A 2 × 2 LATTICE SPACE-TIME CODE OF RANK 5

CHAOPING XING AND WEI LI

(Communicated by Wen-Ching Winnie Li)

Abstract. For all previous constructions of 2 × 2 lattice space-time codes with a positive diversity product, the rank was at most 4. In this paper, we give an example of a 2 × 2 lattice space-time code of rank 5 with a positive diversity product.

1. Introduction

In the recent years, there has been a lot of research on space-time codes. Many mathematical subjects such as number theory, algebra, combinatorics, etc., have been employed to construct good lattice codes [1, 2, 3, 5, 6, 7].

Denote by \( M_n(\mathbb{C}) \) the set of \( n \times n \) matrices over \( \mathbb{C} \). A lattice space-time code over \( \mathbb{C} \) is a set \( \mathcal{A} \) consisting of matrices in \( M_n(\mathbb{C}) \) such that \( \mathcal{A} \) is a free abelian group under the matrix addition. The rank of this group is called the dimension or rank of \( \mathcal{A} \).

There are some parameters to measure a lattice space-time code.

Criteria for lattice space-time codes:

(i) the rank of \( \mathcal{A} \) should be as large as possible;
(ii) the diversity product defined by
\[
\delta(\mathcal{A}) := \inf \{ |\det(A - B)| : A, B \in \mathcal{A}, A \neq B \}
\]
should be as large as possible, where \(|·|\) stands for the absolute value of a real number or complex number;
(iii) the discriminant of \( \mathcal{A} \) should be as small as possible (see the definition of the discriminant of a complex lattice below).

A natural question is: what is the maximal rank of a lattice space-time code \( \mathcal{A} \) such that \( \delta(\mathcal{A}) > 0 \)? In other words, we want to determine

\[
r(n) := \max \{ \text{rank}(\mathcal{A}) : \mathcal{A} \text{ is a lattice in } M_n(\mathbb{C}), \delta(\mathcal{A}) > 0 \}.
\]

Determining the exact value for \( r(n) \) seems difficult. One can imagine that it is also not easy to give some reasonable bounds. One obvious lower bound is \( r(n) \geq 2n \) (see \( \S 1 \)). In this paper, we give an upper bound, i.e., \( r(n) \leq 2n^2 \).

Received by the editors August 24, 2007.
2000 Mathematics Subject Classification. Primary 06B99, 15A15, 11Z05, 11H71.

Key words and phrases. Rank, diversity product, lattice.

The first author is supported by Singapore MDE-ARF research grant R60/07 and National Scientific Research Project 973 of the People’s Republic of China, 2004CB318000.
The case \( n = 2 \) is of particular interest. However, even in this case, we only know \( r(n) \geq 4 \), and so far we have not constructed any \( 2 \times 2 \) lattice space-time codes of rank larger than 4 with a positive diversity product. In this paper, we produce an example of a \( 2 \times 2 \) lattice space-time code of rank 5 with a positive diversity product.

2. An upper bound on rank of lattice space-time codes

The main purpose of this section is to give an upper bound on \( r(n) \).

**Lemma 2.1.** Let \( A \) be a lattice space-time code in \( \mathcal{M}_n(\mathbb{C}) \). If the diversity product \( \delta(A) > 0 \), then the rank of \( A \) is at most 2\( n^2 \). Therefore, \( r(n) \leq 2n^2 \).

**Proof.** We can identify the space \( \mathcal{M}_n(\mathbb{C}) \) with \( \mathbb{C}^{n^2} \). Thus, we introduce the usual distance in \( \mathcal{M}_n(\mathbb{C}) \) defined by

\[
d(A, B) = \sqrt{\sum_{i,j} |a_{ij} - b_{ij}|^2}
\]

for two matrices \( A = (a_{ij}) \) and \( B = (b_{ij}) \) in \( \mathcal{M}_n(\mathbb{C}) \). It is clear that we have the obvious inequality.

