Discrete Mathematics 326 (2014) 4–8

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

Note

Existence of a folding in multidimensional coding ☆

Jie Cui, Junying Pei, Pei Yang

Department of Mathematics, Soochow University, Suzhou, 215006, China

ARTICLE INFO

Article history:
Received 21 September 2013
Received in revised form 20 February 2014
Accepted 22 February 2014
Available online 13 March 2014

Keywords:
Lattice tiling
Folding
Smith normal form

ABSTRACT

Folding a sequence into a multidimensional box is an important technique in multidimensional coding. In this paper, the definition of folding defined by T. Etzion is explained from an algebraic point of view, and furthermore, a necessary and sufficient condition is derived for the existence of a folding for any given shape in $\mathbb{Z}^m$.

1. Introduction

Some memory devices, such as page-oriented optical memories [12] and holographic storage [8,9], require that information is stored on two-dimensional surfaces and two-dimensional error patterns must be recovered. Here we refer to errors as burst errors, which mean that errors are confined in a cluster.

Folding is one of important techniques in multidimensional coding. In some recent papers [1–3,6,7,14], one-dimensional burst-correcting codes or error-correcting codes were transferred into two-dimensional codes. Other applications about this technique include synchronization patterns [13], and pseudo-random arrays [4,11]. T. Etzion generalized the definition of folding using lattice tiling in [5]. His definition makes one-dimensional codes feasible not only for multidimensional boxes, but also for many other different shapes. Moreover, all previous known definitions of folding are special cases of his definition.

The rest of this paper is organized as follows. In Section 2 we introduce T. Etzion's definition of folding and explain it from an algebraic point of view. In Section 3 we discuss the existence of a folding for any given shape in $\mathbb{Z}^m$. Finally, the conclusions are given in Section 4.

2. Lattice tiling and folding

We start this section with a short introduction to the lattice tiling.

Let m be a positive integer, $\mathbb{Z}$ be the ring of integers, and $\mathbb{Z}^m$ be the set of all m-tuples over $\mathbb{Z}$. In this paper we always write vectors in $\mathbb{Z}^m$ as column vectors. Any subset S of $\mathbb{Z}^m$ is called an m-dimensional shape. Without loss of generality we assume that the origin is in S. We shall be solely interested in sublattices of $\mathbb{Z}^m$ since our shapes are defined in $\mathbb{Z}^m$. For any vectors $v_1, \dots, v_m \in \mathbb{Z}^m$, if they are linearly independent over $\mathbb{Z}$, then the abelian group $\Lambda = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_m$ is called an m-dimensional lattice, and $\{v_1, \dots, v_m\}$ is called a basis of Λ. Let G be the $m \times m$ matrix with v_i's as its columns, then G is

☆ Supported by the National Nature Science Foundation of China (60603016), and by the National Basic Research Program of China (2006CB 805900).
E-mail address: cuijie@suda.edu.cn (J. Cui).

http://dx.doi.org/10.1016/j.disc.2014.02.019

called a generator matrix of Λ. For an m-dimensional shape S and an m-dimensional lattice Λ, if

$$\begin{cases}(g_1+S)\cap(g_2+S)=\emptyset, \quad \forall g_1,g_2\in\Lambda,\ g_1\neq g_2;\ \text{and}\\ \bigcup_{g\in\Lambda}(g+S)=\mathbb{Z}^m,\end{cases} \tag{1}$$

i.e., disjoint copies of S cover $\mathbb{Z}^m$, we say that (Λ, S) is a lattice tiling of $\mathbb{Z}^m$.

The following definition is due to Etzion [5]. Let (Λ, S) be a lattice tiling of $\mathbb{Z}^m$, and δ be a nonzero vector in $\mathbb{Z}^m$, we define recursively a folded-row starting at the origin. If the point $s \in S$ is the current point in the folded-row, then the next point in the folded-row is defined as follows: If $s+\delta \in S$, then it is the next point; if $s+\delta \in g+S$, a disjoint copy of S, for some $g \in \Lambda$, then $s+\delta-g \in S$ is the next point. If the folded-row defined above includes all the points of S, we say that the triple (Λ, S, δ) defines a folding, and δ is a direction vector.

