数理解析研究所講究録
1063巻 1998年 158-162

Isometric embeddings of metric Q-vector spaces into $\mathbf{Q}^N$

Toshihiro Kumada (熊田 敏宏)*

Abstract

Let $\mathbf{W}$ be an n-dimensional $\mathbf{Q}$-vector space which has a positive definite symmetric bilinear form. We prove that $\mathbf{W}$ is isometrically embeddable into $\mathbf{Q}^{n+3}$. We give a formula to obtain the minimum N such that $\mathbf{W}$ is isometrically embeddable into $\mathbf{Q}^N$.

1 Introduction

In this paper, we denote by $\mathbf{Q}^+$ the set of positive rational numbers, and by $\mathbf{Q}^\times$ the multiplicative group of the rational number field. For $a_1,\ldots,a_n \in \mathbf{Q}^+$, we define the following number $N(a_1,\ldots,a_n)$.

Definition Let $a_1,\ldots,a_n \in \mathbf{Q}^+$. We define $N(a_1,\ldots,a_n) :=$
$\min\{k \mid$ *we can find* n *vectors* $\mathbf{v}_1,\ldots,\mathbf{v}_n \in \mathbf{Q}^k$ *s.t.* $(\mathbf{v}_i,\mathbf{v}_j) = \delta_{ij}a_i\}$.

In the above definition $(\ ,\ )$ is the canonical inner product of $\mathbf{Q}^k$ and δ_{ij} is the Kronecker's delta. Maehara[2] studied this number for some special cases. The purpose of this paper is to give a formula for determining $N(a_1,\ldots,a_n)$.

2 Main Result

Theorem 1 *For all* $a_1,\ldots,a_n \in \mathbf{Q}^+$, $n \leq N(a_1,\ldots,a_n) \leq n+3$ *holds.*

Let $\mathcal{V}$ be the set $\{p \mid p$ *is prime number*$\} \cup \{\infty\}$. We denote by $\mathbf{Q}_\infty$ the real number field $\mathbf{R}$, and by $\mathbf{Q}_p$ the p-adic number field for a prime p. The following three theorems give a formula to obtain $N(a_1,\ldots,a_n)$ for given $a_1,\ldots,a_n \in \mathbf{Q}^+$.

*e-mail: kumada@math.keio.ac.jp

Theorem 2 *Let* $a_1, \ldots, a_n \in \mathbf{Q}^+$. *Put* $D := \prod_{i=1}^n a_i \in \mathbf{Q}^+$ *and* $E_v := \prod_{1 \le i < j \le n} (a_i, a_j)_v \in \{\pm 1\}$. *where* $v \in \mathcal{V}$ *and* $(\ ,\ )_v$ *is the Hilbert symbol on* $\mathbf{Q}_v$. $N(a_1, \ldots, a_n) = n$ *holds if and only if* $D = 1 \pmod{\mathbf{Q}^{*2}}$ *holds and* $E_v = 1$ *holds for all* $v \in \mathcal{V}$.

The Hilbert symbol $(\ ,\ )_v$ is a map from $\mathbf{Q}_v^*/\mathbf{Q}_v^{*2} \times \mathbf{Q}_v^*/\mathbf{Q}_v^{*2}$ to $\{\pm 1\}$ defined so that $(a, b)_v = 1$ holds if and only if $z^2 = ax^2 + by^2$ has a solution $(x, y, z) \in (\mathbf{Q}_v)^3 \setminus \{0, 0, 0\}$. It is bilinear and symmetric. The Hilbert symbol is easy to compute, see Serre[3, p.20, Theorem 1].

Theorem 3 *Let* $a_1, \ldots, a_n \in \mathbf{Q}^+$. *Let* D, E_v *be as in Theorem 2. Assume* $N(a_1, \ldots, a_n) \neq n$. *Then* $N(a_1, \ldots, a_n) = n + 1$ *holds if and only if* $E_v \cdot (D, -1)_v = 1$ *holds for all* $v \in \mathcal{V}$.

