Europ. J. Combinatorics (1998) **19**, 701–706
Article No. ej980220

Isometric Embeddings of Metric Q-vector Spaces into $\mathbf{Q}^N$

TOSHIHIRO KUMADA

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. MAIN RESULT

In this paper, we denote by $\mathbf{Q}^+$ the set of positive rational numbers, and by $\mathbf{Q}^*$ the multiplicative group of the rational number field. For $a_1, \dots, a_n \in \mathbf{Q}^+$, let $N := N(a_1, \dots a_n)$ denote the minimum number such that there exist $\mathbf{v}_1, \dots, \mathbf{v}_n \in \mathbf{Q}^N$ satisfying $(\mathbf{v}_i, \mathbf{v}_j) = \delta_{ij} a_i$, where $(\ ,\ )$ is the canonical inner product of $\mathbf{Q}^N$ and δ_{ij} is the Kronecker's delta. Maehara [1] studies this number for some special cases. Here we give an explicit formula to determine $N(a_1, \dots, a_n)$.

THEOREM 1. *For all $a_1, \dots, a_n \in \mathbf{Q}^+$, $n \le N(a_1, \dots, a_n) \le n + 3$ holds.*

Let $\mathcal{V}$ be the set $\{p | p \textit{ is prime number}\} \cup \{\infty\}$. 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 $N(a_1, \dots, a_n)$ for a given $a_1, \dots, a_n \in \mathbf{Q}^+$.

THEOREM 2. *Let $a_1, \dots, a_n \in \mathbf{Q}^+$. 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 $\mathbf{Q}_v$, $N(a_1, \dots, a_n) = n$ holds if and only if $D = 1 (\mathrm{mod}\, \mathbf{Q}^{*2})$ 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 non-trivial solution $(x, y, z) \in (\mathbf{Q}_v)^3$. It is bilinear and symmetric. The Hilbert symbol is easy to compute, see Serre [2, p. 20, Theorem 1].

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

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

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

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 $v \ne 2, \infty$ and $v \nmid abcd$, then $(x, y)_v = 1$ holds (see Serre [2, p. 20, Theorem 1]). Thus the number of $v \in \mathcal{V}$ for which we need to compute the Hilbert symbol is finite. Thus for given $a_1, \dots, a_n \in \mathbf{Q}^+$, $N(a_1, \dots, a_n)$ is computable with finite calculation.

0195-6698/98/060701 + 06 $30.00/0

COROLLARY 1. *For an arbitrary $n \in \mathbf{N}$, put $a_2 = a_3 = \cdots = a_n = 1$. 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.*

PROOF. As $a_2 = a_3 = \cdots = a_n = 1$, $E_v = 1$ holds for all $a_1 \in \mathbf{Q}^+$, $v \in \mathcal{V}$. It is clear that $N(1, a_2, \ldots, a_n) = n$ holds.

$N(2, a_2, \ldots, a_n) = n + 1$ holds because $2 \notin \mathbf{Q}^{*2}$ and $(2, -1)_v = 1$ holds for all $v \in \mathcal{V}$.
$N(3, a_2, \ldots, a_n) = n + 2$ holds because $3 \notin \mathbf{Q}^{*2}$, $(3, -1)_2 = -1$ and $-3 \notin \mathbf{Q}_2^{*2}$.
$N(7, a_2, \ldots, a_n) = n + 3$ holds because $7 \notin \mathbf{Q}^{*2}$, $(7, -1)_2 = -1$ and $-7 \in \mathbf{Q}_2^{*2}$.

