Adv. appl. Clifford alg. 19 (2009), 1–14

0188-7009/010001-14, *published online* August 13, 2008
DOI 10.1007/s00006-008-0129-0

Advances in Applied Clifford Algebras

Reflections, Rotations, and Pythagorean Numbers

G. Aragón-González, J.L. Aragón, M.A. Rodríguez-Andrade and L. Verde-Star

Abstract. In this article, simple reflections, rotations and the Cartan theorem are handled using Clifford algebras. With this tool we provide a constructive proof of the Cartan theorem and the relationship with Pythagorean numbers is discussed.

Mathematics Subject Classification (2000). 15A66, 12D15.

Keywords. Clifford algebras, reflections, rotations, Pythagorean numbers.

1. Introduction

In how many ways can an orthogonal transformation in an n-dimensional Euclidean space be decomposed?

This interesting problem was raised and answered about 50 years ago, and constitutes a particular case of the Cartan-Dieudonné theorem [1, 2]. This is one of the big theorems of geometry and yields as a corollary a theorem of Cartan of 1937 [1], which asserts that every orthogonal transformation in $\mathbb{R}^n$ can be written as the product of at most n simple reflections (reflections by hyperplanes). The Cartan-Dieudonné theorem is an existence theorem, and its proofs in the classical literature are based on the induction process, without providing an explicit procedure to determine the simple reflections that decompose a given orthogonal transformation. The theorem, however, considers reflections as the primitive transformations which, interestingly, is consistent with both the mathematical structure [3] and the cognitive structure of a college student [4]. Any student, for instance, can easily realize that, in three dimensions, a simple reflection corresponds to the effect of looking oneself on a two-dimensional mirror.

A student of linear algebra can understand intuitively that the orthogonal transformations in $\mathbb{R}^n$ are those linear transformations that preserve distances and, even more, that one can calculate the determinant of the matrix associated

with the transformation and deduce if it is either a rotation (+1) or a reflection (−1) [5]. The importance of reflections, on the other hand, resides in the fact that a simple reflection is associated with a matrix (Householder) which has several important applications in numerical linear algebra [6, 7]. A particular case is the QR decomposition method to solve a system of linear equations, where Q is an orthogonal matrix and R is an upper triangular matrix.

Thus, given that simple reflections are primitive orthogonal transformations, and taking into account the previous discussion, it is natural to ask

What are the simple reflections that determine a given orthogonal transformation in $\mathbb{R}^n$ *?*

Or, in particular

What Householder matrices determine a given orthogonal matrix in $\mathbb{R}^n$ *?*

A partial answer to this question has been given in the constructive proof of Theorem 1 in [6]. The idea behind the proof is the following. Given an $n \times n$ orthogonal matrix A, construct an $n \times n$ upper triangular matrix R such that

$$H_{n-1} \cdots H_2 H_1 A = R, \tag{1}$$

where

$$H_i = I_n - 2u_i u_i^T, \quad i = 1, 2, \ldots, n-1$$

are $n \times n$ Householder matrices, I_n is the $n \times n$ identity matrix, u_i are unit vectors and $u_i^T u_i = 1$, for $i = 1, 2, \ldots, n-1$. Since the set of $n \times n$ orthogonal matrices is a group under the standard matrix product, we must have $R = \pm I_n$ (the identity $I_n = R^T R$ establishes that R is diagonal with diagonal entries equal to ± 1 [6]). But, if we set $H_n = I_n - 2e_n e_n^T$, then $H_n R = I_n$ and, since each Householder matrix is its own inverse, we obtain from (1) that

$$A = H_1 H_2 \cdots H_n.$$

With this procedure, we have expressed A as the product of n Householder matrices. The method, however does not provide an explicit geometrical procedure to calculate each Householder matrix H_i, $i = 1, 2, \ldots n$, for a given orthogonal matrix A.

In this work the originally posed question is addressed and an explicit geometrical procedure to determine the simple reflections that decompose a given orthogonal transformation is proposed. This in fact constitutes a constructive proof of the Cartan-Dieudonné theorem for the Euclidean space $\mathbb{R}^n$. Our proof produces an algorithm that serves also to generate all the Pythagorean triples and boxes without using number theory.

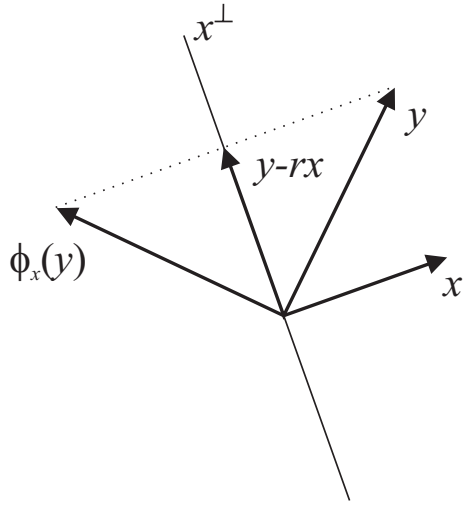

FIGURE 1. Reflection of the vector y through the hyperplane $x^\perp$.

