MATRIX GENERATION OF PYTHAGOREAN $n$-TUPLES

DANIEL CASS AND PASQUALE J. ARPAIA

(Communicated by William Adams)

Abstract. We construct, for each $4 \leq n \leq 9$, a matrix $A_n$ which generates all the primitive Pythagorean $n$-tuples $(x_1, \ldots, x_n)$ with $x_n > 1$

\[(1) \quad x_1^2 + \cdots + x_{n-1}^2 = x_n^2, \quad \gcd(x_1, \ldots, x_n) = 1\]

from the single $n$-tuple $(1, 0, \ldots, 0, 1)$. Once a particular $n$-tuple is generated, one permutes the first $n-1$ coordinates and/or changes some of their signs, and applies $A_n$ to obtain another $n$-tuple. This extends a result of Barning which presents an appropriate matrix $A_3$ for the Pythagorean triples. One cannot so generate the Pythagorean $n$-tuples if $n > 10$; in fact we show the Pythagorean $n$-tuples fall into at least $\lfloor (n + 6)/8 \rfloor$ distinct orbits under the automorphism group of (1).

Call an $n$-tuple $x = (x_1, \ldots, x_n)$ of integers ($n \geq 3$) Pythagorean if

\[(1) \quad x_1^2 + \cdots + x_{n-1}^2 = x_n^2, \quad \gcd(x_1, \ldots, x_n) = 1\]

and primitive provided $\gcd(x_1, \ldots, x_n) = 1$. In what follows, all Pythagorean $n$-tuples are implicitly primitive, and when $x$ postmultiplies an $n \times n$ matrix it will be regarded as a column vector. Let $Z_n$ denote the quadratic space of the form (1), consisting of $n$-tuples of integers with inner product $x \cdot y = x_1y_1 + \cdots + x_{n-1}y_{n-1} - x_ny_n$. Then $x$ is Pythagorean when $x \cdot x = 0$.

For a particular Pythagorean $n$-tuple $x_0$, by $S(x_0)$ we mean the set of solutions $x$ of (1) which are associated to $x_0$ in the sense that $x$ is obtained from $x_0$ by permuting the first $n-1$ coordinates of $x_0$ and/or changing some of their signs. For example, if $n = 3$ and $x_0 = (3, 4, 5)$, then $S(x_0)$ contains eight elements $(\pm 3, \pm 4, 5)$, $(\pm 4, \pm 3, 5)$.

It follows from a result of Barning [B] that the matrix

\[
A_3 = \begin{bmatrix}
1 & 2 & 2 \\
2 & 1 & 2 \\
2 & 2 & 3 \\
\end{bmatrix}
\]

has the following property: For any Pythagorean 3-tuple $x$ with $x_3 > 1$, there is a sequence $(1, 0, 1) = w_0, w_1, \ldots, w_m = x$ of Pythagorean 3-tuples where for $0 \leq i \leq m - 1$, the matrix $A_3$ carries some element of $S(w_i)$ to some

Received by the editors February 23, 1989 and, in revised form, May 20, 1989.
1980 Mathematics Subject Classification (1985 Revision). Primary 10B05.

©1990 American Mathematical Society
0002-9939/90 $1.00 + .25$ per page

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
element of \( S(w_{i+1}) \). In this sense the matrix \( A_3 \) can be said to generate all the Pythagorean 3-tuples.

Consider the quadratic space \( Z_3 \) of the form

\[(2) \quad x_1^2 + x_2^2 - x_3^2.\]

In this space, reflection in the 3-tuple \((1, 1, 1)\) (of norm \( N = (1, 1, 1) \cdot (1, 1, 1) = 1 \)) may be computed by the usual formula

\[(x, y, z) \rightarrow (x, y, z) - (2/N)[(x, y, z) \cdot (1, 1, 1)](1, 1, 1);\]

in matrix form this reflection is

\[A_3' = \begin{bmatrix}
-1 & -2 & 2 \\
-2 & -1 & 2 \\
-2 & -2 & 3
\end{bmatrix}.\]

When this is postmultiplied by the matrix

\[B = \begin{bmatrix}
-1 & 0 & 0 \\
0 & -1 & 0 \\
0 & 0 & 1
\end{bmatrix}\]

one obtains Barning’s matrix \( A_3 \). Note that \( A_3' \) works as well as \( A_3 \) to generate the Pythagorean 3-tuples, since \((A_3'B)x = A_3'(Bx)\), and \(Bx\) amounts to changing signs on \(x_1\) and \(x_2\).