□

REMARK 1. *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.*

These theorems give complete answers to Maehara's open problems [1]. His upper bound $N(a_1, \ldots, a_n) \leq 2n+1$ for $n \geq 2$ is improved here to $n+3$. He also proved that $N(a_1, a_2) \leq 4 (= 2 + 2)$ if and only if a_1a_2 is a sum of three squares of rational numbers. This result is a corollary of Theorem 4, as follows. A positive rational number x is a sum of three squares of rational numbers if and only if $-x \notin \mathbf{Q}_2^{*2}$ (see Serre [2, p. 45, Lemma A]). Put $x := a_1a_2$, and note that $E_v := (a_1, a_2)_v = (a_1, -a_1a_2)_v$ holds for all $v \in \mathcal{V}$. Let V be as in Theorem 4. Assume that the condition of Theorem 4 is satisfied. If $2 \in V$, then $-a_1a_2 \notin \mathbf{Q}_2^{*2}$ holds. If $2 \notin V$, then again $-a_1a_2 \notin \mathbf{Q}_2^{*2}$ holds because $E_2 = (a_1, -a_1a_2)_2 = -1$. In both cases, $-a_1a_2 \notin \mathbf{Q}_2^{*2}$ holds. Conversely, assume that $-a_1a_2 \notin \mathbf{Q}_2^{*2}$ holds. Let $v \in V$. If v is odd prime, $-a_1a_2 \notin \mathbf{Q}_v^{*2}$ holds because $E_v = (a_1, -a_1a_2)_v = -1$. If $v = 2$, $-a_1a_2 \notin \mathbf{Q}_2^{*2}$ holds from the assumption. Thus the condition of Theorem 4 is satisfied.

Maehara proposed characterizing a_1, a_2 such that $N(a_1, a_2) \leq 3$. By Theorem 3, $N(a_1, a_2) \leq 3$ holds if and only if $(a_1, a_2)_v(a_1a_2, -1)_v = 1$ holds for all $v \in \mathcal{V}$. Note that $(a_1, a_2)_v (a_1a_2, -1)_v = (-a_1, -a_2)_v(-1, -1)_v$ holds for all $v \in \mathcal{V}$, because the Hilbert symbol is a bilinear map. Thus $N(a_1, a_2) \leq 3$ holds if and only if $(-a_1, -a_2)_v(-1, -1)_v = 1$ holds for all $v \in \mathcal{V}$.

2. 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 $B = {}^tXAX$ 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 $(\mathbf{w}'_i)$ obtained by the transformation of $(\mathbf{w}_i)$ by X. If $A \overset{K}{\sim} B$, then $\det A = \det B (\mathrm{mod}\, K^{*2})$ holds.

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

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

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

holds.

PROOF. The right side of the above is a matrix of the canonical inner product w.r.t. the canonical basis of $\mathbf{Q}^N$. The above equivalence implies the existence of orthogonal basis $\{\mathbf{v}_1, \dots, \mathbf{v}_n, \dots, \mathbf{v}_N\}$ of $\mathbf{Q}^N$ with $(\mathbf{v}_i, \mathbf{v}_i) = a_i$ for $1 \le i \le n$. Conversely, if we have $\mathbf{v}_1, \dots, \mathbf{v}_n \in \mathbf{Q}^N$ satisfying $(\mathbf{v}_i, \mathbf{v}_j) = \delta_{ij} a_i$, then we can extend these vectors to an orthogonal basis, see Lemma 2 below. □

3. PROOF OF THEOREM 1

In this section, we give proof of Theorem 1. Before the proof of Theorem 1, we prepare two lemmas.

LEMMA 2. *Let $\mathbf{W}$ be a finite dimensional $\mathbf{Q}$-vector space with a positive definite symmetric bilinear form. Let $\{\mathbf{w}_1, \dots, \mathbf{w}_l\}$ be linearly independent vectors. Assume $\{\mathbf{w}_1, \dots, \mathbf{w}_l\}$ are mutually orthogonal. Then we can obtain an orthogonal basis of $\mathbf{W}$ which includes $\{\mathbf{w}_1, \dots, \mathbf{w}_l\}$.*

PROOF. The bilinear form on $\mathbf{W}$ is positive definite. Thus we may perform Schmidt orthogonalization without normalization to a basis extending $\{\mathbf{w}_1, \dots, \mathbf{w}_l\}$. □

LEMMA 3. *Let c be a positive rational number and $c_1, \dots, c_4$ be elements of $\mathbf{Q}^*$. Assume that $c_1 > 0$. Then the next quadratic equation has a rational solution $(x_1, \dots, x_4) \in \mathbf{Q}^4$:*

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

For the proof of the lemma, see, for example, Serre [2, Corollary, Theorem 8 (Hasse–Minkowski), pp. 37, 41].

