CHARACTERIZATION OF A CLASS OF PLANAR SELF-AFFINE TILE DIGIT SETS

LI-XIANG AN AND KA-SING LAU

ABSTRACT. We call a finite set $\mathcal{D} \subset \mathbb{Z}^s$ a *(self-affine) tile digit set* with respect to an expanding integral matrix $\mathbf{A}$ if the self-affine set $T(\mathbf{A}, \mathcal{D})$ is a tile in $\mathbb{R}^s$. It has been a widely open problem to characterize the tile digit sets for a given $\mathbf{A}$. While there are substantial investigations on $\mathbb{R}$, there is no result on $\mathbb{R}^s$ other than the case where $|\det \mathbf{A}| = p$ with p a prime. In this paper, we make an initiation to study a basic case $\mathbf{A} = p\mathbf{I}_2$ in $\mathbb{R}^2$. We characterize the tile digit sets by making use of the zeros of the mask polynomial of $\mathcal{D}$ associated with a tile criterion of Kenyon [K], together with a recent result of Iosevich *et al* on factorization of sets in $\mathbb{Z}_p \times \mathbb{Z}_p$ [IMP].

CONTENTS

1. Introduction

Let $\mathbf{A}$ be an $s \times s$ expanding matrix (i.e., all eigenvalues have moduli > 1) with integral entries; let $\mathcal{D} = \{\mathbf{0} = \boldsymbol{d}_0, \boldsymbol{d}_1, \cdots \boldsymbol{d}_{b-1}\} \subset \mathbb{Z}^s$ be a finite set, and call it a *digit set*. The *affine pair* $(\mathbf{A}, \mathcal{D})$ defines an iterated function system $\{\phi_i\}_{i=0}^{b-1}$ with $\phi_i(\boldsymbol{x}) = \mathbf{A}^{-1}(\boldsymbol{x} + \boldsymbol{d}_i)$. It follows that there exists a unique compact set $T := T(\mathbf{A}, \mathcal{D}) \subset \mathbb{R}^s$ (*self-affine set*) satisfying the set-valued relation

$$\mathbf{A}T = T + \mathcal{D}. \tag{1.1}$$

2010 *Mathematics Subject Classification.* Primary 11B75, 52C22; Secondary 11A63, 28A80 .

Key words and phrases. Digit sets, direct summands, mask polynomials, modulus, prime number, spectral sets, self-affine tiles, tile digit sets,zeros.

The research is supported in part by the HKRGC grant and the NNSF of China (no. 11371382 and 11601175).

It is well-known that when T has non-empty interior, then T is a translational tile (Bandt [B]), i.e., there exists a discrete set $\mathcal{J}$ such that

$$T + \mathcal{J} = \mathbb{R}^s \quad \text{and} \quad (T + \boldsymbol{t}_1)^o \cap (T + \boldsymbol{t}_2)^o = \emptyset, \ \ \boldsymbol{t}_1 \neq \boldsymbol{t}_2 \in \mathcal{J}.$$

We call such T a *self-affine tile*, and $\mathcal{D}$ a *tile digit set* with respect to $\mathbf{A}$. In this case, $\#\mathcal{D} = |\det \mathbf{A}|$.

The self-affine tile has its origin in the study of finite automata and recurrent sets ([K], [Th], [R]). The development was strongly motivated by wavelet theory, fractal geometry and geometry of numbers ([AB1,2], [B], [BS], [CT], [GaY], [HL1,2], [KiL1,2], [LgW1-4], [LL], [RWY], [SW]), and the connection with the Fuglede's conjecture on tiles and spectral sets ([F], [T], [Ko], [KoM], [FHL]). Despite the large literature on self-affine tiles, there is a fundamental question that is still widely open:

Question. For a given expanding integral matrix $\mathbf{A}$, characterize the tile digit sets $\mathcal{D}$ of $\mathbf{A}$, i.e., the digit sets $\mathcal{D}$ such that $T(\mathbf{A}, \mathcal{D})$ is a self-affine tile.