2. Simple Reflections and Rotations

Let us first clarify what we mean by a simple reflection in $\mathbb{R}^n$. Let $x, y \in \mathbb{R}^n$ be two non-zero and non-collinear vectors [1]. Consider the orthogonal complement (hyperplane) of the vector x, defined by

$$x^\perp = \{z \in \mathbb{R}^n \ \mid \ (x, z) = 0\},$$

where $(\cdot, \cdot)$ is the canonical inner product in $\mathbb{R}^n$. The projection of a vector y onto $x^\perp$ (Figure 1) is $y - rx$, where $r \in \mathbb{R}$ is chosen such that $y - rx \in x^\perp$. That is

$$0 = (y - rx, x) = (y, x) - r\,(x, x)\,,$$

thus

$$r = \frac{(x, y)}{\parallel x \parallel^2}.$$

In this way, the reflection of y through the hyperplane $x^\perp$ is called a simple reflection and is given by

$$\phi_x(y) = y - 2rx = y - 2\frac{(x, y)}{\parallel x \parallel^2}x. \tag{2}$$

Note that, if $y \in x^\perp$ then $\phi_x(y) = y$, that is, ϕ_x acts as the identity map on the subspace $x^\perp$.

[1] In what follows, n-dimensional vectors will be denoted by plain letters but bold letters will be used in Sections 5 and 6 to denote vectors in $\mathbb{R}^2$ and $\mathbb{R}^3$.

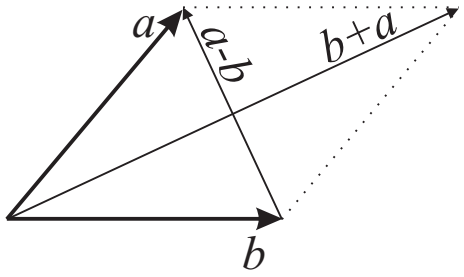

FIGURE 2. Simple reflection of the vector b through the hyperplane $\{a-b\}^{\perp}$.

We can easily check that the inverse of a simple reflection is the reflection itself. Indeed

$$\begin{aligned}\phi_x\left(\phi_x(y)\right) &= \phi_x\left(y-2rx\right),\\ &= y-2rx-2\frac{(x,(y-2rx))}{\parallel x\parallel^2}x,\\ &= y-2rx-2rx+4rx,\\ &= y.\end{aligned}$$

ϕ_x is an orthogonal transformation, as follows from

$$\begin{aligned}\parallel \phi_x\left(y\right)\parallel^2 &= \left(y-2\frac{(x,y)}{\parallel x\parallel^2}x,\ y-2\frac{(x,y)}{\parallel x\parallel^2}x\right),\\ &= (y,y)-4\frac{(x,y)}{\parallel x\parallel^2}\left(x,y\right)+4\frac{(x,y)^2}{\parallel x\parallel^4}\left(x,x\right),\\ &= (y,y),\\ &= \parallel y\parallel^2.\end{aligned}$$

Now, let a,b be non-zero vectors in $\mathbb{R}^n$, such that $a\neq b$ and $\parallel a\parallel=\parallel b\parallel$. If we want to obtain b as a simple reflection of the vector a, we can proceed as follows. Clearly b can be obtained as a simple reflection of a through the hyperplane $(a-b)^{\perp}$ (Figure 2), that is, $\phi_{a-b}(a)=b$. In fact, from (2) we have

$$\begin{aligned}\phi_{a-b}(a) &= a-2\frac{(a,a-b)}{\parallel a-b\parallel^2}(a-b),\\ &= a-\frac{\parallel a\parallel^2-(a,b)}{\parallel a\parallel^2-(a,b)}(a-b),\\ &= a-(a-b)=b,\end{aligned}$$

where we have used that

$$(a,a-b)=\parallel a\parallel^2-(a,b),$$

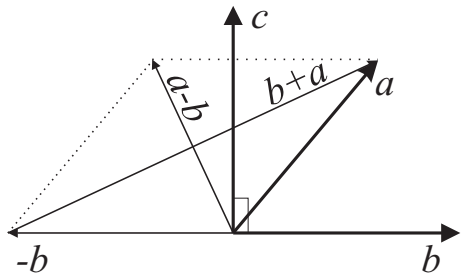

FIGURE 3. Rotation that brings the vector a onto coincidence with vector b.

and

$$\| a - b \|^2 = \| a \|^2 + \| b \|^2 - 2\,(a, b) = 2 \| a \|^2 - 2\,(a, b)\,.$$

If it turns out that $b = -a$, it is required that $\phi_x(a) = -a$ and from (2) we can easily check that $x = a$ and the required reflection is thus $\phi_a = -I$, where I is the identity operation.

