ELSEVIER
Discrete Mathematics 192 (1998) 273–279
DISCRETE MATHEMATICS

Embedding a set of rational points in lower dimensions

Hiroshi Maehara

Ryukyu University, College of Education, Nishihara, Okinawa, Japan

Received 18 September 1996; revised 15 May 1997; accepted 10 June 1997

Abstract

Let X^n be a set of rational points lying on an n-dimensional flat in a Euclidean space. We prove that for $n \geqslant 2$, X^n is congruent to a set of rational points in $\mathbb{R}^{2n+1}$, and that for $n \geqslant 3$, X^n is similar to a set of rational points in $\mathbb{R}^{2n-1}$.

1. Introduction

Let $\mathbb{Q}^n$ denote the subset of Euclidean space $\mathbb{R}^n$ consisting of all rational points. A point-set X of a Euclidean space is called a $\sqrt{\mathbb{Q}}$-set [3] if the square-distances among the points in X are all rationals. Every subset of $\mathbb{Q}^n$ is clearly a $\sqrt{\mathbb{Q}}$-set, and it was proved in [2] that any $\sqrt{\mathbb{Q}}$-set lying on an n-dimensional flat in a (possibly, very high dimensional) Euclidean space is congruent to a subset of $\mathbb{Q}^{3n+1}$. It was then asked whether there is a 3-point $\sqrt{\mathbb{Q}}$-set that is not congruent to a subset of $\mathbb{Q}^6$. We are going to prove the following theorem, answering this question.

Let X^n denote an arbitrary set of rational points lying on an n-dimensional flat in a Euclidean space.

Theorem 1. *For $n \geqslant 2$, X^n is congruent to a subset of $\mathbb{Q}^{2n+1}$. If n is even and $\geqslant 4$ then X^n is congruent to a subset of $\mathbb{Q}^{2n}$.*

Thus, any 3-point $\sqrt{\mathbb{Q}}$-set is congruent to a subset of $\mathbb{Q}^5$. Since the vertex-set of the triangle with sides $1, \sqrt{7}, \sqrt{8}$ is never congruent to a subset of $\mathbb{Q}^4$ (Lemma 5), the dimension 5 is the least possible for $\sqrt{\mathbb{Q}}$-triples.

Since a pair of points with mutual distance $\sqrt{7}$ is not congruent to any subset of $\mathbb{Q}^3$, we cannot drop the condition $n \geqslant 2$ in the above theorem.

Any two point-sets X and Y are called *similar* if there is a real $\lambda > 0$ such that $\lambda X := \{\lambda \boldsymbol{x}\colon \boldsymbol{x} \in X\}$ is congruent to Y.

PII S0012-365X(98)00075-2

Theorem 2. *For $n \geqslant 3$, X^n is similar to a subset of* $\mathbb{Q}^{2n-1}$.

A lattice point is a point whose coordinates are all integers. A lattice tetrahedron is a tetrahedron whose vertices are lattice points in some $\mathbb{R}^N$. By the above theorem, any lattice tetrahedron is similar to a tetrahedron with vertices in $\mathbb{Q}^5$. Then, by dilating suitably, we can deduce that any lattice tetrahedron is similar to a lattice tetrahedron in $\mathbb{R}^5$. This answers the second question (Problem 2) in [2].

Problem. Is there a constant c such that every X^n is congruent to a subset in $\mathbb{Q}^{n+c}$?

2. The three- and four-square theorems

First, let us recall the following two theorems.

(1) **(The four-square theorem).** *Every positive integer can be represented as the sum of the squares of four integers.*

(2) **(The three-square theorem).** *A positive integer can be represented as the sum of three integral squares if and only if it is not of the form* $4^i(8m+7)$ *for some integers* i, m.

For the proof of the four-square theorem, see Niven–Zuckerman [5] or Pach [6], and for the three-square theorem, see Narkiewicz [4].

By the four-square theorem, every positive rational number is represented by the sum of four squares of rationals. Let us call a positive rational number *3-square-type* if it can be represented as the sum of three squares of rationals, otherwise, it is called *4-square-type*. By the three-square theorem, a positive rational α is 4-square-type if and only if $n^2\alpha = 4^i(8m+7)$ for some integers n, i, m.

Remark. If α is of 4-square-type, then since $(2\ell+1)^2 = 8\ell(\ell+1)/2 + 1 \equiv 1 \pmod 8$, $k^2\alpha$ is also of 4-square-type for any integer $k \neq 0$.