If $\mathcal{D}$ is a complete residue set modulus $\mathbf{A}$, then $T(\mathbf{A}, \mathcal{D})$ is a self-affine tile [B]. Kenyon [K] proved that on $\mathbb{R}$, the converse is also true if $\mathbf{A} = [p]$ is a prime; it was extended to $\mathbb{R}^s$ with a mild assumption that $\mathcal{D}$ spans $\mathbb{R}^s$ [HL1] (see also [LgW3] for another more restricted condition). For the non-prime case, Lagarias and Wang [LgW3] enlarged the class of tile digit sets by generalizing a direct sum setup (Odlyzko [O]) to the class of *product-form* digit sets:

$$\mathcal{D} = \mathcal{E}_0 \oplus \mathbf{A}^{\ell_1}\mathcal{E}_1 \cdots \oplus \mathbf{A}^{\ell_k}\mathcal{E}_k \pmod{\mathbf{A}^{\ell_k+1}},$$

where

$$\mathcal{E} = \mathcal{E}_0 \oplus \mathcal{E}_1 \cdots \oplus \mathcal{E}_k,$$

and $\mathcal{E}$ is a complete residue set modulus $\mathbf{A}$. More recently Lai, Rao and one of the author further extended the above form to certain *modulo product-forms* and *higher order modulo product-forms* in $\mathbb{R}$ ([LR], [LLR1,2]). These classes cover all tile digit sets with respect to $\mathbf{A} = [p^l]$ and $[p^r q]$, where p, q are primes, and it is speculated that the higher order modulo product-form may cover all tile digit sets in $\mathbb{R}$. The techniques used are based on the cyclotomic polynomials, and factorization of cyclic groups on $\mathbb{R}$. As there is no suitable extension to higher dimension, we know very little about the structure of tile digit sets in higher dimensional spaces.

In this paper, our main purpose is to initiate a study of the tile digit sets $\mathcal{D}$ in $\mathbb{R}^2$ with respect to $\mathbf{A} = p\mathbf{I}_2$, where p is prime and $\mathbf{I}_2$ is the identity matrix on $\mathbb{R}^2$; necessarily, $\#\mathcal{D} = p^2$. For simplicity, we write $T(p, \mathcal{D}) := T(p\mathbf{I}_2, \mathcal{D})$. The structure of tile digit set $\mathcal{D}$ with respect to $p\mathbf{I}_2$ has closed connection with the decomposition of sets in $\mathbb{Z}_p^2$, which was studied in detail by Iosevich, Mayeli and Pakianatha [IMP]. We call a digit set $\mathcal{W}$ a $\mathbb{Z}_p^2$-*summand* if there is a set $\mathcal{E}$ such that $\mathcal{W} \oplus \mathcal{E}$ is a complete residue set modulus $p\mathbf{I}_2$, and call $\mathcal{E}$ a complementary summand of $\mathcal{W}$. (In [IMP], $\mathcal{W}$

is called a $\mathbb{Z}_p^2$-tile, we use an alternative name to avoid confusion with the tile digit set.) Note that $\mathcal{E}$ is not uniquely defined (see Section 2). We let

$$\mathcal{F}_{\mathcal{W}} = \{\mathcal{E} : \mathcal{E} \text{ is a complementary summand of } \mathcal{W}\}.$$

Our main theorem is:

Theorem 1.1. *Assume $\mathbf{A} = p\mathbf{I}_2$, and the affine pair $(\mathbf{A}, \mathcal{D})$ is primitive. Then $\mathcal{D}$ is a tile digit set with respect to $\mathbf{A}$ if and only if there is an invertible matrix $\mathbf{B} \in M_2(\mathbb{Z})$ with $|\det \mathbf{B}| = 1$ and a $\mathbb{Z}_p^2$-summand $\mathcal{W} = \{\boldsymbol{w}_i\}_{i=0}^{p-1}$ such that*

$$\mathbf{B}\mathcal{D} \equiv \bigcup_{i=0}^{p-1} (\boldsymbol{w}_i + \mathbf{A}^k \mathcal{E}_i) \quad (mod\ \mathbf{A}^{k+1}), \tag{1.2}$$

for some $k \geq 0$, where $\mathcal{E}_i \in \mathcal{F}_{\mathcal{W}}$. In particular, when $k = 0$, then the $\mathcal{E}_i$'s are all identical, and $\mathcal{D}$ is a complete residue set modulus $\mathbf{A}$.

