J. Symbolic Computation (1991) **11**, 213-229

Rational Geometry in Space

GRAZIANO GENTILI AND MICHAEL A. O'CONNOR[†]

International School for Advanced Studies,
Strada Costiera, 11, 34014 Trieste, Italy.

[†]*IBM Thomas J. Watson Research Center,*
P.O. Box 218, Yorktown Heights, New York 10589

(Received 9 November 1988)

The objects and motions of geometrical modelling, graphics and robotics are most often described by rational (or close to rational) data in R^3. This leads naturally to a notion of rational geometry (as opposed to the classical notion of Euclidean geometry) where two objects are considered equal if there exists a rational rigid motion from one to the other.

We show here that although the notion of equality in rational geometry differs from that of Euclidean geometry for lines and planes, the two notions coincide on collections of line segments, in particular for polyhedra. Next, by an explicit symbolic calculation and the use of a simple technique of classical number theory, we obtain a rational parameterization of the subgroup of all rational linear movements of the space which keep a given point fixed. Finally we study the equivalence relation of Q-equality among segments in the space Q^3, and give a representation of the space of equivalence classes, i.e. of the quotient space $Q^3/O(3, Q)$.

0747-7171/91/030213+17 \$03.00/0

1. Introduction

Many algorithms and techniques of geometrical modelling, graphics, robotics and other areas are based on Euclidean geometry (see, e.g., [Coxeter (1969)]). Euclidean geometry, in turn, is based on point sets and transformations of vector spaces over the real numbers. Currently available implementations of these tools utilize floating point calculations, which yield values in a fixed subset of the rational numbers. Certain experimental systems and research efforts propose the use of infinite precision rational calculations or calculations involving simple real extensions [Godement (1963), § 26.4] of the rational numbers.[Ocken *et al.*(1983)]. Either the rational numbers or any simple real extension of the rationals is of course a restriction of the real numbers, so that an implementation based on these existent or proposed schemes must then restrict the available point sets and transformations of Euclidean geometry to those describable by rational data or by a simple extension of rational data. However, this restriction can call into question the correctness of a geometric algorithm dependent on facts gleaned from Euclidean geometry or even the possibility of the solution of a problem. For example, consider the classic problem of placing a block on a table. From a purely geometric perspective the solution is trivial: map the plane containing a face of the block to the plane of the table by a rigid motion and translate the block along the plane to the table. The foundations of Euclidean geometry assure the existence of the rigid motion. If, however, the algorithm is to be implemented in an existent geometrical modeller, then the block and the table will be described by rational data and the rigid motion must also be rational, and a subtle question remains: does such a rational rigid motion always exist? More generally, we could ask what happens to Euclidean geometry when the data is rational, or close to rational. In this paper the authors try to explain in what sense a geometry over the rational numbers in the space R^3 can be constructed involving simple rational objects such as planes, lines, polygons, polyhedra and their Boolean combinations.

An immediate motivation for this work follows from the results contained in a previous paper,[O'Connor & Gentili(1987)], in which the following problem is completely discussed: given a non-zero rational vector v (i.e. a vector whose entries are all rationals) in the space R^3, when is it possible to find two other vectors u and u', orthogonal with respect to each other and to v, having unitary norm, with entries as "simple" as possible and belonging to Q, the field of rational numbers, or to some simple extension of Q.

This problem often appears in situations in which it is most advantageous to find (when possible) exact, rational u and u' and naturally suggests the definition of Q-equality (see Definition 2.1) and the study of a rational geometry in the space R^3 (See Section 2).

It is somewhat surprising that Q-equality and classical Euclidean equality do not coincide for rational objects: the two rational planes $\pi : \quad z = 0$ and $\pi' : \quad x + y + z = 0$ are not Q-equal, i.e. there does not exist any rational rigid motion mapping π onto π', (see Proposition 2.2).