Since $7^2 = 49 \equiv 1 \pmod 8$, the next lemma follows.

Lemma 1. *If two positive rationals α, β are both of 4-square-type, then the product $\alpha\beta$ is of 3-square-type.*

Lemma 2. *For any three positive rationals α, β, γ, there are four rational numbers u, v, w, x such that $\alpha = \beta(u^2 + v^2 + w^2) + \gamma x^2$.*

Proof. (1) If α/β is of 3-square-type, then $\alpha = \beta(u^2 + v^2 + w^2)$ for some rationals u, v, w.

(2) Suppose that α/β is of 4-square-type. There are positive integers k, n such that $k^2(\gamma/\beta) = 4^i n$ where $n \equiv 2$ or $4 \pmod 8$. Using Remark, we can choose two integers

a, b so that $a^2(\alpha/\beta) = 4^{i+j}(8m + 7)$ and $b^2(\gamma/\beta) = 4^{i+j}n$ where i, j, m, n are integers, $n \equiv 2$ or $4 \pmod 8$, and $8m + 7 > n$. Then

$$a^2(\alpha/\beta) - b^2(\gamma/\beta) = 4^{i+j}(8m + 7 - n),$$

and since $8m - n$ is even and not divisible by 8, $a^2(\alpha/\beta) - b^2(\gamma/\beta)$ is of 3-square-type. The Lemma now follows easily. □

3. Inner product spaces over $\mathbb{Q}$

By an *inner product space over* $\mathbb{Q}$, we mean a subset V of a Euclidean space such that V constitutes a vector space over the rational field $\mathbb{Q}$, and for any $\boldsymbol{u}, \boldsymbol{v} \in V$, the inner product $(\boldsymbol{u}, \boldsymbol{v})$ is a rational. Let us denote by V^n an n-dimensional inner product space over $\mathbb{Q}$. From any basis $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n\}$ of V^n, we can get an orthogonal basis $\{\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n\}$ by Schmidt orthogonalization (without normalization). That is,

$$\boldsymbol{a}_1 = \boldsymbol{v}_1,$$

$$\boldsymbol{a}_2 = \boldsymbol{v}_2 - \frac{(\boldsymbol{v}_2, \boldsymbol{a}_1)}{(\boldsymbol{a}_1, \boldsymbol{a}_1)}\boldsymbol{a}_1,$$

$$\boldsymbol{a}_3 = \boldsymbol{v}_3 - \frac{(\boldsymbol{v}_3, \boldsymbol{a}_1)}{(\boldsymbol{a}_1, \boldsymbol{a}_1)}\boldsymbol{a}_1 - \frac{(\boldsymbol{v}_3, \boldsymbol{a}_2)}{(\boldsymbol{a}_2, \boldsymbol{a}_2)}\boldsymbol{a}_2,$$

$$\ldots$$

Note that the coefficients appearing in the above orthogonalization are all rational numbers.

A $\mathbb{Q}$-linear map $\varphi : V^n \to \mathbb{Q}^m$ that satisfies $(\varphi(\boldsymbol{u}), \varphi(\boldsymbol{v})) = (\boldsymbol{u}, \boldsymbol{v})$ for every $\boldsymbol{u}, \boldsymbol{v} \in V^n$ is called an *embedding* of V^n in $\mathbb{Q}^m$. If there is an embedding of V^n in $\mathbb{Q}^m$, then V^n is said to be *embeddable* in $\mathbb{Q}^m$.

Lemma 3. *If $V^n \subset V^{n+1}$, and V^n is embeddable in $\mathbb{Q}^m$, $m > n$, then V^{n+1} is embeddable in $\mathbb{Q}^{m+3}$.*

Proof. Let $\varphi : V^n \to \mathbb{Q}^m$ be an embedding. Since $m > n$, there is a nonzero vector $\boldsymbol{c} = (c_1, \ldots, c_m) \in \mathbb{Q}^m$ orthogonal to $\varphi(V^n)$. Let $\boldsymbol{a} \in V^{n+1}$ be a nonzero vector orthogonal to V^n, and let $\alpha = (\boldsymbol{a}, \boldsymbol{a})$, $\gamma = (\boldsymbol{c}, \boldsymbol{c})$. By Lemma 2, there are four rational numbers u, v, w, x such that

$$\alpha = u^2 + v^2 + w^2 + \gamma x^2.$$

Let $\psi : V^n \to \mathbb{Q}^{m+3}$ be the linear map defined by $\psi(\boldsymbol{v}) = (\varphi(\boldsymbol{v}), 0, 0, 0)$, and let

$$\psi(\boldsymbol{a}) = (xc_1, \ldots, xc_m, 0, 0, 0) + (0, \ldots, 0, u, v, w) \in \mathbb{Q}^{m+3}.$$