With all these results, we can state the following lemma, which shows that simple reflections are primitive orthogonal transformations.

Lemma 1. *Consider the Euclidean space $\mathbb{R}^n$. For any two non-zero vectors a and b in $\mathbb{R}$, such that $a \neq b$ and $\| a \| = \| b \|$, there exists a unique simple reflection ϕ such that $\phi\,(a) = b$.*

Proof. From (2) and the above discussion, we have that the reflection is given by

$$\phi(x) = \begin{cases} \phi_a(x), & \text{if } b = -a, \\ \phi_{a-b}(x), & \text{otherwise.} \end{cases} \tag{3}$$

By construction, since $a \neq b$, the simple reflection is unique. □

Remark 2. *The case $b = a$ is special. Any hyperplane that contains the vector a determines a simple reflection ϕ that satisfies $\phi(a) = a$. Therefore, in general, there are infinitely many different simple reflections that leave a fixed. For this reason, in the remainder of this paper, for the case $b = a$ we will take ϕ as the identity operator instead of taking a simple reflection.*

By applying the previous Lemma twice, it turns out that the composition (product) of two simple reflections (that can be *a priori* called simple rotation) is the next orthogonal transformation to be considered, following the order imposed by the mathematical structure and, possibly, by the cognitive structure of a college student [4].

Let now a and b be two non-zero and non-collinear vectors in $\mathbb{R}^n$ and suppose that we want to obtain b by means of a simple rotation of the vector a. We proceed as follows. Assume that $\| a \| = \| b \|$, then the reflection of a through the

hyperplane $(b+a)^{\perp}$ produces the vector $-b$, which in turn can be reflected through the hyperplane $b^{\perp}$, leading to the vector b (Figure 3). That is

$$\phi_b\left(\phi_{a+b}(a)\right) = b. \tag{4}$$

Indeed, since

$$\begin{aligned} (a, a+b) &= \| a \|^2 + (a, b), \\ \| a+b \|^2 &= 2 \| a \|^2 + 2(a, b), \end{aligned}$$

we have that

$$\begin{aligned} \phi_{a+b}(a) &= a - 2\frac{(a, a+b)}{\| a+b \|^2}(a+b), \\ &= a - \frac{\| a \|^2 + (a, b)}{\| a \|^2 + (a, b)}(a+b), \\ &= a - (a+b), \\ &= -b, \end{aligned}$$

and, finally

$$\begin{aligned} \phi_b(-b) &= -b - 2\frac{(b, -b)}{\| b \|^2}(-b), \\ &= -b + 2b, \\ &= b. \end{aligned}$$

As expected, it can be proved that the simple rotation $\phi_b \circ \phi_{a+b}$, where $\circ$ denotes composition, is also an orthogonal transformation.

In summary, the vector b was obtained by means of either a simple reflection or a simple rotation (the composition of two simple reflections) of the vector a.

Proposition 3. *Consider the Euclidean space $\mathbb{R}^n$. For any two non-zero and non-collinear vectors a and b in $\mathbb{R}^n$, such that $\| a \| = \| b \|$, there exists a simple rotation $R : \mathbb{R}^n \to \mathbb{R}^n$ such that $R(a) = b$.*

Proof. From (3), (4) and the previous discussion, we have that the desired rotation is given by

$$R(x) = \phi_b\left(\phi_{a+b}(x)\right)$$

□

3. A Constructive Proof of the Cartan Theorem

The procedure used to obtain a simple rotation allows us to envisage an algorithm to decompose any given orthogonal transformation as the composition of simple reflections. This is based on the recurrent application of Lemma 1; simple reflections that decompose the orthogonal transformation can be explicitly obtained from (3) as in the procedure that led to Proposition 3. To achieve this, it is enough to adequately select the vectors a and b in (3) at each step of the algorithm. Notice

that all this discussion constitutes Cartan's theorem and therefore a constructive and geometrical proof of this special case can be given:

Theorem 4. *Consider the Euclidean space $\mathbb{R}^n$. Any orthogonal transformation $T : \mathbb{R}^n \to \mathbb{R}^n$ can be decomposed by at most n simple reflections.*

Proof. We will apply Lemma 1 recurrently and, at each step, the vectors a and b, from Equation (3), can be chosen as follows (see Figure 3). Let $T : \mathbb{R}^n \to \mathbb{R}^n$ be an orthogonal transformation and let $\{e_1, e_2, \ldots, e_n\}$ be an orthogonal basis for $\mathbb{R}^n$.