The results contained in this paper show that Euclidean equality and Q-equality coincide for rational segments, polygons, polyhedra and their combinations, (see Proposition 3.1 and corollaries), and hence provide a basis for the discussion of "rational" geometry of Section 3. This property of the space is especially interesting in view of the contrasting situation for the two rational planes π and π'. It implies, for example, that a rational triangle lying on the plane π can never be equal to a rational triangle lying on the plane π'.

Actually, our attention towards these geometric questions began with a study of rational movements and related exact computation experiments in the Scratchpad II computer algebra system [Jenks *et al.* (1988)]. Certain of these computations allowed us to reduce the problem of determining the rational isotropy subgroup [Berger (1977), Ch.1 sec.6] of a given rational vector (i.e . the subgroup consisting of all the rational orthogonal transformations of the space which fix the given vector) to where a simple technique from classical number theory yields an injective parameterization of the subgroup itself. This result provides a means to obtain the set of all rational orthogonal matrices which transform a rational vector v_1 into a rational vector v_2 having the same length. These results are discussed in Section 5.

The quotient space [Godement (1963), § 4.2] of Q^3 with respect to the action of the group $O(3, Q)$ of all rational orthogonal linear transformations (briefly $Q^3/O(3, Q)$) is the space whose elements are the equivalence classes of points of Q^3 with respect to the following equivalence relation

$\sim$: $u \sim v$ if there exists $n \in O(3, Q)$ such that $u = nv$. In Section 6 the quotient space $Q^3/O(3, Q)$ is studied, to further elucidate the difference between classical Euclidean equality and Q-equality. A representation of this quotient is exhibited.

Lastly, it should be noted that Sections 2 through 5 easily generalize to any subfield K of R. In fact, if we replace Q by K in the definitions of rational objects to obtain definitions of K-objects, then we can restate all results in terms of K. The proofs that we present here also suffice in the more general setting. In this paper Q has been used for the sake of simplicity and homogeneity and to make clear its connections with exact computational questions. Only Section 6 makes use of results linked intrinsically to the rational numbers .

The authors want to thank the T.J. Watson Research Center of IBM and the International School for Advanced Studies of Trieste for their kind support.

2. Q-Equality and rational geometry

Geometry transforms the theory of sets into something dynamical, by generalizing the idea of equality. In the theory of sets one says that two sets are equal if they contain exactly the same elements. In geometry two sets are said to be equal if there exists a "movement" of the "space" which carries one onto the other.

For example in the case of Euclidean geometry in R^3 two subsets A and B are equal if there exists a rigid motion g (i.e. a translation plus a rotation) of the space such that $g(A) = B$.

Clearly the idea of equality among objects in a geometrical space depends on the group of movements we want to consider on the space. For example, in R^2, let $T(2, R)$ be the group of all translations and let

$$GL(2, R) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : \quad a,\ b,\ c,\ d \in R \quad \text{such} \quad \text{that} \quad ab - cd \neq 0 \right\}$$

be the group of all invertible linear transformations. Denote by $\tau(2, R)$ the semidirect product of $GL(2, R) \cdot T(2, R)$. If one considers the group of movements $\tau(2,R)$ acting on R^2, then all the triangles of the plane are equal. In fact the transformation

$$\begin{bmatrix} e & f \\ g & h \end{bmatrix} \cdot \begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1}$$

carries the triangle with vertices $(0,0)$, (a,c), (b,d) onto the triangle with vertices $(0,0)$, (e,g), (f,h)

If one considers instead $\tau'(2,R) = SL(2,R) \cdot T(2,R)$,where

$$SL(2,R) = \{u \in GL(2,R) \quad : \quad \det u = 1\}$$

then only the triangles having the same area are equal. This last assertion depends on the fact that if $(a,c) = x$, $(b,d) = y$, then

$$\det \begin{bmatrix} a & b \\ c & d \end{bmatrix} = |x||y| sin\theta$$

with θ the angle between x and y.