Then $(\psi(\boldsymbol{a}),\psi(\boldsymbol{a}))=u^2+v^2+w^2+\gamma x^2=\alpha$, and $\psi(\boldsymbol{a})$ is orthogonal to $\psi(V^n)$. Hence the linear map $V^{n+1}\to\mathbb{Q}^{n+3}$ determined by ψ preserves the inner product, and hence V^{n+1} is embeddable in $\mathbb{Q}^{m+3}$. □

Lemma 4. *If $V^n\subset V^{n+2}$, and V^n is embeddable in $\mathbb{Q}^m, m>n$, then V^{n+2} is embeddable in $\mathbb{Q}^{m+4}$.*

Since V^0 is embeddable in $\mathbb{Q}^1$, V^2 is embeddable in $\mathbb{Q}^5$.

Proof. Let $\varphi: V^n\to\mathbb{Q}^m$ be an embedding. Since $m>n$, there is a nonzero vector $\boldsymbol{c}=(c_1,\dots,c_m)\in\mathbb{Q}^m$ orthogonal to $\varphi(V^n)$. Let $\boldsymbol{a},\boldsymbol{b}\in V^{n+2}$ be two mutually orthogonal nonzero vectors, each orthogonal to V^n, and let $\alpha=(\boldsymbol{a},\boldsymbol{a})$, $\beta=(\boldsymbol{b},\boldsymbol{b})$, $\gamma=(\boldsymbol{c},\boldsymbol{c})$. By Lemma 2, there are four rational numbers u,v,w,x such that

$$\alpha=\beta(u^2+v^2+w^3)+\gamma x^2.$$

Now, by the four squares theorem, there are four rationals p,q,r,s such that $\beta=p^2+q^2+r^2+s^2$. Let $\psi: V^n\to\mathbb{Q}^{m+4}$ be the linear map defined by $\psi(\boldsymbol{v})=(\varphi(\boldsymbol{v}),0,0,0,0)$. Define $\psi(\boldsymbol{b})$, $\psi(\boldsymbol{a})\in\mathbb{Q}^{m+4}$ by

$$\psi(\boldsymbol{b})=(0,\dots,0,p,q,r,s),$$

$$\psi(\boldsymbol{a})=u(0,\dots,0,-q,p,-s,r)+v(0,\dots,0,r,-s,-p,q)$$
$$+w(0,\dots,0,s,r,-q,-p)+x(c_1,\dots,c_m,0,0,0,0).$$

Then $\psi(\boldsymbol{b})$, $\psi(\boldsymbol{a})$ are both orthogonal to $\psi(V^n)$. Since five vectors

$$(0,\dots,0,p,q,r,s),(0,\dots,0,-q,p,-s,r),(0,\dots,0,r,-s,-p,q),$$
$$(0,\dots,0,s,r,-q,-p),(c_1,\dots,c_m,0,0,0,0)$$

are mutually orthogonal, we have $(\psi(\boldsymbol{a}),\psi(\boldsymbol{b}))=0$ and $(\psi(\boldsymbol{b}),\psi(\boldsymbol{b}))=\beta$, $(\psi(\boldsymbol{a}),\psi(\boldsymbol{a}))=\alpha$. Hence the linear map $V^{n+2}\to\mathbb{Q}^{m+4}$ determined by ψ preserves the inner product, and hence V^{n+2} is embeddable in $\mathbb{Q}^{m+4}$. □

Lemma 5. *Let $\{\boldsymbol{a},\boldsymbol{b}\}$ be any orthonormal basis of V^2, and let $\alpha=(\boldsymbol{a},\boldsymbol{a})$, $\beta=(\boldsymbol{b},\boldsymbol{b})$. Then V^2 is embeddable in $\mathbb{Q}^4$ if and only if $\alpha\beta$ is of 3-square-type.*

Proof. Suppose that $\alpha\beta$ is of 3-square-type. Then $\beta/\alpha=x^2+y^2+z^2$ for some rationals x,y,z. Let $\alpha=p^2+q^2+r^2+s^2$, $p,q,r,s\in\mathbb{Q}$. The linear map $\varphi: V^2\to\mathbb{Q}^4$ determined by

$$\varphi(\boldsymbol{a})=(p,q,r,s),$$

$$\varphi(\boldsymbol{b})=x(-q,p,-s,r)+y(r,-s,-p,q)+z(s,r,-q,-p)$$

is an embedding of V^2 in $\mathbb{Q}^4$.