Since $\mathcal{W}$ is a $\mathbb{Z}_p^2$-summand, the $\boldsymbol{w}_i$'s are in different coset modulo $\mathbf{A}$, hence the expression in (1.2) is a disjoint union. When all $\mathcal{E}_i$ is the same, say $\mathcal{E}$, then the digit set

$$\mathcal{D} \equiv \mathcal{W} \oplus \mathbf{A}^k \mathcal{E} \quad (\text{mod } \mathbf{A}^{k+1}),$$

which is a product-form. For the case $p = 2$ or 3, the characterization of the tile digit sets is particularly simple: for $p = 2$, they are complete residue sets with respect to $2\mathbf{I}_2$; for $p = 3$, they are product-forms. These will be proved separately in the remark section.

The sufficiency of Theorem 1.1 is straight forward (Proposition 2.5). The main part is on the necessity. For $\boldsymbol{v} \in \mathbb{Z}^2 \setminus \{\mathbf{0}\}$, we define a projection of $\mathcal{D}$ in the direction of $\boldsymbol{v}$ by

$$\pi_{\boldsymbol{v}}(\mathcal{D}) = \{\langle \boldsymbol{d}, \boldsymbol{v}\rangle : \boldsymbol{d} \in \mathcal{D}\},$$

and let $m_{\mathcal{D}}(\boldsymbol{\xi}) = \sum_{\boldsymbol{d}\in\mathcal{D}} e^{2\pi i\langle \boldsymbol{d},\boldsymbol{\xi}\rangle}$ be the mask polynomial of $\mathcal{D}$. We will use the following relation of $\pi_{\boldsymbol{v}}(\mathcal{D})$ and the zeros of $m_{\mathcal{D}}(\boldsymbol{\xi})$ throughout the paper (Proposition 3.2).

Proposition 1.2. *Let $(\mathbf{A}, \mathcal{D})$ be as the above, then $m_{\mathcal{D}}(\mathbf{A}^{-(k+1)}\boldsymbol{v}) = 0$ if and only if*

$$\pi_{\boldsymbol{v}}(\mathcal{D}) \equiv \{0 = \eta_0, \eta_1, \cdots, \eta_{p-1}\} + p^k\{0, 1, \cdots, p-1\}\ (mod\ p^{k+1}), \tag{1.3}$$

where $0 \leq \eta_i \leq p^k - 1$.

By using the Kenyon's criterion ([K]) of tile digit sets through the zeros of $m_{\mathcal{D}}(\boldsymbol{\xi})$ (Theorem 2.4), and by multiplying an invertible matrix $\mathbf{B}$ with $|\det \mathbf{B}| = 1$ to $\mathcal{D}$ if necessary, we have (Proposition 3.11)

$$\pi_{\boldsymbol{e}_1}(\mathcal{D}) \equiv \{0, \alpha_1, \cdots, \alpha_{p-1}\} + p^{k_1}\{0, 1, \cdots, p-1\} \pmod{p^{k_1+1}},$$
$$\pi_{\boldsymbol{e}_2}(\mathcal{D}) \equiv \{0, \beta_1, \cdots, \beta_{p-1}\} + p^{k_2}\{0, 1, \cdots, p-1\} \pmod{p^{k_2+1}},$$

for some $k_1, k_2 \geq 0$, where $\boldsymbol{e}_1 = (1,0)^t, \boldsymbol{e}_2 = (0,1)^t$. The case that $k_1 = k_2 = 0$ is equivalent to $\mathcal{D}$ being a complete residue set (Corollary 3.10). Our main effort is to consider the case that $k_1, k_2 \geq 1$ and prove that $k_1 = k_2$. For this we use the projection on $\boldsymbol{e}_1$ to decompose the tile digit set $\mathcal{D}$ (Lemma 4.1, Definition 4.2), and show that in this decomposition, the second coordinate match up with the projection on $\boldsymbol{e}_2$ (Section 5). This decomposition eventually yields the expression (1.2) in Theorem 1.1.

For the organization of the paper, in Section 2, we summarize some of the direct sum decomposition of $\mathbb{Z}_p^2$ in [IMP], and prove the sufficiency of Theorem 1.1. In Section 3, we consider the $\pi_{\boldsymbol{v}}(\mathcal{D})$, and lay down the connection with the zeros of the mask polynomial of $\mathcal{D}$. We carry out the decomposition of $\mathcal{D}$ in Section 4, and prove the necessity of the theorem in Section 5. In Section 6, we prove the stronger conclusion for the case $p = 2, 3$, and also give some remarks and outlooks of the related problems.

