{v}$, and if bit(n_i) $\leq n$ for all $1 \leq i \leq 3$, then bit(u_i) $\leq 4n + 4$ for all $1 \leq i \leq 3$.

Proof For $s = n_1b - n_2a$ by (14) we have

$$pq = (n_1^2 + n_2^2)(a^2 + b^2) = (n_1a + n_2b)^2 + (n_1b - n_2a)^2$$
$$= r^2 + s^2 = (-r)^2 + s^2,$$

so that by Proposition 3 $(q - r, p - r, n_3s)$ solves (3). Since

$$\begin{aligned} n_1n_3(p - r) + n_2n_3s &= n_1n_3(n_1^2 + n_2^2 - r) + n_2n_3s \\ &= n_1n_3(n_1^2 + n_2^2) + n_3(n_2s - n_1r) \\ &= n_1n_3(n_1^2 + n_2^2) + n_1n_2n_3b - n_3n_2^2a \\ &\quad - n_3n_1^2a - n_1n_2n_3b \\ &= n_3(n_1 - a)(n_1^2 + n_2^2), \end{aligned}$$

and similarly

$$-n_2n_3(p - r) + n_1n_3s = n_3(b - n_2)(n_1^2 + n_2^2),$$

Corollary 1 implies that $\mathbf{u}$ defined as above is unit and orthogonal to $\mathbf{v}$. The claims on bit length now follow trivially from the definition of $\mathbf{u}$ and simple obvious estimates of the length of products and square roots. □

The method of Proposition 3 is thus seen to produce vectors $\mathbf{u}$ requiring at most four times the storage of $\mathbf{v}$ plus 12 bits. For some applications this may seem too costly, but in general it seems quite reasonable, and in fact agrees almost exactly with the storage requirements of the cross product and norm of (1).

The only time-intensive parts of the above method are the factorization of an integer and the decomposition of an integer into the sum of the squares of two integers. Factorization is known to be hard. In fact, its difficulty is the basis of many modern cryptographic schemes. Probabilistic algorithms exist which run in average time proportional to the fourth root of the integer. For the decomposition problem the situation is better. Probabilistic algorithms exist which run in average time proportional to a polynomial of the logarithm of the integer [10]. Since factorization is necessary for deciding whether a rational orthogonal unit vector exists, the method is always dominated by the factorization when the constants of proportionality are comparable. Because we have shown that a rational orthogonal unit vector does not always exist, it will be necessary in any case to have recourse to solutions of the form of (1) or better, (6), so that it seems reasonable and prudent to restrict application of these methods to vectors $\mathbf{v} \in \mathbb{Q}^3$ which are parallel to vectors $\mathbf{w} \in \mathbb{Z}^3$ such that $\|\mathbf{w}\|^2$ is not too large. Unfortunately, this "not too large" is difficult to define precisely, since it is dependent on the constant of proportionality in the time estimation of factorization, the computational resources available, and the needs of the applications [11]. These, however, are typically problems only in very special cases.

6. Concluding remarks

In this paper we have examined the problem of finding computationally simple unit vectors orthogonal to a given rational vector, **v**. We have shown that the unit vectors can be chosen to be rational, if and only if $\|\mathbf{v}\|$ is rational, while in general they can be chosen to involve only $\|\mathbf{v}\|$ and rational numbers. We have shown that the existence of one rational vector is equivalent to the solvability of a Diophantine equation, and have developed a method to decide the solvability of this equation. When the equation is solvable, we have presented a specific solution. The solution leads directly to a rational unit vector orthogonal to the given vector, and we have estimated the storage requirements of this unit vector.

In a sense we have completely answered the original question, but as often happens, this leads to new questions. The time and space estimates are worst-case. Average-case estimates are also needed. Result 2 provides a sharp estimate for the solution of the controlling Diophantine equation. Is there a comparable estimate for the components of a rational unit vector? Lemma 3 and Corollary 5 can be viewed as determining sets of equivalence classes of vectors or planes or lines under $O(3, \mathbb{Q})$. Can we extend this to more general vectors, planes, or lines? More generally, what can be said about extensions to $O(3, \mathbb{Q})$ that allow an arbitrary plane to be mapped to another?

Appendix

In the introduction, we presented an intuitive definition of one expression being simpler than another. It seems precise enough to allow understanding of and agreement with the claims of relative simplicity of expressions found elsewhere in the paper. However, in order to remove any possible ambiguity we present a more formal definition here. It is convenient to pose it in a greater generality than is necessary in the paper. Elsewhere nothing more complex appears in any expression than a few simple square roots. The definition, however, remains valid over expressions involving nth roots and nesting of roots. In fact, its natural setting is algebraic numbers. For more information on the terms and constructs we use and for proofs of the claims we make, almost any textbook on modern algebra would suffice. For example see Chapter 5 of [12].

Let $F = \mathbb{Q}(x_1, \cdots, x_n)$ be the field of rational functions in n indeterminates with rational coefficients. If f is a function and $p(y)$ is a nonzero univariate polynomial in y with coefficients in F such that $p(f) = 0$, then we say that f is algebraic over F. If each element of $\{f_1, \cdots, f_k\}$ is algebraic over F, then $F(f_1, \cdots, f_k)$ (the field generated by adjoining $\{f_1, \cdots, f_k\}$ to F) forms a finite-dimensional vector space over F, whose dimension we denote as $(F(f_1 \cdots, f_k): F)$. Given two sets of vectors, $\mathbf{A} = \{\alpha^1\,{}^t(u_1^1, u_2^1, u_3^1), \cdots, \alpha^k\,{}^t(u_1^k, u_2^k, u_3^k)\}$ and $\mathbf{B} = \{\beta^1\,{}^t(v_1^1, v_2^1, v_3^1), \cdots, \beta^k\,{}^t(v_1^k, v_2^k, v_3^k)\}$ with each of $\alpha^1, \cdots, \alpha^k, u_1^1, u_2^1, \cdots, u_2^k, u_3^k, \beta^1, \cdots, \beta^k, v_1^1, v_2^1, \cdots, v_2^k, v_3^k$ being algebraic over F, we say that **A** is algebraically simpler than **B** if $(F(\alpha^1, \cdots, \alpha^k, u_1^1, \cdots, u_3^k): F) < (F(\beta^1, \cdots, \beta^k, v_1^1, \cdots, v_3^k): F)$, or if