1. First consider $b = e_1$ and $a = T(e_1)$. Since T is an orthogonal transformation, we have $\| a \| = \| b \|$. If $T(e_1) \neq e_1$ then, according to Lemma 1, there exists a simple reflection ϕ_1 given by
$$\phi_1(x) = \begin{cases} \phi_{e_1}(x), & \text{if } \ T(e_1) = -e_1, \\ \phi_{a_1}(x), & \text{otherwise,} \end{cases}$$
where $a_1 = T(e_1) - e_1$, that satisfies $\phi_1(T(e_1)) = e_1$. Since $\phi_1 \circ T$ is an orthogonal transformation, for $i \neq 1$ we have that $\phi_1(T(e_i))$ is orthogonal to $\phi_1(T(e_1)) = e_1$. Therefore
$$\phi_1(T(e_i)) \in \mathcal{L}\{e_2, \ldots, e_n\}, \qquad i = 2, 3, \ldots, n,$$
where $\mathcal{L}\{e_2, \ldots, e_n\}$ stands for the subspace spanned by $\{e_2, \ldots, e_n\}$.

   If it turns out that $T(e_1) = e_1$, then, according to Remark 2 we take ϕ_1 as the identity operator. We will do the same in the corresponding case of subsequent steps of the procedure.
2. Now consider $b = e_2$ and $a = \phi_1(T(e_2))$. If $\phi_1(T(e_2)) \neq e_2$, then, application of Lemma 1 again yields the simple reflection
$$\phi_2(x) = \begin{cases} \phi_{e_2}(x), & \text{if } \ \phi_1(T(e_2)) = -e_2, \\ \phi_{a_2}(x), & \text{otherwise,} \end{cases}$$
where $a_2 = \phi_1(T(e_2)) - e_2$. By construction, ϕ_2 satisfies $\phi_2(\phi_1(T(e_2))) = e_2$. Since $\phi_1 \circ T$ is an orthogonal transformation, we have that $e_1 = \phi_1(T(e_1))$ is orthogonal to $\phi_1(T(e_2))$ and hence $e_1 \in a_2^{\perp}$ and then $\phi_2(e_1) = e_1$. Therefore we have
$$\begin{aligned} \phi_2(\phi_1(T(e_j))) &= e_j, \qquad j = 1, 2, \\ \phi_2(\phi_1(T(e_i))) &\in \mathcal{L}\{e_3, \ldots, e_n\}, \qquad i = 3, \ldots, n. \end{aligned}$$
3. Following with this recurrent application of Lemma 1, we can obtain orthogonal transformations $\phi_1, \phi_2, \ldots, \phi_n$ such that:
$$\begin{aligned} \phi_k(\cdots \phi_2(\phi_1(T(e_j)))) &= e_j, \quad j = 1, 2, \ldots, k, \\ \phi_k(\cdots \phi_2(\phi_1(T(e_i)))) &\in \mathcal{L}\{e_{k+1}, \ldots, e_n\}, \quad i = k+1, \ldots, n. \end{aligned}$$
The orthogonal transformation ϕ_k is given by
$$\phi_k(x) = \begin{cases} \phi_{e_k}(x), & \text{if } \ \phi_{k-1}(\cdots \phi_2(\phi_1(T(e_k)))) = -e_k, \\ \phi_{a_k}(x), & \text{otherwise,} \end{cases}$$

where

$$a_k = \phi_{k-1}\left(\cdots \phi_2\left(\phi_1(T(e_k))\right)\right) - e_k,$$

and ϕ_k is the identity if $a_k = 0$.

Since

$$\phi_n\left(\cdots \phi_2\left(\phi_1(T(e_j))\right)\right) = e_j, \quad j = 1, 2, \ldots, n,$$

it is clear that

$$\phi_n \circ \phi_{n-1} \circ \cdots \circ \phi_2 \circ \phi_1 \circ T = I.$$

Consequently, the orthogonal transformation T can be expressed as the following product of n simple reflections

$$T = \phi_1^{-1} \circ \phi_2^{-1} \circ \cdots \circ \phi_n^{-1} = \phi_1 \circ \phi_2 \circ \cdots \circ \phi_n. \qquad \square$$

Definition 5. *If the number of reflections that decompose a given orthogonal transformation is even (odd) then the transformation is a rotation (reflection).*

Theorem 4 gives an answer to the general question originally stated. As it was shown, the simple reflections that decompose a given orthogonal transformation are obtained by applying (3) recurrently. We can easily convince ourselves that after the first two steps of this recurrent procedure, the algebra may become cumbersome (just try to obtain the expression for a simple rotation). A great simplification can be obtained by using the framework of Clifford algebras[2], mainly because the algebraic properties of these algebras provide us with a convenient way of representing reflections and rotations [8]. In what follows, we briefly introduce Clifford algebras.