Theorem 4 *Let* $a_1, \ldots, a_n \in \mathbf{Q}^+$. *Let* D, E_v *be as in Theorem 2. Assume* $N(a_1, \ldots, a_n) \neq n, n + 1$. *Then* $N(a_1, \ldots, a_n) = n + 2$ *holds if and only if* $-D \notin \mathbf{Q}_v^{*2}$ *holds for all* $v \in V$. *where*

$$V = \{v \mid v \text{ is an odd prime with } E_v = -1\} \cup \begin{cases} \{2\} & \text{if } E_2 = 1 \\ \emptyset & \text{if } E_2 = -1 \end{cases}$$

In the above three theorems, if $n = 1$, then define $E_v := 1$ for all $v \in \mathcal{V}$.

If $x = b/a$, $y = d/c (a, b, c, d \in \mathbf{Z})$ and $v \neq 2, \infty$ and $v \nmid abcd$, then $(x, y)_v = 1$ holds(see Serre[3, p.20, Theorem 1]). This shows that the number of $v \in \mathcal{V}$ for which we need to compute the Hilbert symbol is finite. Thus for given $a_1, \ldots, a_n \in \mathbf{Q}^+$, $N(a_1, \ldots, a_n)$ is computable with finite calculation.

Corollary 1 *For an arbitrary* $n \in \mathbf{N}$, *put* $a_2 = a_3 = \ldots = a_n = 1$. *Then* $N(1, a_2, \ldots, a_n) = n$, $N(2, a_2, \ldots, a_n) = n + 1$, $N(3, a_2, \ldots, a_n) = n + 2$ *and* $N(7, a_2, \ldots, a_n) = n + 3$ *hold. Consequently, the bound in Theorem 1 is the best possible.*

Remark. Let $\mathbf{W}$ be a finite dimensional $\mathbf{Q}$-vector space with a positive definite symmetric bilinear form. The above three theorems give an explicit algorithm to obtain the minimum dimensional $\mathbf{Q}^N$ into which $\mathbf{W}$ is isometrically embeddable by a $\mathbf{Q}$-linear map. This is because for any $\mathbf{W}$, we can obtain an orthogonal basis.

3 Proof of Theorem 1

In this section, we prove Theorem 1. For the proof of Theorem 1, the following lemma is essential.

Lemma 1 [Meyer] *Let c be a positive rational number and $c_1, \ldots, c_4$ be elements of $\mathbf{Q}^\times$. Assume that $c_1 > 0$. Then the next quadratic equation has a rational solution $(x_1, \ldots, x_4) \in \mathbf{Q}^4$:*

$$c = \sum_{i=1}^{4} c_i x_i^2.$$

Proof of Theorem 1 Let $a_1, \ldots, a_n$ be arbitrary n elements in $\mathbf{Q}^+$. It is clear that $n \leq N(a_1, \ldots, a_n)$. So we prove $N(a_1, \ldots, a_n) \leq n+3$. By the definition of $N(a_1, \ldots, a_n)$, it is sufficient to find n vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n \in \mathbf{Q}^{n+3}$ such that $(\mathbf{v}_i, \mathbf{v}_j) = \delta_{ij} a_i$. We use induction on n. If $n = 1$, by Lemma 1, there are four rational numbers p, q, r, s such that

$$a_1 = p^2 + q^2 + r^2 + s^2.$$

Then put $\mathbf{v}_1 := (p, q, r, s)$. $\{\mathbf{v}_1\}$ satisfies the requirement.
Next, assume that Theorem 1 holds for n. We consider $n+1$. By the assumption of induction, there are n vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n \in \mathbf{Q}^{n+3}$ such that $(\mathbf{v}_i, \mathbf{v}_j) = \delta_{ij} a_i$. Put $\mathbf{u}_i := (\mathbf{v}_i, 0) \in \mathbf{Q}^{n+4}$. Clearly $(\mathbf{u}_i, \mathbf{u}_j) = (\mathbf{v}_i, \mathbf{v}_j) = \delta_{ij} a_i$ holds and $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ is linearly independent over the rational number field. Let $\{\mathbf{u}_1, \ldots, \mathbf{u}_n, \mathbf{e}_{n+1}, \mathbf{e}_{n+2}, \mathbf{e}_{n+3}, \mathbf{e}_{n+4}\}$ be an basis of $\mathbf{Q}^{n+4}$ which includes $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$. We can choose $\{\mathbf{u}_1, \ldots, \mathbf{u}_n, \mathbf{e}_{n+1}, \mathbf{e}_{n+2}, \mathbf{e}_{n+3}, \mathbf{e}_{n+4}\}$ so that they are mutually orthogonal. Because we may do Schmidt orthogonalization without normalization to a basis extending $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ if necessary. Let $e_i = (\mathbf{e}_i, \mathbf{e}_i)$. By Lemma 1, there are four rational numbers p, q, r, s such that