Finally, if one considers $\tau''(2,R) = O(2,R) \cdot T(2,R)$, where $O(2,R)$ is the orthogonal group in R^2, then the equality is the classical Euclidean equality.

Let us denote by $O(3,Q) = O(Q)$ the group of all orthogonal 3×3 matrices with rational entries, and by $T(3,Q) = T(Q)$ the group of all translations by vectors with rational entries in R^3. If $M(3,Q) = M(Q)$ denotes the semidirect product $O(Q) \cdot T(Q)$, then

Definition **2.1** *Two subsets A and B of R^3 are said to be Q*-equal *if there exists a movement $m \in M(Q)$ such that $m(A) = B$.*

The geometry obtained from the Euclidean geometry in R^3 by restricting the group of movements to $M(Q)$ will be referred to as the *Rational Geometry of R^3*. Since the group of motions is now $M(Q)$, some "rational" subsets become of natural interest. The *rational points* (or *rational vectors*) of R^3 will of course be the points of $Q^3 \subset R^3$. *Rational lines* will be the lines of R^3 containing a rational point and parallel to a rational vector. *Rational planes* will be the planes containing a rational point and orthogonal to a rational vector. A *rational segment* will be a segment whose endpoints are rational. In the same way one can define *rational polygons, polyhedra* and so on.

Rational planes and lines can be described by means of (parametric or implicit) equations with rational coefficients. For example, the plane π containing the rational point X_0 and perpendicular to the rational vector P can be described as the set of points $X \in R^3$ for which $P(X - X_0) = 0$ or parameterically as

$$(u,v) \mapsto u \cdot (P \times W) + v \cdot (P \times (P \times W)) + X_0$$

for u, $v \in R$ and W any non-zero rational vector not parallel to P.

The set of rational points, lines and planes is closed under intersection, and constitutes a first natural environment on which to investigate the meaning of the rational geometry of the space. A natural first question is to ask whether all rational planes (and all rational lines) are Q-equal: the answer is surprisingly negative as the following proposition points out:

Proposition **2.2** *The two rational planes with equations $z = 0$ and $x + y + z = 0$ are not Q-equal. The two rational lines $t \mapsto (0,0,t)$ and $t \mapsto (t,t,t)$ are not Q-equal.*

For a proof, see [O'Connor & Gentili(1987)].

Since not all rational lines are Q-equal and not all rational planes are Q-equal in R^3, it becomes of immediate interest to investigate what happens for Q-equality among rational objects such as rational segments, polygons, polyhedra of the space. This will be considered in the next section.

3. Q-equality among rational objects

A natural reason to start with the study of Q-equality among rational triangles of the space is the clear fact that Q-equality among rational segments, polygons, polyhedra, planes and so on depends upon Q-equality among rational triangles.

First note that, given any two rational triangles, to require that they be Q-equal is meaningless if they are not equal in the Euclidean sense. So that we can expect at most what is stated in the following

Proposition **3.1** *Euclidean equality and Q-equality coincide for rational triangles in space.*

Proof.

Consider any two rational triangles V and V', equal in the Euclidean sense, in the space R^3. We can suppose, up to a rational translation, that the two equal triangles have two corresponding vertices at the origin. Let a and a', b and b' be corresponding sides of V and V' respectively, with one end-point being the origin and the other being, respectively, A, B, A', B'. Now, the two tetrahedra W and W' with vertices $\{0, A, B, A \times B\}$ and $\{0, A', B', A' \times B'\}$ are equal and rational. Therefore there exists one and only one linear transformation $g \in GL(3, R)$ such that

$$g(A) = A', \quad g(B) = B' \quad \text{and} \quad g(W) = W'$$

and obviously $g \in O(3, R)$. If h and h' are the matrices whose columns are respectively $[A, B, A \times B]$ and $[A', B', A' \times B']$, then h^{-1}, h' and $k = h' \cdot h^{-1}$ have rational entries and

$$k(A) = A', \quad k(B) = B', \qquad k(W) = W'$$

By uniqueness, $g = k$ and hence V and V' are Q-equal.