PROOF OF THEOREM 1. Let $a_1, \dots, a_n$ be arbitrary n elements in $\mathbf{Q}^+$. It is clear that $n \le N(a_1, \dots, a_n)$. So we prove $N(a_1, \dots, a_n) \le n+3$. By the definition of $N(a_1, \dots, a_n)$, it is sufficient to find n vectors $\mathbf{v}_1, \dots, \mathbf{v}_n \in \mathbf{Q}^{n+3}$ such that $(\mathbf{v}_i, \mathbf{v}_j) = \delta_{ij} a_i$. We use induction on n. If $n = 1$, by Lemma 3, 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 $\mathbf{v}_1, \dots, \mathbf{v}_n \in \mathbf{Q}^{n+3}$ 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 $\{\mathbf{u}_1, \dots, \mathbf{u}_n\}$ is linearly independent over the rational number field. By Lemma 2, we may obtain an orthogonal basis of $\mathbf{Q}^{n+4}$ which includes

$\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$. 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 orthogonal basis of $\mathbf{Q}^{n+4}$. Let $e_i = (\mathbf{e}_i, \mathbf{e}_i)$. By Lemma 3, 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. PROOFS OF THEOREMS 2 AND 3

In this section, we give proofs of Theorems 2 and 3. We use Hasses's principle and the Hilbert symbol. First recall the general notion of the p-adic number field.

$\mathbf{Q}_v$ is an extension field of the rational number field $\mathbf{Q}$. It is a complete metric space and $\mathbf{Q}_v^*/\mathbf{Q}_v^{*2}$ is an Abelian group of order 4 (if $v \neq 2, \infty$), order 8 (if $v = 2$), order 2 (if $v = \infty$), respectively.

LEMMA 4. *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 5. *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 $A = \mathrm{diag}(a_1, \ldots, a_N)$. If $N = 1$, we define $\epsilon_v(A) := 1$ as usual.*

For the proof of both lemmas, see, for example, Serre [2, Theorem 7, Theorem 9, pp. 39, 44].

PROOF OF THEOREM 2. By Lemma 1, $N(a_1, \ldots, a_n) = n$ holds if and only if $\mathrm{diag}(a_1, \ldots, a_n) \overset{\mathbf{Q}}{\sim} I_n$. Now $\det(I_n) = 1$ holds and $\epsilon_v(I_n) = 1$ holds for all $v \in \mathcal{V}$. Thus the theorem follows from Lemmas 4 and 5. □

PROOF OF THEOREM 3. We assume that $N(a_1, \ldots, a_n) \neq n$. By Lemma 1, $N(a_1, \ldots, a_n) = n+1$ holds if and only if there exist a rational number x such that $A = \mathrm{diag}(a_1, \ldots, a_n, x) \overset{\mathbf{Q}}{\sim} I_{n+1}$. 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 $A = \mathrm{diag}(a_1, \ldots, a_n, D) \overset{\mathbf{Q}}{\sim} I_{n+1}$ holds or not. As $\det(A) = \det(I_{n+1}) \pmod{\mathbf{Q}^{*2}}$, $\det(A) = \det(I_{n+1}) \pmod{\mathbf{Q}_v^{*2}}$ holds for all $v \in \mathcal{V}$. Thus, all we have to do is to check whether $\epsilon_v(A) = \epsilon(I_{n+1})$ holds for all $v \in \mathcal{V}$ or not (recall Lemmas 4 and 5). Put $E_v := \prod_{1\le i<j\le n}(a_i, a_j)_v$. Then we have

$$\begin{aligned}
\epsilon_v(\mathrm{diag}(a_1, \ldots, a_n, D)) &= \prod_{1\le i<j\le n}(a_i, a_j)_v \prod_{i=1}^n (a_i, D)_v \\
&= E_v\left(\prod_{i=1}^n a_i, D\right)_v \\
&= E_v(D, D)_v \\
&= E_v(D, -1(-D))_v \\
&= E_v(D, -1)_v.
\end{aligned}$$

In the above transformation, we used bilinearity of the Hilbert symbol. At the last transformation, we used $(D, -D)_v = 1$. Now the theorem is proved. □

5. Proof of Theorem 4

Before the proof of Theorem 4, we prepare a lemma.