\[
|d(A, B)| = \left( \sum_{i=1}^{n} \sum_{j=1}^{n} |a_{ij} - b_{ij}|^2 \right)^{1/2} \\
\geq n \left( \prod_{i=1}^{n} \sum_{j=1}^{n} |a_{ij} - b_{ij}|^2 \right)^{1/n^2}^{1/2} \\
= \sqrt{n} |\det(A - B)|^{1/n^2}.
\]

Hence, we have

\[
|\det(A - B)| \leq n^{-n^2/2} |d(A, B)|^{n^2}.
\]

Let \( \{A_1, \ldots, A_t\} \) be a \( \mathbb{Z} \)-basis with \( t = \text{rank}(A) \). Then \( \{A_1, \ldots, A_t\} \) is linearly independent over \( \mathbb{Q} \).

We conclude that \( \{A_1, \ldots, A_t\} \) is linearly independent over \( \mathbb{R} \) as well. Suppose that \( \{A_1, \ldots, A_t\} \) is linearly dependent over \( \mathbb{R} \). Then one of the matrices is a \( \mathbb{R} \)-linear combination of others. We may assume that

\[
A_t = \sum_{i=1}^{t-1} \alpha_i A_i \quad \text{for some } \alpha_i \in \mathbb{R}.
\]

Define the set

\[
T := \left\{ \sum_{i=1}^{t-1} a_i A_i : 0 \leq a_i < 1, \; 1 \leq i \leq t - 1 \right\}.
\]

Then \( T \) is a bounded domain. For each \( m \geq 1 \), by (2.3), we have

\[
m A_t = \sum_{i=1}^{t-1} m \alpha_i A_i = \sum_{i=1}^{t-1} c_i A_i + \sum_{i=1}^{t-1} b_i A_i
\]
Theorem 3.2. Let $t = \text{rank}(A) = \dim_{\mathbb{R}}(A_{\mathbb{R}}) \leq \dim_{\mathbb{R}}(\mathcal{M}_n(\mathbb{C})) = 2n^2$, where $A_{\mathbb{R}} := \{\sum_{i=1}^{t} \alpha_i A_i : \alpha_i \in \mathbb{R}\}$ is the linear space over $\mathbb{R}$ generated by $\{A_1, \ldots, A_t\}$. \hfill $\square$

3. Construction

We need the following result from elementary number theory for this section (see [22] Th. 3 of p. 391).

Lemma 3.1. A positive integer can be expressed as a sum of three squares of integers only if it is not of the form $4^r(8t+7)$ for some integers $r, t \geq 0$.

Consider the five $5 \times 5$ matrices over $\mathbb{C}$:

$$A_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \quad A_2 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}; \quad A_3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix};$$

and

$$A_4 = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}; \quad A_5 = \begin{pmatrix} \sqrt{7} & 0 \\ 0 & -\sqrt{7} \end{pmatrix}.$$

Theorem 3.2. Let $\mathcal{A}$ be the lattice generated by the above five matrices. Then the rank of $\mathcal{A}$ is 5 and the diversity product of $\mathcal{A}$ is 1.

Proof. First of all, we have $\det(A_1) = 1$. Hence, the diversity product of $\mathcal{A}$ is at most 1.

To show that the rank of $\mathcal{A}$ is 5 and the diversity product of $\mathcal{A}$ is at least 1, it is sufficient to prove that for any five integers $a, b, c, d, e$ with $(a, b, c, d, e) \neq (0, 0, 0, 0, 0)$ we have $|\det(A)| \geq 1$ with $A = aA_1 + bA_2 + cA_3 + dA_4 + eA_5$.

It is easy to verify that

$$|\det(A)| = |a^2 + b^2 + c^2 + d^2 - 7e^2 - 2\sqrt{7}bei| = \sqrt{(a^2 + b^2 + c^2 + d^2 - 7e^2)^2 + 28b^2e^2}.$$ 

We can show $|\det(A)| \geq 1$ by distinguishing several cases:

(i) If $be \neq 0$, then we have $|\det(A)| \geq \sqrt{28}$.