Notice that the proof above is constructive in the sense that if one is given the vertices of two equal rational triangles, then by following the proof one computes in an exact fashion the rational entries of a transformation $m \in M(3, Q)$ which maps one triangle onto the other.

Proposition 3.1 directly implies the following

Corollary **3.2** *If g is a rigid Euclidean motion of R^3 which maps a rational triangle onto a rational triangle, then g is a rational rigid motion and maps all rational triangles onto rational triangles.*

Corollary **3.3** *Euclidean equality and Q-equality coincide for rational segments, polygons and polyhedra of R^3.*

Proof

The claims for polygons and polyhedra follow directly from Corollary 3.2. Suppose v_1 and v_2 are two rational points of R^3 with $||v_1|| = ||v_2||$. If $v_1 = \pm v_2$ then the claim is obvious, so assume that $v_1 \neq \pm v_2$.The two triangles with vertices $\{0, v_1, v_1 \times v_2\}$ and $\{0, v_2, v_1 \times v_2\}$ are equal, and Proposition 3.1 now implies the assertion concerning segments.

It is worthwile noticing that any rational triangle contained in the plane $\pi: \quad z = 0$ cannot be equal to any rational triangle contained in the plane $\pi': \quad x + y + z = 0$. In fact if this were the case, by Proposition 3.1 and Corollary 3.2, the two planes π and π' would be Q-equal, contradicting Proposition 2.2.

Since equality between sets in geometry is intrinsically linked to the existence of transformations which map one set onto the other, it is worthwhile and customary to study the set of all such transformations. In fact it is often of importance to determine which motions of the space leave an object fixed.

In Q-equality, by definition, if two objects are not equal, there can be no rational transformation between them. For the case of polyhedra or the case of polygons, it is easy to see that there can exist at most finitely many rational transformations. For the case of two Q-equal segments, the situation is much more interesting. In Section 5 we will see that there are always infinitely many such transformations.

Before proceeding to this study, we present in the next section some preliminary facts on the structure of the real orthogonal group $O(R) = O(3, R)$.

4. Simple facts on the orthogonal group

For v_1, $v_2 \in R^3$, let $O(R)_{v_1,v_2}$be the subset of the orthogonal group $O(R)$ whose elements carry v_1 into the half line through the origin and v_2. If $q \in O(R)_{v_1,v_2}$ then for any other $p \in O(R)_{v_1,v_2}$ the matrix $c = pq^{-1}$ belongs to $O(R)_{v_2,v_2}$. Thus $p \in O(R)_{v_2,v_2} \cdot q$ so that $O(R)_{v_1,v_2} \subset O(R)_{v_2,v_2} \cdot q$, and since the opposite inclusion is obvious, it follows that

$$O(R)_{v_1,v_2} = O(R)_{v_2,v_2} \cdot q \tag{4.1}$$

If $p' \in O(R)_{v_1,v_1}$ then $qp'q^{-1} \in O(R)_{v_2,v_2}$ so that $O(R)_{v_1,v_1} \subset q^{-1} \cdot O(R)_{v_2,v_2} \cdot q$, and since the opposite inclusion is obvious

$$O(R)_{v_1,v_1} = q^{-1} \cdot O(R)_{v_2,v_2} \cdot q \tag{4.2}$$

i.e. the isotropy subgroups of any two points in the same orbit [see, e.g., [Berger (1977), Ch.1 sec.6] are conjugate [Godement (1963), § 7.13]. What we need in the sequel is the following

Proposition **4.1** *Let z be the vector $\begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \in R^3$. For any $m \in O(R)_{v_1,z}$ and any $n \in O(R)_{z,v_2}$ the following equality holds:*

$$O(R)_{v_1,v_2} = n \cdot O(R)_{z,z} \cdot m. \tag{4.3}$$

Proof.
By (4.1)

$$O(R)_{v_1,v_2} = O(R)_{v_2,v_2} \cdot n \cdot m$$

and by (4.2)

$$O(R)_{v_2,v_2} = n \cdot O(R)_{z,z} \cdot n^{-1}$$

Therefore (4.3) follows.