Now we give a new explanation of the above definition. Clearly, (1) is equivalent to

$$\begin{cases}(s_1+\Lambda)\cap(s_2+\Lambda)=\emptyset, \quad \forall s_1,s_2\in S, s_1\neq s_2;\ \text{and}\\ \bigcup_{s\in S}(s+\Lambda)=\mathbb{Z}^m.\end{cases} \tag{2}$$

Thus, if (Λ, S, δ) defines a folding, then S is a complete set of coset representatives of Λ in $\mathbb{Z}^m$. Moreover, if the elements in the folded-row defined by (Λ, S, δ) are regarded as the elements in the quotient group $\mathbb{Z}^m/\Lambda$, then they form the cyclic group generated by $\delta+\Lambda$, and hence, $\mathbb{Z}^m/\Lambda$ is the cyclic group with $\delta+\Lambda$ as a generator. The converse is also true. Therefore we get the following theorem.

Theorem 1. *Let S be a shape in $\mathbb{Z}^m$, Λ be an m-dimensional lattice, and let δ be a vector in $\mathbb{Z}^m$. Then the triple (Λ, S, δ) defines a folding if and only if $\mathbb{Z}^m/\Lambda$ is the cyclic group with $\delta+\Lambda$ being a generator, and S is a complete set of coset representatives of Λ in $\mathbb{Z}^m$.* □

A nature question is whether there exists a folding for any given shape. We shall discuss this question in the next section.

Actually, a folding (Λ, S, δ) yields an order for the points in the shape S. In multidimensional coding one-dimensional codes are written into the shape S one by one in the order defined by (Λ, S, δ).

3. Existence of a folding

We first introduce some basic properties about matrices over $\mathbb{Z}$. The reader may refer to the chapter 3 of [10] for details. Denote the set of all $m\times m$ matrices over $\mathbb{Z}$ by $Mat_{m\times m}(\mathbb{Z})$. For any $P \in Mat_{m\times m}(\mathbb{Z})$, P is invertible if and only if $\det P = \pm 1$. For any $A \in Mat_{m\times m}(\mathbb{Z})$, there exist invertible matrices $P, Q \in Mat_{m\times m}(\mathbb{Z})$ such that

$$PAQ = \mathrm{diag}\{d_1, \ldots, d_r, 0, \ldots, 0\}, \tag{3}$$

where $r = \operatorname{rank} A$ and $d_1, \ldots, d_r$ are positive integers such that $d_1 \mid d_2 \mid \cdots \mid d_r$. Moreover, the diagonal matrix in (3) is uniquely determined by A, and is called the Smith normal form of A.

By Theorem 1 we know that the existence of a folding for a given shape S completely depends on the existence of a lattice Λ satisfying some conditions, and the direction vector δ only determines the order of the points in the folded-row. Thus the following theorem is immediate.

Theorem 2. *Let S be a shape in $\mathbb{Z}^m$. Then there exists a folding for S if and only if there exists an m-dimensional lattice Λ such that $\mathbb{Z}^m/\Lambda$ is cyclic and S is a complete set of coset representatives of Λ in $\mathbb{Z}^m$.* □

Lemma 1. *Let Λ be an m-dimensional lattice, and let G be a generator matrix of Λ. Then $\mathbb{Z}^m/\Lambda$ is cyclic if and only if the Smith normal form of G is* $\mathrm{diag}\{1, \ldots, 1, n\}$, *where $n = |\det G|$.*

Proof. Assume that $G = (v_1, \ldots, v_m)$. For $i = 1, \ldots, m$, let ε_i be the vector with 1 in the ith position and zeros elsewhere. Then $\{\varepsilon_1, \ldots, \varepsilon_m\}$ is a basis of $\mathbb{Z}^m$, and

$$(v_1, \ldots, v_m) = (\varepsilon_1, \ldots, \varepsilon_m)G.$$

There exist invertible matrices P and Q such that

$$PGQ = \mathrm{diag}\{d_1, \ldots, d_m\},$$

where d_i's are positive integers such that $d_1 \mid \cdots \mid d_m$. Clearly, $|\det G| = d_1 \cdots d_m$. Let

$$(f_1, \ldots, f_m) = (v_1, \ldots, v_m)Q, \qquad (e_1, \ldots, e_m) = (\varepsilon_1, \ldots, \varepsilon_m)P^{-1}. \tag{4}$$

Since Q and P^{-1} are invertible, $\{f_1, \ldots, f_m\}$ is also a basis of Λ, and $\{e_1, \ldots, e_m\}$ is also a basis of $\mathbb{Z}^m$. Moreover,

$$\begin{aligned}(f_1, \ldots, f_m) &= (v_1, \ldots, v_m)Q = (\varepsilon_1, \ldots, \varepsilon_m)GQ\\ &= (\varepsilon_1, \ldots, \varepsilon_m)P^{-1}PGQ = (e_1, \ldots, e_m)\mathrm{diag}\{d_1, \ldots, d_m\},\end{aligned}$$