The matrix \( G \) of the form (2) is diagonal with diagonal entries \(1, 1, -1\); since \( A_3'G A_3 = G \) we have that \( A_3 \) is an automorphism of (2). \( A_3' \) is also an automorphism of (2) since it is the matrix of a reflection.

Now permutation of \(x_1\) and \(x_2\), and the maps which multiply an \(x_i\) by \(-1\) \((i = 1, 2)\), are also automorphisms of (2). In this terminology Barning’s result implies that the automorphism group of the form (2) (consisting of linear norm-preserving isomorphisms of the inner product space \( Z_3 \)) acts transitively on its zero set. Our results will establish that for \(4 \leq n \leq 9\) the form \( x_1^2 + \cdots + x_{n-1}^2 - x_n^2 \) also has its automorphism group acting transitively on its zero set, but that for \(n \geq 10\) the zero set falls into at least \([(n + 6)/8]\) orbits.

**Theorem 1.** For \(4 \leq n \leq 9\) let \( A_n \) denote the matrix associated with reflection in the \(n\)-tuple \((1, 1, 1, 0, \ldots, 0, 1)\), in the quadratic space of (1):

\[
A_n = \begin{bmatrix}
0 & -1 & -1 & 0 & 1 \\
-1 & 0 & -1 & 0 & 1 \\
-1 & -1 & 0 & 1 & 0 \\
0 & \ddots & \ddots & \ddots & 0 \\
-1 & -1 & -1 & 0 & 2
\end{bmatrix}
\]
Then if $x$ is any Pythagorean $n$-tuple with $x_n > 1$ there is a sequence

$$(1, 0, \ldots, 0, 1) = w_0, w_1, \ldots, w_m = x$$

of Pythagorean $n$-tuples where, for $0 \leq i \leq m - 1$, $A_n$ carries some element of $S(w_i)$ to some element of $S(w_{i+1})$.

**Proof.** Since it is the matrix of a reflection, $A_n$ preserves the form (1) and in particular carries Pythagorean $n$-tuples to Pythagorean $n$-tuples, and $A_n$ is self-inverse. Let $y$ be any Pythagorean $n$-tuple with $y_n \geq 2$ and pick $x$ in $S(y)$ with $x_1 \geq x_2 \geq \cdots \geq x_{n-1} \geq 0$. Put $z = A^{-1}_n x$. The theorem is established (by induction on the $n$th coordinate) if we show that $0 < z_n < x_n$, since to a sequence $w_0, \ldots, w_m$ for $z$, we may append $w_{m+1} = y$ to obtain a sequence for $y$.

Now $0 < z_n$ means that $x_1 + x_2 + x_3 < 2x_n$. Interpreting the variables as real, the maximum of $x_1 + x_2 + x_3$ subject to the constraint $x_1^2 + x_2^2 + x_3^2 = C^2 \leq x_n^2$ occurs when $x_1 = x_2 = x_3 = C/\sqrt{3}$, for which $x_1 + x_2 + x_3 = \sqrt{3}C$. Thus we have $x_1 + x_2 + x_3 < \sqrt{3}x_n < 2x_n$.

It remains to show $z_n < x_n$, which is $x_1 + x_2 + x_3 > x_n$. On squaring both sides of this and subtracting the relation (1) we obtain the equivalent inequality

$$(3)\quad 2x_1x_2 + 2x_1x_3 + 2x_2x_3 > x_4^2 + \cdots + x_{n-1}^2.$$

Since $x_n = y_n \geq 2$ and $x_1 \geq x_2 \geq \cdots \geq x_n$ we have $x_1x_2 > 0$. So if $n = 4$ we are done, since the right of (3) is 0 and the left positive. Otherwise there are, since $5 \leq n \leq 9$, at most five variables on the right of (3). Now $x_i x_j \geq x_h^2$ for any indices $i, j, h$ satisfying $1 \leq i < j < 3$, $4 \leq h \leq n - 1$. This gives

$$x_1x_2 + 2x_1x_3 + 2x_2x_3 \geq x_4^2 + \cdots + x_{n-1}^2.$$

Since $x_1x_2 > 0$ we have strict inequality in (3). \(\square\)