Equality (4.3) gives the possibility of decomposing any orthogonal matrix carring the vector v_1 to the vector v_2 in the form

$$n \cdot o \cdot m$$

where

$$m = \left[u, \quad u', \quad \frac{v_1}{||v_1||}\right]^{-1} \tag{4.4}$$

$$n = \left[\tilde{u}, \quad \tilde{u}', \quad \frac{v_2}{||v_2||}\right] \tag{4.5}$$

and

$$o \in O(R)_{z,z} = \left\{ \begin{bmatrix} x & y & 0 \\ -y & x & 0 \\ 0 & 0 & 1 \end{bmatrix} : x, \ y \in R, x^2 + y^2 = 1 \right\} \tag{4.6}$$

with $\left\{u, \quad u', \quad \frac{v_1}{||v_1||}\right\}$ and $\left\{\tilde{u}, \quad \tilde{u}', \quad \frac{v_2}{||v_2||}\right\}$ orthonormal bases in R^3.

The above decomposition and the structure of $O(R)_{z,z}$ gives a simple parameterization of the set $O(R)_{v_1,v_2}$ in terms of x, $y \in R$, which will be used in the explicit calculations of the following section.

5. Computation of the rational isotropy subgroup

Our study of rational geometry began with computational experiments concerning Q-equality of rational segments that where performed in the Scratchpad II computer algebra system. Certain of these experiments led us to attempt to find the set of rational transformations mapping a vector, v_1, to another vector, v_2, by solving a related system of Diophantine equations. When $v_1 = v_2$, that is when the set of transformations being investigated is the subgroup consisting of all the elements of $O(3, Q)$ which fix the vector $v_1 = v_2$ (the so called isotropy subgroup of v_1 in $O(3, Q)$), the system of equations assume a particularly simple form: simple enough, in fact, to yield an explicit rational parameterization of the subgroup.

Proposition **5.1** *For a fixed, non-zero rational vector $v = (v_x, v_y, v_z)$, let $q = ||v||^2$ and $p = v_x^2 + v_y^2$. The rational isotropy subgroup of v is composed of the identity and the set S which can be injectively parameterized as*

$$S = \left\{ n \begin{bmatrix} \frac{qm^2-1}{qm^2+1} & -\frac{2m\sqrt{q}}{qm^2+1} & 0 \\ \frac{2m\sqrt{q}}{qm^2+1} & \frac{qm^2-1}{qm^2+1} & 0 \\ 0 & 0 & 1 \end{bmatrix} n^{-1} : m \in Q \right\} \tag{5.1}$$

where:
if $p \neq 0$ *then*

$$n = \frac{1}{p\sqrt{q}} \begin{bmatrix} -v_x^2 v_z + v_y^2\sqrt{q} & v_x v_y v_z + v_x v_y \sqrt{q} & pv_x \\ -v_x v_y v_z - v_x v_y \sqrt{q} & v_y^2 v_z - v_x^2 \sqrt{q} & pv_y \\ pv_x & -pv_y & pv_z \end{bmatrix} \tag{5.2}$$

otherwise n *is the identity.*
Proof

By Section 2 of [O'Connor & Gentili(1987)], $n \in O(R)$ and maps the vector $(0, 0, ||v||)$ to v, so that by Proposition 4.1

$$O(R)_{v,v} = nO(R)_{z,z}n^{-1}$$

If, for x, $y \in R$, with $x^2 + y^2 = 1$ we let

$$t(x,y) = \begin{bmatrix} x & y & 0 \\ -y & x & 0 \\ 0 & 0 & 1 \end{bmatrix} \tag{5.3}$$

then (4.6) implies that

$$t(x,y;v) = nt(x,y)n^{-1} \tag{5.4}$$

describes the general matrix belonging to $O(R)_{v,v}$. If $\sqrt{q}$ is rational, then by (5.2), n is rational. Thus $t(x,y;v)$ is rational if, and only if, $t(x,y)$ is rational. Since in this case the parameterization of $t(x,y)$ in (5.1) is nothing but a rational reparameterization of the standard rational parameterization of the sine and cosine, the claims follow trivially.