LEMMA 6. *Let a be an element of $\mathbf{Q}^*$, and let $(b_v)_{v\in\mathcal{V}}$ be a family of numbers in $\{\pm 1\}$. In order that there exists $x \in \mathbf{Q}^*$ 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 $V' = \{v | v \in \mathcal{V}, b_v = -1\}$ is finite and even.
(2) For each $v \in \mathcal{V}$, there exists $x_v \in \mathbf{Q}_v^*$ such that $(a, x_v)_v = b_v$.

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

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

For the proofs, see, for example, Serre [2, Theorem 2, Theorem 4, pp. 20, 24].

PROOF OF THEOREM 4. We assume that $N(a_1, \ldots, a_n) \neq n, n+1$. By Lemma 1, $N(a_1, \ldots, a_n) = n+2$ holds if and only if there exist rational numbers x, y such that $A = \mathrm{diag}(a_1, \ldots, a_n, x, y) \overset{\mathbf{Q}}{\sim} I_{n+2}$. 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. It is necessary that $Dx = y (\mathrm{mod}\, \mathbf{Q}^{*2})$ holds. Thus we discuss the existence of a rational number x such that $A = \mathrm{diag}(a_1, \ldots, a_n, x, Dx) \overset{\mathbf{Q}}{\sim} I_{n+2}$. Like the proof of Theorem 3, all we have to do is to check whether $\epsilon_v(A) = 1$ holds for all $v \in \mathcal{V}$ or not (recall Lemmas 4 and 5). Put $E_v := \prod_{1\le i<j\le n} (a_i, a_j)_v$. Then we have

$$\begin{aligned}
\epsilon_v(\mathrm{diag}(a_1, \ldots, a_n, x, Dx)) &= \prod_{1\le i<j\le n} (a_i, a_j)_v (x, Dx)_v \prod_{i=1}^n (a_i, x)_v \prod_{i=1}^n (a_i, Dx)_v \\
&= E_v (x, Dx)_v \left(\prod_{i=1}^n a_i, x\right)_v \left(\prod_{i=1}^n a_i, Dx\right)_v \\
&= E_v (x, Dx)_v (D, Dx^2)_v \\
&= E_v (x, -D(-x))_v (D, D)_v \\
&= E_v (x, -D)_v (D, -1)_v \\
&= E_v (x, -D)_v (-D, -1)_v (-1, -1)_v \\
&= E_v (-x, -D)_v (-1, -1)_v.
\end{aligned}$$

Now our problem is reduced to the existence of a rational number x such that $(-x, -D)_v = E_v(-1, -1)_v$ holds for all $v \in \mathcal{V}$. Let us recall that $(-1, -1)_v = -1$ holds iff $v = 2$ or ∞. Then Theorem 4 follows from Lemma 6. Note that for $v = \infty$, $-D \notin \mathbf{Q}_\infty^{*2}$ is automatically satisfied as $D > 0$. □

Acknowledgements

I want to thank Miwa Isobe and Ayako Sugawara, both secretaries in my department, for their help. I also want to thank Makoto Matsumoto, my mathematical supervisor, for his useful advice.

REFERENCES

1. H. Maehara, Embedding a set of rational points in lower dimensions, *Discrete Math.* to appear.
2. J. P. Serre, *A Course in Arithmetic*, *GTM*, **7**, Springer-Verlag, New York, 1973.

Received 31 December 1997 and accepted 27 March 1998

T. KUMADA
Department of Mathematics,
Faculty of Science and Technology,
Keio University,
Hiyoshi 3-14-1,
Kohoku-ku, Yokohama 223,
Japan