Conversely, suppose that there is an embedding $\varphi: V^2 \to \mathbb{Q}^4$. Let $(p,q,r,s)=\varphi(\boldsymbol{a})$. Then, since four vectors

$$(p,q,r,s),(-q,p,-s,r),(r,-s,-p,q),(s,r,-q,-p)$$

form an orthogonal basis of $\mathbb{Q}^4$, we can write $\varphi(\boldsymbol{b})=x(-q,p,-s,r)+y(r,-s,-p,q)+z(s,r,-q,-p)$, $x,y,z\in\mathbb{Q}$. Then $\beta=(\varphi(\boldsymbol{b}),\varphi(\boldsymbol{b}))=\alpha(x^2+y^2+z^2)$. Hence β/α is of 3-square-type, and hence $\alpha\beta$ is of 3-square-type. □

Problem. Characterize those V^2 that are embeddable in $\mathbb{Q}^3$.

Lemma 6. *Any V^3 contains a two-dimensional subspace that is embeddable in $\mathbb{Q}^4$.*

Proof. Let $\{\boldsymbol{a},\boldsymbol{b},\boldsymbol{c}\}$ be an orthogonal basis of V^3, and let

$$\alpha=(\boldsymbol{a},\boldsymbol{a}),\quad \beta=(\boldsymbol{b},\boldsymbol{b}),\quad \gamma=(\boldsymbol{c},\boldsymbol{c}).$$

By Lemma 5, it is enough to show that one of $\alpha\beta,\alpha\gamma,\beta\gamma$ is of 3-square-type. If both $\alpha\beta,\alpha\gamma$ are of 4-square-type, then $\alpha\beta\alpha\gamma=\alpha^2\beta\gamma$ is of 3-square-type by Lemma 1, and hence $\beta\gamma$ is of 3-square-type. □

Corollary 1. *V^3 is embeddable in $\mathbb{Q}^7$.*

Proof. Since there is a two-dimensional subspace W of V^3 that is embeddable in $\mathbb{Q}^4$, V^3 is embeddable in $\mathbb{Q}^{4+3}$ by Lemma 3. □

Using Lemma 4 instead of Lemma 3, we have the next corollary.

Corollary 2. *V^4 is embeddable in $\mathbb{Q}^8$.*

4. Similar embeddings

For a positive rational number λ and a V^n, let $\sqrt{\lambda}V^n$ denote the *dilation* of V^n by $\sqrt{\lambda}$, that is,

$$\sqrt{\lambda}V^n=\{\sqrt{\lambda}\boldsymbol{v}:\ \boldsymbol{v}\in V^n\}.$$

Note that $\sqrt{\lambda}V^n$ is also an inner product space over $\mathbb{Q}$.

If $\sqrt{\lambda}V^n$ is embeddable in $\mathbb{Q}^m$ for some positive rational λ, then V^n is said to be *similarly embeddable* (or *s-embeddable*) in $\mathbb{Q}^m$.

Lemma 7. *For any positive rational λ, $\sqrt{\lambda}\mathbb{Q}^{4m}$ is embeddable in $\mathbb{Q}^{4m}$.*

Proof. Express λ as $\lambda = x^2+y^2+z^2+w^2$ $(x, y, z, w \in \mathbb{Q})$. Let M be the $4m \times 4m$-matrix

$$M = \begin{pmatrix} A & & & 0 \\ & \ddots & & \\ & & \ddots & \\ 0 & & & A \end{pmatrix},$$

where

$$A = \begin{pmatrix} x & -y & z & w \\ y & x & -w & z \\ z & -w & -x & -y \\ w & z & y & -x \end{pmatrix}.$$

Then the map $\varphi : \sqrt{\lambda}\mathbb{Q}^{4m} \to \mathbb{Q}^{4m}$ defined by $\varphi(\sqrt{\lambda}\boldsymbol{v}) = \boldsymbol{v}M$ is an embedding of $\sqrt{\lambda}\mathbb{Q}^{4m}$ in $\mathbb{Q}^{4m}$. Indeed, for any $\sqrt{\lambda}\boldsymbol{u}, \sqrt{\lambda}\boldsymbol{v} \in \sqrt{\lambda}\mathbb{Q}^{4m}$,

$$(\varphi(\sqrt{\lambda}\boldsymbol{u}), \varphi(\sqrt{\lambda}\boldsymbol{v})) = (\boldsymbol{u}M, \boldsymbol{v}M) = (\boldsymbol{u}MM^t, \boldsymbol{v}) = \lambda(\boldsymbol{u}, \boldsymbol{v}) = (\sqrt{\lambda}\boldsymbol{u}, \sqrt{\lambda}\boldsymbol{v}). \qquad \square$$