4. Orthogonal Transformations with Clifford Algebras

One of the most simple and direct ways to define a Clifford algebra is by making use of their generators [9].

Definition 6. *The real associative and distributive algebra generated by the Euclidean space $\mathbb{R}^n$ with the product rules*

$$\begin{aligned} e_i^2 &= 1, \quad i = 1, 2, \ldots, n, \\ e_i e_j + e_j e_i &= 0, \quad i \neq j, \end{aligned} \tag{5}$$

where $\{e_1, e_2, \ldots, e_n\}$ is the canonical basis of $\mathbb{R}^n$, is called universal Clifford algebra of the space $\mathbb{R}^n$ and is denoted by $\mathbb{R}_n$.

As a real vector space, the dimension of $\mathbb{R}_n$ is 2^n. A basis consists of the identity 1 and all vector products of the form $e_1^{m_1} \cdots e_n^{m_n}$, where $m_i = 0$ or 1. The elements $e_1 e_2 \cdots e_k$ are called k-vectors, and linear combinations of k-vectors are called multivectors.

[2]The constructive proof of Theorem 4 was envisaged when we revisited this theorem by using Clifford algebras.

Proposition 7. *If $x, y \in \mathbb{R}^n$ then $x^2 \geq 0$ and $xy + yx \in \mathbb{R}$. Even more*

$$\begin{aligned} x^2 &= (x, x) \\ \frac{xy + yx}{2} &= (x, y)\,. \end{aligned} \tag{6}$$

Proof. It is enough to write x and y in terms of the canonical basis $\{e_1, e_2, \ldots, e_n\}$ and use Equation (5). □

The previous proposition establishes the relationship between the canonical scalar product in $\mathbb{R}^n$ and the so-called geometric product of the algebra $\mathbb{R}_n$.

In a Clifford algebra the inverse of a nonzero vector can be defined [9]. In particular, the inverse of any vector $x \in \mathbb{R}^n$, $x \neq 0$, is given by

$$x^{-1} = \frac{x}{x^2} = \frac{x}{\| x \|^2}. \tag{7}$$

The geometric product relates algebraic operations with geometric properties. In particular, the following important geometric relationships hold

$$\begin{aligned} xy &= yx \Longleftrightarrow x \parallel y \\ xy &= -yx \Longleftrightarrow x \perp y. \end{aligned}$$

That is, parallel vectors commute under the geometric product and perpendicular vectors anticommute.

As mentioned above, Clifford algebras provide us with a convenient way of representing reflections and rotations. In particular, simple reflections are obtained by geometric products between vectors belonging to $\mathbb{R}^n$.

Lemma 8. *The simple reflection $\phi_x : \mathbb{R}^n \to \mathbb{R}^n$ given by (2) can be written as*

$$\phi_x(y) = -xyx^{-1}.$$

Proof. From (2), and using (6) and (7), we have:

$$\begin{aligned} \phi_x(y) &= y - 2\frac{(x, y)}{x^2}x, \\ &= y - \frac{xy + yx}{x^2}x, \\ &= y - (xy + yx)\,x^{-1} \\ &= -xyx^{-1}. \end{aligned}$$

□

As in Proposition 3, the simple rotation of two unitary vectors in $\mathbb{R}^n$ can be also obtained.

Proposition 9. *Consider any two non-zero and non-collinear vectors a and b in $\mathbb{R}^n$, such that $a^2 = b^2 = 1$. The simple rotation $R : \mathbb{R}^n \to \mathbb{R}$, that brings the vector a onto coincidence with the vector b is given by:*

$$R(x) = \frac{(1 + ba)\,x\,(1 + ab)}{2\,(1 + (a, b))}.$$

Proof. From Lemma 8 and (4), we know that

$$\begin{aligned} R(x) &= \phi_b\left(\phi_{a+b}(x)\right) \\ &= b(a+b)x(a+b)^{-1}b^{-1}. \end{aligned}$$

The desired result readily follows from (6) and the following identities

$$\begin{aligned} b(1+ba) &= (1+ba)a, \\ a(1+ab) &= (1+ab)b, \\ (1+ba)^2 &= (1+ab)^2 = 2(1+(a,b)). \end{aligned}$$

□

From the recurrent application of Lemma 8, we have that any orthogonal transformation $T : \mathbb{R}^n \to \mathbb{R}^n$ can be decomposed as

$$T(x) = (-1)^n \left(\prod_{i=1}^{n} a_i\right) x \left(\prod_{i=1}^{n} a_i\right)^{-1}, \tag{8}$$

where the vectors a_i were derived in the proof of Theorem 4.