2. **Preliminaries**

In this section, we will introduce some standard notations and basic facts that are needed. Let p be a prime number, and let $\mathbb{Z}_p^2$ be the quotient group of $\mathbb{Z}_p^2 := \mathbb{Z}^2/p\mathbb{Z}^2$.

Definition 2.1. *We say that $\mathcal{W} \subset \mathbb{Z}_p^2$ is a $\mathbb{Z}_p^2$-summand if there exists $\mathcal{E}$ such that $\mathcal{W} \oplus \mathcal{E} = \mathbb{Z}_p^2$. Note that $\mathcal{E}$ is also a $\mathbb{Z}_p^2$-summand, and call it a* complementary summand *of $\mathcal{W}$.*

It follows that a non-trivial $\mathbb{Z}_p^2$-summand has cardinality p. If we let $\mathcal{W}', \mathcal{E}' \subset \mathbb{Z}^2$ be representations of the above $\mathcal{W}$ and $\mathcal{E}$ respectively, then we have

$$\mathcal{W}' \oplus \mathcal{E}' \oplus p\mathbb{Z}^2 = \mathbb{Z}^2.$$

Hence $\mathcal{W}'$ tiles $\mathbb{Z}^2$ with a tiling set $\mathcal{E}' \oplus p\mathbb{Z}^2$. With a slight abuse of notation for convenience, we use the same $\mathcal{W}$ to mean a set in the quotient group $\mathbb{Z}_p^2$, or its representation in $\mathbb{Z}^2$.

Let $\mathcal{W}$ be a $\mathbb{Z}_p^2$-summand with $\#\mathcal{W} = p$, and let $m_{\mathcal{W}}(\boldsymbol{\xi}) = \sum_{\boldsymbol{w}\in\mathcal{W}} e^{2\pi i\langle \boldsymbol{w}, \boldsymbol{\xi}\rangle}$ be the mask function of $\mathcal{W}$. Let $\mathcal{Z}(g)$ denote the zeros of a function g. It follows that

$$\mathcal{Z}(m_{\mathcal{W}}) \cup \mathcal{Z}(m_{\mathcal{E}}) = \mathcal{Z}(m_{\mathbb{Z}_p^2}) = p^{-1}\mathbb{Z}^2 \setminus \mathbb{Z}^2. \tag{2.1}$$

Therefore there is non-zero $\boldsymbol{v} \in \mathbb{Z}^2 \setminus p\mathbb{Z}^2$ such that $m_{\mathcal{W}}(p^{-1}\boldsymbol{v}) = 0$. According to [IMP, Section 5], a set $\mathcal{W}$ is a $\mathbb{Z}_p^2$-summand if and only if $\mathcal{W}$ is a graph, i.e.,

$$\mathcal{W} = \{x\boldsymbol{e}_1 + f(x)\boldsymbol{e}_2 : x \in \mathbb{Z}_p\}, \tag{2.2}$$

where $\boldsymbol{e}_1, \boldsymbol{e}_2$ is a basis for $\mathbb{Z}_p^2$ and $f : \mathbb{Z}_p \to \mathbb{Z}_p$ is a function. The basis can be chosen from a zero $\boldsymbol{v}$ of $m_{\mathcal{W}}(p^{-1}\boldsymbol{\xi})$ in two cases: (i) if $\langle \boldsymbol{v}, \boldsymbol{v}\rangle \notin p\mathbb{Z}$, let $\boldsymbol{e}_1 = \boldsymbol{v}$, $\boldsymbol{e}_2$ orthogonal to $\boldsymbol{e}_1$; (ii) if $\langle \boldsymbol{v}, \boldsymbol{v}\rangle \in p\mathbb{Z}$, let $\boldsymbol{e}_2 = \boldsymbol{v}$ and let $\boldsymbol{e}_1$ be an element off the line generated by $\boldsymbol{e}_2$ and $\langle \boldsymbol{e}_1, \boldsymbol{e}_2\rangle \in 1 + p\mathbb{Z}$. Also it follows from the expression of $\mathcal{W}$ that $\{\langle \boldsymbol{v}, \boldsymbol{w}\rangle : \boldsymbol{w} \in \mathcal{W}\} \equiv \{0, 1, \cdots, p-1\} (\mathrm{mod}\ p)$. Hence we can obtain a complementary summand by taking $\mathcal{E} \subset \mathbb{Z}_p^2$ to be a line passes through the origin and perpendiculars to $\boldsymbol{v}$. The following example is an illustration of this construction, and shows that such $\mathcal{E}$ is not unique.