$$a_{n+1} = e_1 p^2 + e_2 q^2 + e_3 r^2 + e_4 s^2.$$

Put $\mathbf{u}_{n+1} := p\,\mathbf{e}_{n+1} + q\,\mathbf{e}_{n+2} + r\,\mathbf{e}_{n+3} + s\,\mathbf{e}_{n+4}$. Then $\{\mathbf{u}_1, \ldots, \mathbf{u}_{n+1}\}$ satisfies the requirements.

4 Symmetric bilinear forms

Let $\mathbf{W}$ be a finite dimensional vector space over a field K with a symmetric non-degenerate bilinear form $(\ ,\ ) : \mathbf{W} \times \mathbf{W} \to K$. Put $n = \dim \mathbf{W}$. Let $(\mathbf{w}_i)_{1 \leq i \leq n}$ be a basis of $\mathbf{W}$. If $\mathbf{u} = \sum \alpha_i \mathbf{w}_i$ and $\mathbf{v} = \sum \beta_i \mathbf{w}_i$, then we have

$$(\mathbf{u}, \mathbf{v}) = (\alpha_1, \ldots, \alpha_n) A\, {}^t(\beta_1, \ldots, \beta_n),$$

where A is a symmetric matrix in $GL(n, K)$ given by $A = (a_{ij})$, $a_{ij} = (\mathbf{w}_i, \mathbf{w}_j)$. If we use another basis $(\mathbf{w}'_i)_{1 \leq i \leq n}$, then we have another symmetric matrix B, where $B = (b_{ij})$, $b_{ij} = (\mathbf{w}'_i, \mathbf{w}'_j)$. These matrices are related by $B = {}^t X A X$ with $X \in GL(n, K)$.

In general, we denote $A \overset{K}{\sim} B$ if and only if there exists $X \in GL(n, K)$ such that $B = {}^tXAX$ holds. If A is the symmetric matrix of the bilinear form w.r.t. a basis $(\mathbf{w}_i)$ of $\mathbf{W}$, and $A \overset{K}{\sim} B$, then B is the symmetric matrix of the bilinear form w.r.t. the basis $(\mathbf{w}'_i)$ that is obtained by the transformation of $(\mathbf{w}_i)$ by X. If $A \overset{K}{\sim} B$, then $\det A = \det B \pmod{K^{*2}}$ holds.

To save the space of paper, we will use a notation $diag(a_1, \ldots, a_N)$ for an $N \times N$ diagonal matrix whose (i, i) element is a_i. I_N denotes the identity matrix of size N.

Lemma 2 *Let $a_1, \ldots, a_n \in \mathbf{Q}^+$. $N(a_1, \ldots, a_n)$ is characterised as the minimum value of N such that we can choose $b_{n+1}, \ldots, b_N \in \mathbf{Q}^+$ so that*

$$diag(a_1, \ldots, a_n, b_{n+1}, \ldots, b_N) \overset{\mathbf{Q}}{\sim} I_N$$

holds.

5 Outline of proofs of Theorems 2, 3 and 4

In this section, we give an outline of proofs of Theorems 2, 3 and 4. For the proofs of them, the following two lemmas are essential.