Hence hereafter we assume that $\sqrt{q}$ is not rational. Let $\widetilde{Q}$ be the field of rational functions in v_x, v_y, v_z with coefficients in Q, and let $\widetilde{Q}(\sqrt{q})$ be the extension of $\widetilde{Q}$ by $\sqrt{q}$. By (5.4) it is now easy to see that each entry of $t(x,y;v)$ is a linear function in x and y with coefficients in $\widetilde{Q}(\sqrt{q})$. For $k = 3(i-1)+j$ let $\alpha_k x + \beta_k y + \gamma_k$ be the (i,j)-entry of $t(x,y;v)$. Matrix $t(x,y;v)$ is rational if and only if

$$\begin{cases} \alpha_1 x + \beta_1 y + \gamma_1 \in \tilde{Q} \\ \dots \\ \dots \\ \alpha_9 x + \beta_9 y + \gamma_9 \in \tilde{Q} \\ x^2 + y^2 = 1 \end{cases} \tag{5.5}$$

Since α_j and $\beta_j \in \widetilde{Q}(\sqrt{q})$, α_j and β_j can be represented in a unique way as

$$\alpha_j = \alpha_j^r + \alpha_j^i \sqrt{q}$$
$$\beta_j = \beta_j^r + \beta_j^i \sqrt{q}$$

where α_j^r, α_j^i, β_j^r, β_j^i belong to $\widetilde{Q}$.

Explicit symbolic calculations yield that the linear part of (5.5) is equivalent to

$$M \begin{bmatrix} x \\ y \end{bmatrix} + \gamma \in \widetilde{Q}^9 \tag{5.6}$$

where

$$M = \begin{bmatrix} v_y^2 + v_z^2 & 0 \\ -v_x v_y & -v_z\sqrt{q} \\ -v_x v_z & v_y\sqrt{q} \\ -v_x v_y & v_z\sqrt{q} \\ v_x^2 + v_z^2 & 0 \\ -v_x v_y & -v_x\sqrt{q} \\ -v_x v_z & -v_y\sqrt{q} \\ -v_y v_z & v_x\sqrt{q} \\ p & 0 \end{bmatrix} \tag{5.7}$$

$$\gamma = \begin{bmatrix} v_x^2 \\ v_x v_y \\ v_x v_z \\ v_x v_y \\ v_y^2 \\ v_y v_z \\ v_x v_z \\ v_y v_z \\ v_z^2 \end{bmatrix} \tag{5.8}$$

so that, since $\gamma \in \widetilde{Q}^9$, (5.6) is equivalent to

$$M \begin{bmatrix} x \\ y \end{bmatrix} \in \widetilde{Q}^9 \tag{5.9}$$

The matrix M has rank two because $p \neq 0$, therefore, by the standard Rouchè-Capelli method (See e.g. [Fekete(1985)], page 189), every solution (x, y) of (5.5) belongs to $(\widetilde{Q}(\sqrt{q}))^2$. If x and y belong to $\widetilde{Q}(\sqrt{q})$, we can uniquely decompose them as

$$\begin{aligned} x &= x^r + x^i\sqrt{q} \\ y &= y^r + y^i\sqrt{q} \end{aligned}$$

where x^r, x^i, y^r, y^i belong to $\widetilde{Q}$.
In terms of this decomposition and in view of (5.6), (5.5) is equivalent to

$$\begin{cases} M \begin{bmatrix} x^i \\ y^r \end{bmatrix} = 0 \\ (x^r)^2 + (y^r)^2 + q(x^i)^2 + q(y^i)^2 = 1 \\ x^r x^i + y^r y^i = 0 \end{cases} \tag{5.10}$$