Consider now the quadratic space $Z_n$ of (1). For an $n$-tuple $a$ in this space, let $C(a)$ denote its orthogonal complement

$$C(a) = \{b|a \cdot b = 0\}.$$

$C(a)$ is called even provided that $x \cdot x$ is even for all $x \in C(a)$; otherwise $C(a)$ is odd. For any automorphism $T$ of (1) we have that $C(a)$ is even if and only if $C(Ta)$ is even. Now if $a = (1, 0, \ldots, 0, 1)$, $C(a)$ is clearly odd. However, we have the following:

**Lemma 1.** Let $a$ be any $n$-tuple in $Z_n$ with each $a_i$ odd. Then $C(a)$, the orthogonal complement of $a$ in $Z_n$, is even.

**Proof.** Let $b \in C(a)$ so that $b$ satisfies

$$a_1b_1 + a_2b_2 + \cdots + a_{n-1}b_{n-1} - a_nb_n = 0.$$

Since the $a_i$ are odd, modulo 2 this reads

$$b_1 + b_2 + \cdots + b_{n-1} - b_n \equiv 0$$
and since \( x^2 \equiv x \pmod{2} \) this implies that
\[
b_1^2 + b_2^2 + \cdots + b_{n-1}^2 - b_n^2 \equiv 0 \pmod{2},
\]
that is, \( b \cdot b \) is an even integer as required. \( \square \)

This shows immediately why we cannot generate the Pythagorean 10-tuples with some matrix \( A_{10} \) preserving the form (1) with \( n = 10 \). For in this case we have the 10-tuple \( a_1 = (1, 1, \ldots, 1, 3) \), which is Pythagorean and by Lemma 1 has even orthogonal complement. Hence no automorphism of (1) can carry the Pythagorean 10-tuple \( a_0 = (1, 0, \ldots, 0, 1) \) to \( a_1 \).

In fact, there are Pythagorean \( n \)-tuples with all coordinates odd whenever \( n = 8k + 2 \). (Note that \( n \) must be of this form for there to be such \( n \)-tuples, since the square of an odd number is 1 modulo 8.) We give an explicit list of such \( n \)-tuples here for later use:

\[
a_0 = (1) \ast 1, \ 1 \\
a_1 = (9) \ast 1, \ 3 \\
a_2 = (16) \ast 1, \ (1) \ast 3, \ 5 \\
a_3 = (25) \ast 1, \ 5 \\
a_4 = (31) \ast 1, \ (2) \ast 3, \ 7 \\
a_5 = (40) \ast 1, \ (1) \ast 3, \ 7 \\
a_6 = (49) \ast 1, \ 7 \\
\vdots
\]

In this list the notation \((m) \ast 1, (n) \ast 3, \ p\) means a tuple consisting of \( m \) 1's followed by \( n \) 3's with last coordinate \( p \). This gives a Pythagorean tuple as long as \( m + 9n = p^2 \). When the subscript \( k \) is of the form \( r(r+1)/2 \) the tuple \( a_k \) is \((m) \ast 1, \ p\), where \( m = (2r+1)^2 \) and \( p = 2r+1 \). Between subscripts \((r-1)r/2 \) and \( r(r+1)/2 \), the tuple \( a_{k-j} \) \((1 \leq j \leq r-1)\) is \((m) \ast 1, (n) \ast 3, \ p\) with \( m = (2r+1)^2 - 9j \), \( n = j \), \( p = 2r+1 \). Since \((2r+1)^2 - 9(r-1) > 0\), the coefficient \( m \) remains positive, and \( a_{k-j} \) satisfies \( m + 9n = p^2 \) and so is Pythagorean. Note that each tuple \( a_k \) in (4) has \( m+n+1 = 8k+2 \) coordinates and is a Pythagorean tuple with all coordinates odd.