Lemma 3 *Let A and B be symmetric matrices in $GL(N, \mathbf{Q})$. Then $A \overset{\mathbf{Q}}{\sim} B$ holds if and only if $A \overset{\mathbf{Q}_v}{\sim} B$ holds for all $v \in \mathcal{V}$.*

Lemma 4 *Let A and B be diagonal matrices in $GL(N, \mathbf{Q}_v)$. Then $A \overset{\mathbf{Q}_v}{\sim} B$ holds if and only if $\det(A) = \det(B) \pmod{\mathbf{Q}_v^{*2}}$ and $\epsilon_v(A) = \epsilon_v(B)$ hold, where $\epsilon_v(A) := \prod_{1 \le i < j \le N} (a_i, a_j)_v \in \{\pm 1\}$ for $A = diag(a_1, \ldots, a_N)$. If N=1, we define $\epsilon_v(A) := 1$ as usual.*

Note that $a \in \mathbf{Q}^{*2}$ is equivalent to $a \in \mathbf{Q}_v^{*2}$ for all $v \in \mathcal{V}$. And it is clear that $\det(I_n) = 1 \pmod{\mathbf{Q}_v^{*2}}$ holds and $\epsilon_v(I_n) = 1$ holds for all $v \in \mathcal{V}$. Hence Theorem 2 follows from Lemmas 2, 3 and 4.

Proof of Theorem 3 We assume that $N(a_1, \ldots, a_n) \neq n$. By Lemma 2, $N(a_1, \ldots, a_n) = n+1$ holds if and only if there exist a rational number x such that $A = diag(a_1, \ldots, a_n, x) \overset{\mathbf{Q}}{\sim} I_{n+1}$. Put $D := \prod_{i=1}^{n} a_i$. The determinant of the left side is Dx, and that of the right side is 1, so $Dx = 1 \pmod{\mathbf{Q}^{*2}}$ holds. Thus x is determined by D as an element of $\mathbf{Q}^*/\mathbf{Q}^{*2}$. Then we check whether $A = diag(a_1, \ldots, a_n, D) \overset{\mathbf{Q}}{\sim} I_{n+1}$ holds or not. By the computation of $\epsilon_v(A)$, we have Theorem 3.

For the proof of Theorem 4, we need a following lemma.

Lemma 5 *Let a be an element of $\mathbf{Q}^\times$, and let $(b_v)_{v\in\mathcal{V}}$ be a family of numbers in $\{\pm 1\}$. In order that there exists $x \in \mathbf{Q}^\times$ such that $(a,x)_v = b_v$ for all $v \in \mathcal{V}$, it is necessary and sufficient that the following conditions are satisfied:*

1. *The cardinality of the set $V' = \{v \mid v \in \mathcal{V},\ b_v = -1\}$ is finite and even.*
2. *For each $v \in \mathcal{V}$, there exists $x_v \in \mathbf{Q}_v^\times$ such that $(a, x_v)_v = b_v$.*

Since the Hilbert symbol is non-degenerate, $(a,y)_v = 1$ holds for all $y \in \mathbf{Q}_v^\times$ if and only if $a \in \mathbf{Q}_v^{\times 2}$. Thus we may replace *2* in the above lemma with

2'. For all $v \in V'$, a is not contained in $\mathbf{Q}_v^{\times 2}$.

Proof of Theorem 4 We assume that $N(a_1,\ldots,a_n) \neq n, n+1$. By Lemma 2, $N(a_1,\ldots,a_n) = n+2$ holds if and only if there exist rational numbers x, y such that $A = diag(a_1,\ldots,a_n,x,y) \overset{\mathbf{Q}}{\sim} I_{n+2}$. Put $D := \prod_{i=1}^n a_i$. As we observed in the proof of Theorem 3, the last rational number y is determined by Dx from the discussion of determinant. Now our problem is reduced to the existence of a rational number x such that $A = diag(a_1,\ldots,a_n,x,Dx) \overset{\mathbf{Q}}{\sim} I_{n+2}$. Applying Lemma 5 to $\epsilon_v(A)$, we obtain a necessary and sufficient condition for the existence of x such that $A = diag(a_1,\ldots,a_n,x,Dx) \overset{\mathbf{Q}}{\sim} I_{n+2}$. Then we have Theorem 4.

References

[1] T. Kumada: *Isometric embeddings of metric $\mathbf{Q}$-vector spaces into $\mathbf{Q}^N$*, to appear in European Journal of Combinatorics.

[2] H. Maehara: *Embedding a set of rational points in lower dimensions*, to appear in Discrete Math.

[3] J. P. Serre, *A Course in Arithmetic*. Volume 7 of GTM, Springer-Verlag, New York, 1973.

Keio University
Department of Mathematics
3-14-1, Hiyoshi, Kohoku-ku
Yokohama 223 Japan