Example 2.2. *Let* $\mathcal{W} = \{\mathbf{0}, \begin{bmatrix} 3 \\ 1 \end{bmatrix}, \begin{bmatrix} 4 \\ 0 \end{bmatrix}, \begin{bmatrix} 4 \\ 3 \end{bmatrix}, \begin{bmatrix} 4 \\ 1 \end{bmatrix}\}$,

$$\mathcal{E}_1 = \{0, 1, 2, 3, 4\}\begin{bmatrix} 1 \\ 1 \end{bmatrix}, \quad \mathcal{E}_2 = \{0, 1, 2, 3, 4\}\begin{bmatrix} 1 \\ 3 \end{bmatrix}$$

Then $\mathcal{W}$ *is a* $\mathbb{Z}_5^2$*-summand, and both* $\mathcal{E}_1, \mathcal{E}_2$ *are complementary summands of* $\mathcal{W}$*, and* $\mathcal{F}_{\mathcal{W}} = \{\mathcal{E}_1, \mathcal{E}_2\}$.

Proof: We observe that $m_{\mathcal{W}}(5^{-1}(1, 4)^t) = 0$. Let $\boldsymbol{e}_1 = (1, 4)^t$, and let $\boldsymbol{e}_2 = (1, 1)^t$ (as in case (i) of (2.2)). Then $\{\boldsymbol{e}_1, \boldsymbol{e}_2\}$ forms an orthogonal basis for $\mathbb{Z}_5^2$, and

$$\mathcal{W} = \{x\boldsymbol{e}_1 + f(x)\boldsymbol{e}_2 : x \in \{0, 1, 2, 3, 4\}\},$$

with

$$(f(0), f(1), f(2), f(3), f(4)) = (0, 2, 2, 1, 0).$$

Therefore by the above $\mathcal{W}$ is a $\mathbb{Z}_5^2$-summand. Alternatively, note that $m_{\mathcal{W}}(5^{-1}(2, 1)^t) = 0$ and $\langle (2, 1)^t, (2, 1)^t\rangle = 5$, as in case (ii) of (2.2), we can let $\boldsymbol{e}_2 = (2, 1)^t$, $\boldsymbol{e}_1 = (3, 0)^t$, and express $\mathcal{W}$ in terms of this basis.

Let $\mathcal{E}_1$ and $\mathcal{E}_2$ be as given, they are lines through the origin, perpendicular to $(1, 4)^t$ and $(2, 1)^t$ respectively, they are complementary summands of $\mathcal{W}$. To show that $\mathcal{F}_{\mathcal{W}} = \{\mathcal{E}_1, \mathcal{E}_2\}$, we let $\mathcal{E} \in \mathcal{F}_{\mathcal{W}}$, then $\mathcal{W} \oplus \mathcal{E} = \mathbb{Z}_5^2$ and $\mathcal{E} = \{y\boldsymbol{e}_1' + g(y)\boldsymbol{e}_2' : y \in \mathbb{Z}_5\}$. To determine $\boldsymbol{e}_1'$ and $\boldsymbol{e}_2'$, we note that $Z = \{(1, 0)^t, (1, 1)^t, (1, 2)^t, (0, 1)^t\}$ is a zero set of $m_{\mathcal{E}}(5^{-1}\boldsymbol{\xi})$ (by (2.1)). Similar to the above, we can choose $\boldsymbol{e}_1' = (1, 0)^t$ and $\boldsymbol{e}_2' = (0, 1)^t$ to be a basis of $\mathbb{Z}_5^2$, and for each $\boldsymbol{v} \in Z$,

$$\{\langle y\boldsymbol{e}_1' + g(y)\boldsymbol{e}_2', \boldsymbol{v}\rangle : y \in \mathbb{Z}_5\} \equiv \{0, 1, 2, 3, 4\} \pmod 5.$$