Thus, in the framework of Clifford algebras, Cartan's theorem (Theorem 4) can be rewritten as

Theorem 10. *In the Euclidean space $\mathbb{R}^n$, any orthogonal transformation $T : \mathbb{R}^n \to \mathbb{R}^n$ can be decomposed as in* (8)*. The decomposition is given with respect to an orthogonal basis $\{u_1, u_2, \ldots, u_n\}$ of $\mathbb{R}^n$, and the vectors a_i are given by*

$$a_i = (-1)^i a_{i-1} \cdots a_2 a_1 b_i a_1^{-1} a_2^{-1} \cdots a_{i-1}^{-1} - u_i,$$

where $b_i = T(u_i)$, $i = 2, \ldots, n$, and

$$a_1 = T(u_1) - u_1.$$

5. Pythagorean Triples

Some of the results obtained in the previous section can be used to find the solutions of the Diophantine equation generated by the Pythagorean theorem. That is, find the integers (Pythagorean triples) x, y and z that satisfy

$$x^2 + y^2 = z^2. \tag{9}$$

If $x, y, z > 0$ this problem is geometrically equivalent to finding all the right-angled triangles with integer sides. A solution based on number theory is presented in [10], pp. 437-42.

A Pythagorean triple can be conceived as a vector $\mathbf{x} = (x/z, y/z) \in \mathbb{Z}^2$ such that

$$x^2 + y^2 = z^2, \qquad x, y, z \in \mathbb{Z}, \quad \| \mathbf{x} \| = 1.$$

Let $\{\mathbf{e}_1, \mathbf{e}_2\}$ be an orthonormal basis of $\mathbb{Z}^2$. By Proposition 9, there exists a simple rotation R such that

$$R(\mathbf{y}) = \frac{(1 + \mathbf{x}\mathbf{e}_1)\,\mathbf{y}\,(1 + \mathbf{e}_1\mathbf{x})}{2\,(1 + (\mathbf{x}, \mathbf{e}_1))},$$

which satisfies $R(\mathbf{e}_1) = \mathbf{x}$. Thus, the orthogonal matrix associated to the Pythagorean triple is:

$$\begin{aligned}[R(\mathbf{e}_1), R(\mathbf{e}_2)] &= \begin{pmatrix} \frac{x}{z} & \frac{-2(x+z)z^2y}{2z^3(x+z)} \\ \\ \frac{y}{z} & \frac{2z^2x(x+z)}{2z^3(x+z)} \end{pmatrix}, \\ &= \begin{pmatrix} \frac{x}{z} & -\frac{y}{z} \\ \\ \frac{y}{z} & \frac{x}{z} \end{pmatrix}, \end{aligned} \tag{10}$$

where we use the fact that $\| \mathbf{x} \| = 1$.

On the other hand, since the above orthogonal matrix has rational entries (with respect to the canonical basis) we can apply some properties of coincidence isometries, since such isometries are described by orthogonal matrices with rational entries [11]. In particular, we have:

Theorem 11. *Let $R : \mathbb{R}^2 \to \mathbb{R}^2$ be a non trivial orthogonal transformation. If the matrix representation of R with respect to the canonical basis $\{\mathbf{e}_1, \mathbf{e}_2\}$ has rational entries, then there exists a vector $\mathbf{a} = (\alpha, \beta) \in \mathbb{Z}^2$, with $gcd(\alpha, \beta) = 1$, such that*

$$R(\mathbf{x}) = \mathbf{a}\mathbf{e}_2\mathbf{x}\mathbf{e}_2\mathbf{a}^{-1}.$$

For a proof see [11], Prop. 5. The matrix associated with the orthogonal transformation in the previous theorem is thus

$$[R(\mathbf{e}_1), R(\mathbf{e}_2)] = \begin{pmatrix} \frac{\beta^2-\alpha^2}{\alpha^2+\beta^2} & \frac{2\alpha\beta}{\alpha^2+\beta^2} \\ \\ -\frac{2\alpha\beta}{\alpha^2+\beta^2} & \frac{\beta^2-\alpha^2}{\alpha^2+\beta^2} \end{pmatrix}.$$

Direct comparison with (10) yields

$$\begin{pmatrix} \frac{x}{z} & -\frac{y}{z} \\ \\ \frac{y}{z} & \frac{x}{z} \end{pmatrix} = \begin{pmatrix} \frac{\beta^2-\alpha^2}{\alpha^2+\beta^2} & \frac{2\alpha\beta}{\alpha^2+\beta^2} \\ \\ -\frac{2\alpha\beta}{\alpha^2+\beta^2} & \frac{\beta^2-\alpha^2}{\alpha^2+\beta^2} \end{pmatrix}.$$