Now, because M has rank two it follows immediately that $x^i = 0 = y^r$, so that (5.5) reduces to the following system:

$$\begin{cases} x^i = 0 \\ y^r = 0 \\ (x^r)^2 + q(y^i)^2 = 1 \end{cases} \tag{5.11}$$

Thus only x^r and y^i can vary in $\widetilde{Q}$, so that we need only find all rational solutions of the quadratic equation. Clearly, $x^r = 1$ and $y^i = 0$ solve (5.11). Using this one solution, we can apply a classical technique from number theory, the method of lines, to find all other solutions.

Any line that passes through two rational solutions has a rational slope. Thus if we parameterize the lines through $(1,0)$ with rational slope as $y^i = m(x^r - 1)$, then the second intersection with $(x^r)^2 + q(y^i)^2 = 1$ is

$$\begin{cases} x^r = \frac{qm^2-1}{qm^2+1} \\ y^i = -\frac{2m}{qm^2+1} \end{cases} \tag{5.12}$$

Given two Q-equal vectors u and v, the proofs of Proposition 3.1 and Corollary 3.3 explicitly provide a rational transformation T carrying u to v. Formula (4.1) implies that the set $O(Q)_{u,v}$ is obtained by composing $O(Q)_{u,u}$ and T, so that the previous result, in fact, can be used to obtain a parameterization of $O(Q)_{u,v}$.

In passing we note that the form of the parameterization of $O(Q)_{u,u}$ shows that it is dense in $O(R)_{u,u}$, and hence the same is true for $O(Q)_{u,v}$ and $O(R)_{u,v}$.

6. The quotient space $Q^3/O(3,Q)$

In the Euclidean geometry of R^3 all lines are equal and hence the quotient space $R^3/O(R)$ can be viewed as nothing but a single half-line. However since not all rational lines of the space are Q-equal (see Proposition 2.2), it becomes of interest to try to represent the quotient space of Q^3 with respect to the action of the orthogonal rational group $O(Q)$ (see the Preface).

In view of Corollary 3.3 (or Proposition 5.1), all the rational points (if any) belonging to a given sphere of the space are equivalent. In addition, two rational points with different norms cannot be equivalent and

Proposition **6.1** *For any v_1 and $v_2 \in Q^3$, there exists $T \in O(Q)$ carrying v_1 in the same direction of v_2 if, and only if, $||v_1|| = k||v_2||$ for some $k \in Q$.*

We are now ready to prove that

Theorem 6.2 *The quotient space $Q^3/O(Q)$ can be represented by the set*

$$Q \cdot A = \{ra : r \in Q, \quad a \in A\}$$

where A consists of all triples (a_1, a_2, a_3) of non-negative integers such that

i) If $a_1^2 + a_2^2 + a_3^2 = q$ then q is square free and not equal to $7 \mod 8$.
ii) If b_1, b_2 and b_3 are non-negative integers such that $b_1^2 + b_2^2 + b_3^2 = q$, then $a_1 \leq b_1$, and if $a_1 = b_1$ then $a_2 \leq b_2$.

Proof

Let $a \in Q^3$. We can obviously suppose that the three components of a are non-negative, since a change of the sign of coordinates maintains the equivalence.

Consider the smallest rational multiple b of a whose components are all non-negative integers. If $\tilde{a}$ and $\tilde{b}$ are the equivalence classes of a and b respectively, then $\tilde{a} \in Q \cdot \tilde{b}$.

It is well known from classical number theory ([Hardy & Wright(1938), Ch.20], [O'Connor & Gentili(1987)]) that a positive integer k is the sum of three integers squared, if and only if $k \neq 4^n(8m+7)$ for m and n being non-negative integers. The necessity of this somewhat strange looking result can be seen by a simple case analysis using the easily demonstrated facts that the square of an even integer must equal 0 or 4 mod 8, while the square of an odd integer must equal 1 mod 8; the sufficiency, however, is much more difficult to obtain.