From $\mathbf{0} \in \mathcal{E}$ and $\mathcal{E} \cap \mathcal{W} = \emptyset$, we have $g(0) = 0$ and $g(4) = 2$ or 4. By a direct check, we have for $y = 1, 2, 3$, $g(y) = 3y$ (when $g(4) = 2$) or y (when $g(4) = 4$). This implies either $\mathcal{E} = \mathcal{E}_1$ or $\mathcal{E}_2$. We can check the three other elements in Z (for $\boldsymbol{e}_1' = (1, 2)^t$, use (ii) in (2.2), let $\boldsymbol{e}_2' = (1, 0)^t$), and they end up to be the same $\mathcal{E}_1$ or $\mathcal{E}_2$. $\square$

Remark 1. Note that $\mathcal{E}_1$ is also a $\mathbb{Z}_5^2$-summand with $\mathcal{W}$ as a complementary summand; but $\mathcal{W}$ is not a line in $\mathbb{Z}_5^2$. Therefore the above method of orthogonal line does not determine the class $\mathcal{F}_{\mathcal{E}_1}$ of all complementary summands.

Remark 2. For any $\mathbb{Z}_p^2$-summand, there are at most p^{p-1} complementary summands. In fact, if we let $\mathcal{W} = \left\{\mathbf{0}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 2 \\ 0 \end{bmatrix}, \cdots \begin{bmatrix} p-1 \\ 0 \end{bmatrix}\right\}$, then it has p^{p-1} complementary summands of the form $\mathcal{E} = \left\{\mathbf{0}, \begin{bmatrix} n_1 \\ 1 \end{bmatrix}, \begin{bmatrix} n_2 \\ 2 \end{bmatrix}, \cdots \begin{bmatrix} n_{p-1} \\ p-1 \end{bmatrix}\right\}$, $0 \le n_i \le p-1$.

Let $\mathbf{A} \in M_2(\mathbb{Z})$, for $\boldsymbol{d}, \boldsymbol{d}' \in \mathbb{Z}^2$, we write $\boldsymbol{d} \equiv \boldsymbol{d}'$ (mod $\mathbf{A}$) to mean $\boldsymbol{d} - \boldsymbol{d}' \in \mathbf{A}\mathbb{Z}^2$. For $\mathcal{D}, \mathcal{D}' \subset \mathbb{Z}^2$, we define $\mathcal{D} \equiv \mathcal{D}'$(mod $\mathbf{A}$) similarly; note that in this case $\mathcal{D}$ and $\mathcal{D}'$ may have different cardinalities. We also use $\mathcal{D}_{res}$ (or $\mathcal{D}$(mod $\mathbf{A}$)) to mean the residue set of $\mathcal{D}$ in $\mathbb{Z}^2 \cap \mathbf{A}[0,1)^2$. For the special case $\mathbf{A} = p\mathbf{I}_2$, we will write (mod p) to replace (mod $p\mathbf{I}_2$).

For an affine pair $(\mathbf{A}, \mathcal{D})$, there is a smallest $\mathbf{A}$-invariant sublattice $\mathbb{Z}(\mathbf{A}, \mathcal{D})$ of $\mathbb{Z}^s$ that contains the difference set $\mathcal{D} - \mathcal{D}$. We call a digit set $\mathcal{D}$ *primitive* if $\mathbb{Z}(\mathbf{A}, \mathcal{D}) = \mathbb{Z}^s$, and also call the associated tile $T(\mathbf{A}, \mathcal{D})$ is *primitive tile*. The investigation in [LgW3] shows that every self-affine tile is a primitive tile in essence: there is an invertible matrix $\mathbf{B}$ and an affine pair $(\widetilde{\mathbf{A}}, \widetilde{\mathcal{D}})$ such that $\mathbb{Z}(\widetilde{\mathbf{A}}, \widetilde{\mathcal{D}}) = \mathbb{Z}^s$ and

$$T(\mathbf{A}, \mathcal{D}) = \mathbf{B}T(\widetilde{\mathbf{A}}, \widetilde{\mathcal{D}}).$$

Without loss of generality, we make the assumption that $\mathcal{D}$ is primitive with respect to $\mathbf{A}$ throughout the paper. The following simple fact will be used frequently in the sequel.