Since x, y, z is an arbitrary Pythagorean triple, what we have found is that any Pythagorean triple must be of the form $\left(\beta^2 - \alpha^2, -2\alpha\beta, \alpha^2 + \beta^2\right)$. Thus, we can state the following theorem:

Theorem 12. *The integers x, y and z form a Pythagorean triple if and only if there exist positive integers α and β, relatively prime, such that*

$$\begin{aligned} x &= \beta^2 - \alpha^2 \\ y &= -2\alpha\beta \\ z &= \alpha^2 + \beta^2. \end{aligned}$$

Substitution of these equations in (9) shows that x, y and z form a Pythagorean triple.

6. Pythagorean Boxes

The procedure described in the previous section can be generalized to find Pythagorean boxes [12], that is vectors $\mathbf{x} = (x/w, y/w, z/w) \in \mathbb{Z}^3$ such that

$$x^2 + y^2 + z^2 = w^2, \quad x, y, z, w \in \mathbb{Z}, \quad \| \mathbf{x} \| = 1. \tag{11}$$

All Pythagorean boxes can be obtained from the following

Theorem 13. *The integers x, y, z and w form a Pythagorean box if and only if there exist integers $\alpha, \beta, \gamma, \delta$ and ϵ, that are pairwise relatively prime, such that*

$$\begin{array}{rcl} x & = & -\alpha^2 + \gamma^2 + \beta^2, \\ y & = & -2\alpha\beta, \\ z & = & -2\alpha\gamma, \\ w & = & \alpha^2 + \gamma^2 + \beta^2, \end{array} \tag{12}$$

or

$$\begin{array}{rcl} x & = & 2\alpha(2\gamma\delta\epsilon + \beta(\delta - \epsilon)(\delta + \epsilon)), \\ y & = & 4\beta\gamma\delta\epsilon - \left(-\alpha^2 + \gamma^2 + \beta^2\right)(\delta - \epsilon)(\delta + \epsilon), \\ z & = & \pm 2\left(\left(-\alpha^2 + \gamma^2 + \beta^2\right)\delta\epsilon - \beta\gamma(\delta - \epsilon)(\delta + \epsilon)\right), \\ w & = & \left(\alpha^2 + \gamma^2 + \beta^2\right)\left(\delta^2 + \epsilon^2\right). \end{array} \tag{13}$$

Proof. Let $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$ be an orthonormal basis for $\mathbb{Z}^3$ and let $\mathbf{x} = \left(\frac{x}{w}, \frac{y}{w}, \frac{z}{w}\right) \in \mathbb{Z}^3$ such that

$$x^2 + y^2 + z^2 = w^2, \qquad x, y, z, w > 0, \quad \| \mathbf{x} \| = 1.$$

We have to prove that there exist two vectors with integer entries $\mathbf{a} = (\alpha, \beta, \gamma)$, and $\mathbf{b} = (0, \delta, \epsilon)$ in $\mathbb{Z}^3$, where $\gcd(\alpha, \beta, \gamma) = 1$ and $\gcd(\delta, \epsilon) = 1$, such that

$$R(\mathbf{y}) = \mathbf{a}\mathbf{b}\mathbf{y}\mathbf{b}^{-1}\mathbf{a}^{-1}. \tag{14}$$

Indeed, from Proposition 9 we have

$$R(\mathbf{y}) = \frac{(1 + \mathbf{x}\mathbf{e}_1)\,\mathbf{y}\,(1 + \mathbf{e}_1\mathbf{x})}{2\,(1 + (\mathbf{x}, \mathbf{e}_1))},$$

and by the algorithm used in the proof of Theorem 4 (the Cartan theorem), we can generate $\alpha, \beta, \gamma, \delta$ and ϵ, as follows.

First consider

$$\mathbf{a}_1 = R(\mathbf{e}_1) - \mathbf{e}_1 = \left(\frac{x - w}{w}, y, z\right) = \frac{1}{w}(x - w, y, z).$$

By defining $\mathbf{a}_1' = w\mathbf{a}_1$, we can choose $\mathbf{a} = (\alpha, \beta, \gamma)$, where

$$\alpha = \frac{x - w}{\gcd(x - w, y, z)}; \quad \beta = \frac{y}{\gcd(x - w, y, z)}; \quad \gamma = \frac{z}{\gcd(x - w, y, z)}.$$