$$(F(\alpha^1, \cdots, \alpha^k, u_1^1, \cdots, u_3^k): F) = (F(\beta^1, \cdots, \beta^k, v_1^1, \cdots, v_3^k): F),$$

and

$$\sum_{j=1}^{k} ((F(\alpha^j): F) + \sum_{m=1}^{3} (F(u_m^j): F)) < \sum_{j=1}^{k} ((F(\beta^j): F) + \sum_{m=1}^{3} (F(v_m^j): F)).$$

If neither **A** is algebraically simpler than **B**, nor **B** algebraically simpler than **A**, **A** and **B** have the same algebraic complexity.

Each of the vectors appearing in this paper can be shown to satisfy the assumptions of this definition; that is, all their expressions are algebraic over F for $n = 3$. In terms of these vectors, the first condition implies that **A** has fewer algebraically independent square roots, while the second condition implies that **A** and **B** have the same number but there are fewer occurrences of square roots in **A**.

Finally, we say that **A** is simpler than **B**, if **A** is algebraically simpler than **B**, or if they have the same algebraic complexity, and the sum of the bits needed to represent the rational coefficients of **A** is less than that of **B**.

Acknowledgment

The authors are grateful to the Scuola Normale Superiore, Pisa, Italy, for its partial support of the work reported in this paper.

References and notes

1. J. Levin, "A Parametric Algorithm for Drawing of Solid Objects Composed of Quadric Surfaces," *Commun. ACM* **19,** No. 10, 555–563 (October 1976).
2. This problem can be considered a special case of the general problem of the existence of rational points on algebraic curves, but we do not pursue this.
3. L. Holzer, "Minimal Solutions to Diophantine Equations," *Can. J. Math.* **11,** 238–244 (1950).
4. L. J. Mordell, *Diophantine Equations*, Academic Press, Inc., New York, 1969.
5. E. Landau, *Elementary Number Theory*, Chelsea Publishing Company, New York, 1966.
6. Although it is unnecessary here, the reductions we have presented are a subset of a fuller set that serves to show that Result 1 is in fact a completely general solution to the solvability of an equation of the form $rx^2 + sy^2 + tz^2 = 0$ (see pp. 43–44 of [4]). This more general set of reductions and the same ideas as in the proof of the lemma suffice to show that for p and q the sums of two squares and a, b integers $apx^2 - aqy^2 - bz^2 = 0$ is solvable if and only if $aqx^2 - apy^2 - bz^2 = 0$ is solvable.
7. Clearly $\sqrt{p} \in \mathbb{Q}$ and $\sqrt{q} \in \mathbb{Q}$ are covered by Theorem 1. The lemma also implies that the other case we considered earlier, $\sqrt{pq} \in \mathbb{Q}$, is covered by the theorem, as of course all subcases must be.
8. For a result similar to this, see L. Calzolari, "Nota Sull' Equazione $u^2 = Ax^2 \pm By^2$," *Giornale di Matematiche* **VIII,** 28–34 (1870).
9. Each of these facilities currently exists in Scratchpad II, for example.
10. Each of these algorithms is available in the current implementation of Scratchpad II.
11. In the current Scratchpad II implementation, this "not too large" leads to restricting $\|\mathbf{w}\|^2 \leq 10^{20}$; that is, $\mathbf{w}$ is a vector whose components are approximately single-precision 32-bit integers.
12. J. K. Goldhaber and G. Ehrlich, *Algebra*, The Macmillan Company, London, 1970.

Received October 20, 1986; accepted for publication January 9, 1987

Michael A. O'Connor *IBM Thomas J. Watson Research Center, P.O. Box 218, Yorktown Heights, New York 10598.* Dr. O'Connor received his Ph.D. in mathematics in 1980 from the University of Maryland, College Park. Until 1983 he was a Staff Fellow at the Division of Computer Research and Technology of the National Institutes of Health, Bethesda, Maryland, where he conducted research in invariant metrics, differential geometry, and applications of geometry. Dr. O'Connor joined IBM in 1983 as a Research staff member in Manufacturing Research at the Thomas J. Watson Research Center. During the spring of 1986 he was a visiting assistant professor at the Scuola Normale Superiore, Pisa, Italy, where the research reported in this paper was completed. His current research interests include robust geometrical modeling, geometrical algorithms, and the use of computer algebra systems in geometry.

Graziano Gentili *Scuola Normale Superiore, Piazza dei Cavalieri 7, 56100 Pisa, Italy.* Dr. Gentili received his Ph.D. in mathematics at the Scuola Normale Superiore, Pisa, Italy, in 1981, with a dissertation in Riemannian geometry. His main research interests are in differential and Riemannian geometry, invariant metrics on complex domains, and the theory of functions of several complex variables. He has been a visiting assistant professor at the Department of Mathematics of the University of Maryland, College Park, where he has strong connections with the researchers in geometry-topology and complex analysis. Since 1981 he has been an assistant professor in geometry at the Scuola Normale Superiore.