Lemma 1 together with the list (4) shows that we cannot generate the Pythagorean \( n \)-tuples when \( n = 8k + 2 \) \((k \geq 1)\) from the single \( n \)-tuple \((1, 0, \ldots, 0, 1)\).

If \( n \) is fixed and \( k \geq 0 \) satisfies \( 8k + 2 \leq n \), then we define an \( n \)-tuple \( a'_k \) to coincide with \( a_k \) in the first \( 8k + 1 \) coordinates, to have as \( n \)th coordinate the last coordinate of \( a_k \) and remaining coordinates all 0. There are, for given \( n \), \([(n+6)/8]\) of these \( n \)-tuples \( a'_k \).

**Theorem 2.** Suppose \( a_s \) and \( a_t \) \((s < t)\) are any two Pythagorean tuples on the list (4) and \( n \) is at least \( 8t + 2 \). Then there is no automorphism of (1) carrying \( a_s \) to \( a_t \). Thus the Pythagorean \( n \)-tuples cannot be generated from the single
n-tuple \((1, 0, \ldots, 0, 1)\) by means of any matrix \(A_n\) of an automorphism of \((1)\).

**Proof.** First let \(a\) be any Pythagorean \(n\)-tuple \((a_n > 0)\), with orthogonal complement \(C(a)\). We claim that any element of \(C(a)\) has nonnegative norm, and the only elements of \(C(a)\) having zero norm are the multiples \(ka\), \(k \in \mathbb{Z}\). This follows easily from the following identity, true for \(x\) with \(a \cdot x = 0\):

\[
\sum_{i=1}^{n-1}(a_n x_i - a_i x_n)^2 = a_n^2(x_1^2 + \cdots + x_{n-1}^2 - x_n^2).
\]

That \(x \cdot x \geq 0\) for \(x \in C(a)\) is immediate from (5). If \(x \cdot x = 0\) the left of (5) is 0 from which \(a_n x_i = a_i x_n\) for \(1 \leq i \leq n - 1\). This also holds for \(n\) so that

\[
\gcd(a_n x_1, \ldots, a_n x_n) = \gcd(a_i x_1, \ldots, a_n x_n).
\]

Since \(a\) is primitive, \(\gcd(a_1, \ldots, a_n) = 1\) so that

\[
a_n \gcd(x_1, \ldots, x_n) = \pm x_n.
\]

So with \(k = \pm \gcd(x_1, \ldots, x_n)\) we have \(x_n = ka_n\), and then from \(a_n x_i = a_i x_n\) \((1 \leq i \leq n - 1)\) we have \(x = ka\) as claimed.

Now call \(V_s\) the orthogonal complement of \(a_s\) in \(Z_{8s+2}\), and call \(W_s\) the orthogonal complement of \(a'_s\) in \(Z_n\). Then \(W_s\) is in a natural way the orthogonal direct sum of \(V_s\) and a quadratic space \(E_s\) associated with the form

\[
y_1^2 + \cdots + y_r^2
\]

where \(r = r(s) = n - (8s + 2)\). Suppose \(z \in W_s\) and \(z \cdot z = 1\). Write \(z = v + e\) with \(v \in V_s\), \(e \in E_s\). Then \(z \cdot z = v \cdot v + e \cdot e\). Now \(v \cdot v\) is nonnegative, and even by Lemma 1. And \(e \cdot e\) is also nonnegative, so that we must have \(v \cdot v = 0\) and \(v\) some multiple \(k(z)\) of \(a_s\).

Then \(e \cdot e = 1\) forces \(e\) to be one of the (up to sign) \(r(s)\) elements of \(E_s\) having norm 1, say \(e = e(z)\). So any element \(z\) of \(W_s\) of norm 1 has a unique expression

\[
z = k(z)a_s + e(z) \quad (e(z) \in E_s, \ e(z) \cdot e(z) = 1).
\]

We claim now that the maximal number of mutually orthogonal unit vectors in \(W_s\) is exactly \(r(s) = n - (8s + 2)\). Clearly there are at least that many; if there were more, then since up to sign there are only \(r(s)\) possibilities for \(e(z)\) on the right of (6), two of them, \(z\) and \(z'\) would have \(e(z) = \pm e(z')\), and then

\[
z \cdot z' = (k(z)a_s + e(z)) \cdot (k(z')a_s + e(z')) = \pm 1,
\]

contradicting orthogonality of \(z\) and \(z'\).