Lemma 8. *Let $\boldsymbol{W}$ be a subspace of $\boldsymbol{V}^n$. Suppose that $\sqrt{\lambda}\boldsymbol{W}$ is embeddable in $\mathbb{Q}^j$ for any rational $\lambda > 0$, and that the orthogonal complement $\boldsymbol{W}^\perp$ is similarly embeddable in $\mathbb{Q}^k$. Then $\boldsymbol{V}^n$ is similarly embeddable in $\mathbb{Q}^{j+k}$.*

Proof. Suppose that $\sqrt{\alpha}\boldsymbol{W}^\perp$ is embeddable in $\mathbb{Q}^k$. Since $\sqrt{\alpha}\boldsymbol{W}$ is embeddable in $\mathbb{Q}^j$ by the assumption, we can deduce that $\sqrt{\alpha}\boldsymbol{V}^n = \sqrt{\alpha}(\boldsymbol{W} \oplus \boldsymbol{W}^\perp)$ is embeddable in $\mathbb{Q}^{j+k}$. Hence $\boldsymbol{V}^n$ is similarly embeddable in $\mathbb{Q}^{j+k}$. $\square$

Corollary 3. *$\boldsymbol{V}^3$ is similarly embeddable in $\mathbb{Q}^5$.*

Proof. Let $\boldsymbol{W}$ be a two-dimensional subspace of $\boldsymbol{V}^3$ that is embeddable in $\mathbb{Q}^4$. Then by Lemma 7, for any rational $\lambda > 0$, $\sqrt{\lambda}\boldsymbol{W}$ is embeddable in $\mathbb{Q}^4$. Since any one-dimensional subspace of $\boldsymbol{V}^3$ is similarly embeddable in $\mathbb{Q}^1$, $\boldsymbol{V}^3$ is similarly embeddable in $\mathbb{Q}^5$ by Lemma 8. $\square$

5. Proofs of Theorems 1 and 2

Proof of Theorem 1. By adding a rational vector if necessary, we may suppose that X^n lies on an n-dimensional subspace $\boldsymbol{V}^n \subset \mathbb{Q}^N$. Hence it will be enough to show the theorem for $X^n = \boldsymbol{V}^n$. By Lemma 4, $\boldsymbol{V}^2$ is embeddable in $\mathbb{Q}^5$, and by Corollary 1, $\boldsymbol{V}^3$ is embeddable in $\mathbb{Q}^7$. Hence $\boldsymbol{V}^n$ is embeddable in $\mathbb{Q}^{2n+1}$ by Lemmas 3, 4. For even $n \geqslant 4$, $\boldsymbol{V}^n$ is embeddable in $\mathbb{Q}^{2n}$ by Corollary 2 and Lemma 4. $\square$

Proof of Theorem 2. It will be enough to show that for $n \geqslant 3$, V^n is similarly embeddable in $\mathbb{Q}^{2n-1}$. By Corollary 3, V^3 is similarly embeddable in $\mathbb{Q}^5$. By Corollary 2, V^4 is embeddable in $\mathbb{Q}^8$. It is known [2] that if V^n is embeddable in $\mathbb{Q}^{4m}$, then V^n is similarly embeddable in $\mathbb{Q}^{4m-1}$. Hence, V^4 is similarly embeddable in $\mathbb{Q}^7$. Now the theorem follows by applying Lemma 4. □

References

[1] M.J. Beeson, Triangles with vertices on lattice points, Amer. Math. Monthly 99 (1992) 243–252.

[2] H. Maehara, Embedding a polytope in a lattice, Discrete Comput. Geom. 13 (1995) 585–592.

[3] H. Maehara, On $\sqrt{\mathbb{Q}}$-distances, Europ. J. Combin. 17 (1996) 271–277.

[4] W. Narkiewicz, Classical Problems in Number Theory, PWN-Polish Scientific Publishers, Warszawa, 1986.

[5] I. Niven, H.S. Zuckerman, An Introduction to the Theory of Numbers, Wiley, New York, 1972.

[6] J. Pach, P.K. Agarwal, Combinatorial Geometry, Wiley, New York, 1995.