Let us now consider the positive integer $p = ||b||^2$. Since p is the sum of three squares it cannot be of the form $4^n(8m + 7)$, therefore its square-free part s cannot be equal to 7 mod 8. Hence s can be written as the sum of three squares, i.e. there exists $c \in Q^3$ with non-negative integer components such that $s = ||c||^2$. By Proposition 6.1, the point b can be mapped on the same direction as c by means of a rational motion, therefore, if $\tilde{c}$ is the equivalence class of c, then $\tilde{b} \in Q \cdot \tilde{c}$ and $c \in A$.

Finally, condition *ii)* guarantees that there is only one representative for each equivalence class.

Let u and u' be non-zero rational vectors. If u and u' are orthogonal to the rational planes p and p', respectively, then Proposition 6.1 implies that p and p' are Q-equal if and only if there exists a rational number k such that $||u|| = k||u'||$. The same conclusion holds for the two lines l and l' whose direction vectors are u and u'. Moreover, the set A described in Theorem 6.2 represents the set of equivalence classes of rational lines and hence the equivalence classes of rational planes. These facts and the structure of A itself explain in detail the distinction between Q-equality and Euclidean equality for lines and planes, a distinction exemplified by Proposition 2.2.

It is easy to see that Q-equality and classical Euclidean equality do not coincide in general for rational, non-linear, algebraic subsets of R^3, i.e. for the zero-sets of a finite number of not all linear, algebraic equations with rational coefficients. Take, for example, in R^2 the rational equation of the ellipse $\epsilon : \quad x^2 + \frac{y^2}{4} = 1$. If one rotates it by an angle of $\frac{\pi}{4}$ one obtains $\epsilon' : \quad \frac{5}{8}x^2 + \frac{5}{8}y^2 - \frac{3}{4}xy = 1$ which clearly cannot be Q-equal to the given one. On the other hand one can recover a sort of "Q-equality" among ϵ and ϵ' if one allows orthogonal transformations with entries in $Q(\sqrt{2})$. This last fact seems to be a general fact and the investigation of Q-equality in this generalized sense, for rational algebraic subsets of R^3, should be of interest.

References

Berger, M. (1977). *Geometry I*, Springer-Verlag, Heidelberg.

Calzolari, L. (1870). *Nota Sull'Equazione* $u^2 = Ax^2 \pm By^2$, Giornale di Matematiche, **8**, 28 - 34.

Coxeter, H.S.M. (1969). *Introduction to Geometry*, Wiley, New York, (second edition).

Fekete, A.E. (1985). *Real Linear Algebra*, (Pure and Applied Mathematics, A Series of Monographs and Textbooks), Marcel Dekker Inc., New York and Basel.

Godement, R. (1963). *Cours d'Algèbre*, Hermann Paris.

Hardy, G.H., Wright, E.M. (1938). *An Introduction to the Theory of Numbers*, The Clarendon Press, Oxford.

Jenks, R.D., Sutor, R.S., and Watt, S.M. (1988). *Scratchpad II: An Abstract Datatype System for Mathematical Computation*, in *Scientific Software: IMA Volumes in Mathematics and Its Applications* Volume 14, Springer-Verlag, New York.

LeVeque, W.J. (1977). *Fundamentals of Number Theory*, Addison-Wesley publishing Company, London.

Mordell, L.J. (1969). *Diophantine Equations*, Academic Press Inc., New York.

Ocken, S., Schwartz, J.T., Sharir, M. (1983). *Precise Implementation of CAD Primitives Using Rational Parameterizations of Standard Surfaces*, Technical Report n.67, Computer Science Department, New York University, New York.

O' Connor, M.A., Gentili, G. (1987). *Simple Unit Vectors Orthogonal to a Given Vector*, IBM Journal of Research and Development, n.3, **31**, 335 - 342.