This proves the theorem, since the number \(r(s) = n - (8s + 2)\) has been shown to be an invariant of \(a'_s\), namely the maximal number of mutually orthogonal unit vectors in \(C(a'_s)\).

In the cases \(4 \leq n \leq 10\) it is known [W] that the automorphism group \(G_n\) of the form \((1, 1, 1, 0, \ldots, 0, 1)\) is generated by the reflection in \((1, 1, 1, 0, \ldots, 0, 1)\) (which in
matrix form is the $A_n$ of Theorem 1) together with the trivial automorphisms which permute the first $n - 1$ coordinates or change signs on some of the $n$ coordinates. The matrix $A_n$ of Theorem 1 generates the Pythagorean $n$-tuples from $(1, 0, \ldots, 0, 1)$ only for $4 \leq n \leq 9$. We point out here that the matrix $A_{10}$ nonetheless works to generate the Pythagorean 10-tuples, provided we use the two initial 10-tuples

$$a_0 = (1, 0, \ldots, 0, 1)$$
$$a_1 = (1, 1, \ldots, 1, 3)$$

in the process. To put this another way, the orbits of $a_0$ and $a_1$ under $G_{10}$ (which are distinct by Theorem 2) in fact together exhaust the Pythagorean 10-tuples.

To see this, note that (in the notation of the proof of Theorem 2) we still have $0 < z_n$, and now $z_n \leq x_n$ is equivalent to

$$2x_1x_2 + 2x_1x_3 + 2x_2x_3 \geq x_4 + \cdots + x_9. \tag{7}$$

That (7) holds follows from the inequality $x_i x_j \geq x_h^2$, true here when $1 \leq i < j \leq 3$, $4 \leq h \leq 9$, there being now six variables on the right of (7). Thus application of $A_{10}$ to a Pythagorean 10-tuple never increases the last coordinate.

Now suppose $x$ is a Pythagorean 10-tuple with $x_1 \geq x_2 \geq \cdots \geq x_9 \geq 0$ and $x_{10} > 0$ for which (7) holds with equality. This gives two lists

(a) $x_1 x_2 \ x_1 x_3 \ x_1 x_4 \ x_2 x_3 \ x_2 x_4 \ x_3 x_4$

(b) $x_4 x_5 \ x_5 x_6 \ x_6 x_7 \ x_7 x_8 \ x_8 x_9 \ x_9 x_{10}$

of nonnegative integers where the sum of list (a) is the same as the sum of list (b). Both lists are weakly monotone decreasing, and each number of list (a) is $\geq$ each number of list (b). The numbers of list (a) must all be equal, else the sum of (a) would exceed that of (b). From this we see that all the numbers of both lists must be equal.

If this common value is 0, then since $x_1 > 0$ we have that all of $x_2$ through $x_9$ are 0; then since $x$ is primitive and Pythagorean, $x$ must be the 10-tuple $a_0 = (1, 0, \ldots, 0, 1)$. If the common value is nonzero, then from list (a) we see that $x_1 = x_2 = x_3$; then from list (b) that the components $x_4, \ldots, x_9$ are all equal; since $x$ is primitive and Pythagorean, $x$ must be the 10-tuple $a_1 = (1, 1, \ldots, 1, 3)$.

We have shown that the only Pythagorean 10-tuples whose last component is not strictly lowered by application of $A_{10}$ are $a_0$ and $a_1$. Thus any Pythagorean 10-tuple $x$ other than $a_0$, $a_1$ may be generated from either $a_0$ or $a_1$.

We close with two questions: Do the Pythagorean $n$-tuples fall into more than $[(n + 6)/8]$ orbits under the automorphism group of (1)? Are there any more cases where a single matrix generates the Pythagorean $n$-tuples from an initial set of orbit representatives?
REFERENCES


DEPARTMENT OF MATHEMATICS, SAINT JOHN FISHER COLLEGE, ROCHESTER, NEW YORK 14618