(ii) If $e$ is equal to 0, then $|\det(A)| = \sqrt{a^2 + b^2 + c^2 + d^2} \geq 1$. 

with $c_i = ma_i - \lfloor ma_i \rfloor$ and $b_i = \lfloor ma_i \rfloor$. Put $B_m = \sum_{i=1}^{t-1} b_i A_i$ and $C_m = \sum_{i=1}^{t-1} c_i A_i$. Then we have $B_m \in \mathcal{A}$ and $C_m \in \mathcal{T}$. Consider the sequence $\{mA_t - B_m = C_m\}_{m=1}^{\infty} \subset \mathcal{A} \cap \mathcal{T}$. It is clear that all matrices in the sequence are distinct, as $\{A_1, \ldots, A_t\}$ is linearly independent over $\mathbb{Z}$.

Since this sequence is in the bounded domain $\mathcal{T}$, we can find a matrix $D \in \mathcal{M}_n(\mathbb{C})$ such that there is a subsequence $\{C_{m_i}\}_{i=1}^{\infty}$ with a limit

$$\lim_{i \to \infty} C_{m_i} = D.$$ 

Thus, for any $\varepsilon > 0$, there exists $N$ such that $|d(C_{m_N}, C_{m_{N+1}})| \leq \varepsilon$. Hence, by (2.2) we have $|\det(C_{m_N} - C_{m_{N+1}})| \leq \varepsilon$. This implies that $\delta(\mathcal{A}) = 0$. This contradiction means that $\{A_1, \ldots, A_t\}$ is linearly independent over $\mathbb{R}$. The desired result follows from the fact that

$$t = \text{rank}(A) = \dim_{\mathbb{R}}(A_{\mathbb{R}}) \leq \dim_{\mathbb{R}}(\mathcal{M}_n(\mathbb{C})) = 2n^2,$$ 

where $A_{\mathbb{R}} := \{\sum_{i=1}^{t} \alpha_i A_i : \alpha_i \in \mathbb{R}\}$ is the linear space over $\mathbb{R}$ generated by $\{A_1, \ldots, A_t\}$. 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
(iii) Finally we assume that $b = 0$; then $|\det(A)|^2 = |a^2 + c^2 + d^2 - 7e^2|$. Write $e$ into the form $2^t f$ with $f$ being an odd integer. Then $7e^2 = 4^t(7f^2) = 4^t(8t + 7)$ for some $t \geq 0$. By Lemma 2.1, $7e^2$ cannot be equal to $a^2 + c^2 + d^2$. Thus, $|\det(A)|^2 = |a^2 + c^2 + d^2 - 7e^2| > 0$. Since $|\det(A)|^2$ is an integer, we have $|\det(A)|^2 \geq 1$.

This completes the proof. □

Remark 3.3. For our lattice $A$ in Theorem 3.2 the dimension of the tensor product $A \otimes \mathbb{Q}$ has dimension 5 over $\mathbb{R}$. Although there exists a $2 \times 2$ lattice $B$ of rank 8 such that the determinant of difference of every two distinct matrices in $B$ is not vanishing, its inferior limit is still equal to 0. As far as we know, the lattice in this paper is the first $2 \times 2$ one of rank larger than 4 with a positive inferior limit.

By Lemma 2.1 we know that a $2 \times 2$ lattice space-time code with positive diversity is at most 8, and our Theorem 3.2 shows the existence of a $2 \times 2$ lattice space-time code of rank 5 with a positive diversity product. This raises the following question.

Open Problem. Is there a $2 \times 2$ lattice space-time code of rank bigger than 5 with a positive diversity product?

ACKNOWLEDGEMENT

The authors are grateful to Dr. L. J. Xu for some useful comments.

REFERENCES


Division of Mathematical Science, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore 637616, Republic of Singapore

E-mail address: xingcp@ntu.edu.sg

Department of Mathematical Sciences, Tsinghua University, Beijing, People’s Republic of China

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use