Now, proceeding as in the second step of the proof of Theorem 4, consider

$$\mathbf{a}_2 = \mathbf{a}_1 R(\mathbf{e}_2)\mathbf{a}_1^{-1} - \mathbf{e}_2 = \left(0, \frac{-2z^2}{y^2 + z^2}, \frac{2yz}{y^2 + z^2}\right) = \frac{2}{y^2 + z^2}(0, -z^2, yz).$$

In a similar way, if we define $\mathbf{a}_2' = \frac{y^2+z^2}{2}\mathbf{a}_2$ then $\mathbf{b} = (0, \delta, \epsilon)$, where

$$\delta = \frac{-z^2}{\gcd(z^2, yz)}, \qquad \epsilon = \frac{yz}{\gcd(z^2, yz)}.$$

Clearly, $\mathbf{a}$ and $\mathbf{b}$ satisfy (14) and thus, finally, with the columns of the matrix associated with this rotation

$$[R(\mathbf{e}_1), R(\mathbf{e}_1), R(\mathbf{e}_1)]\,,$$

we obtain (12) and (13).

Now let $\mathbf{a} = (\alpha, \beta, \gamma)$, $\mathbf{b} = (0, \delta, \epsilon) \in \mathbb{Z}^3$, where $\gcd(\alpha, \beta, \gamma) = 1$ and $\gcd(\delta, \epsilon) = 1$, that fulfill equations (12) and (13). A straightforward computation shows that x, y, z, w form a Pythagorean box. □

Note that this theorem extends to Prop. 5 of [11]. Note also that this theorem can be easily extended to $\mathbb{R}^n$.

References

[1] E. Cartan, *La Théorie des Spineurs I, II*. Actualités Scientifiques et Industrielles, No. 643. Hermann, Paris, 1938.

[2] J. Dieudonné, *Sur les Groupes Classiques*. Actualités Scientifiques et Industrielles, No. 1040. Hermann, Paris, 1948.

[3] E. Artin, *Geometric Algebra*. Wiley-Interscience, New York, 1988.

[4] J. C. Moyer, *The relationship between the mathematical structure of euclidean transformations and the spontaneously developed cognitive structures of young children*. J. Res. Math. Educ. **9** (1978), 83-92.

[5] L. Rudolph, *The structure of orthogonal transformations*. Amer. Math. Monthly **98** (1991), 349-52.

[6] F. Uhlig, *Constructive ways for generating (generalized) real orthogonal matrices as products of (generalized) symmetries*. Linear Algebra Appl. **332-334** (2001), 459-67.

[7] J. Gallier, *Geometric Methods and Applications*. Springer-Verlag, New York, 2001.

[8] R. González Calvet, *Treatise of plane geometry through geometric algebra*. Electronic edition, available at http://www.xtec.es/ ˜rgonzal1/treatise-a.pdf, 27, 28 and 57, Chapters 4 and 6.

[9] I. Porteous, *Clifford algebras and the classical groups*. Cambridge University Press, Cambridge, 1995.

[10] K. H. Rosen, *Elementary Number Theory and its applications*, Third edition, Addison-Wesley, 2004.

[11] M. A. Rodríguez, J. L. Aragón and L. Verde-Star, *Clifford algebra approach to the coincidence problem for planar lattices*. Acta Cryst. **A61** (2005), 173-184.

[12] R. A. Beauregard and E. R. Suryanarayan, *Pythagorean boxes*. Math. Mag. **74** (2001), 222-227.

Acknowledgments

This work has been partially supported by the Program for the Professional Development in Automation (grant from the Universidad Autónoma Metropolitana and Parker Haniffin-México), by DGAPA-UNAM (grant IN-117806), CONACyT (grant 50368), MCYT-Spain (grant FIS2004-03237) and COFAA-IPN.

G. Aragón-González
Programa de Desarrollo Profesional en Automatización
Universidad Autónoma Metropolitana, Azcapotzalco
San Pablo 180, Colonia Reynosa-Tamaulipas
02200 D. F. México
México
e-mail: gag@correo.azc.uam.mx

J.L. Aragón
Centro de Física Aplicada y Tecnología Avanzada
Universidad Nacional Autónoma de México
Apartado Postal 1-1010, 76000 Querétaro
México
e-mail: aragon@fata.unam.mx

M.A. Rodríguez-Andrade
Departamento de Matemáticas
Escuela Superior de Física y Matemáticas
Instituto Politécnico Nacional
Unidad Profesional Adolfo López Mateos, Edificio 9
07300 D. F. México
México
e-mail: marco@polaris.esfm.ipn.mx

L. Verde-Star
Departamento de Matemáticas
Universidad Autónoma Metropolitana, Unidad Iztapalapa
Apartado Postal 55–534
09340 D. F. México
México
e-mail: verde@star.izt.uam.mx

Received: April 25, 2008.
Accepted: June 2, 2008.