Lemma 2.3. *Let $\mathbf{A} = p\mathbf{I}_2$ and $\mathcal{D}$ a primitive tile digit set with respect to $\mathbf{A}$. Then for any invertible matrix $\mathbf{B}$ with $|\det \mathbf{B}| = 1$, $\mathbf{B}\mathcal{D}$ is again a primitive tile digit set with respect to $\mathbf{A}$.*

Proof. It follows from a direct check of (1.1) and $\mathbf{A}$ and $\mathbf{B}$ are commutative. □

For $\mathcal{D} \equiv \mathcal{D}'$ (mod p^k), and $\boldsymbol{d} \in \mathcal{D}$, write $\boldsymbol{d} = \boldsymbol{d}' + p^k\mathbf{n}$ with $\boldsymbol{d}' \in \mathcal{D}', \mathbf{n} \in \mathbb{Z}^2$, then

$$m_{\mathcal{D}}(p^{-k}\boldsymbol{v}) = \sum\nolimits_{\boldsymbol{d}\in\mathcal{D}} e^{2\pi i\langle \boldsymbol{d}', p^{-k}\boldsymbol{v}\rangle} e^{2\pi i\langle \mathbf{n}, \boldsymbol{v}\rangle} = m_{\mathcal{D}'}(p^{-k}\boldsymbol{v}), \quad \boldsymbol{v} \in \mathbb{Z}^2. \tag{2.3}$$

Similarly, if $\boldsymbol{v} \equiv \boldsymbol{v}'$(mod p^k), then $m_{\mathcal{D}}(p^{-k}\boldsymbol{v}) = m_{\mathcal{D}}(p^{-k}\boldsymbol{v}')$.

For any integral expanding matrix $\mathbf{A}$, let $T := T(\mathbf{A}, \mathcal{D})$ be a self-affine set in $\mathbb{R}^2$, and let χ_T be the characteristic function of T. It follows from the functional equation $\mathbf{A}T = T + \mathcal{D}$ that

$$\chi_T(\boldsymbol{x}) = \sum_{\boldsymbol{d}\in\mathcal{D}} \chi_T(\mathbf{A}\boldsymbol{x} - \boldsymbol{d}), \qquad \boldsymbol{x} \in \mathbb{R}^2.$$

By taking Fourier transform of χ_T formally, we have

$$\widehat{\chi}_T(\boldsymbol{\xi}) = m_{\mathcal{D}}((\mathbf{A}^T)^{-1}\boldsymbol{\xi})\widehat{\chi}_{\mathbf{A}^{-1}T}(\boldsymbol{\xi}) = \prod_{k=1}^{\infty} m_{\mathcal{D}}((\mathbf{A}^T)^{-k}\boldsymbol{\xi}).$$

The following theorem, due to Kenyon [K], is a basic criterion for a digit set to define a self-affine tile.

Theorem 2.4. (Kenyon [K]) *The self-affine set $T(\mathbf{A}, \mathcal{D})$ is a tile if and only if for any $\mathbf{0} \neq \boldsymbol{v} \in \mathbb{Z}^s$, there exists an integer $k \geq 1$ such that $m_{\mathcal{D}}((\mathbf{A}^T)^{-k}\boldsymbol{v}) = 0$.*

Let $\mathbf{A} = p\mathbf{I}_2$, then the condition in the theorem reduces to : *for any $\mathbf{0} \neq \boldsymbol{v} \in \mathbb{Z}^2$, there exists a $k \geq 0$ such that $m_{\mathcal{D}}(p^{-(k+1)}\boldsymbol{v}) = 0$* (equivalently $m_{p^{-(k+1)}\mathcal{D}}(\boldsymbol{v}) = 0$). The follow proposition is the sufficiency of Theorem 1.1.

Proposition 2.5. *Let p be a prime integer. Suppose $\mathcal{W} = \{\mathbf{0} = \boldsymbol{w}_0, \boldsymbol{w}_1, \cdots, \boldsymbol{w}_{p-1}\}$ is a $\mathbb{Z}_p^2$-summand, let*

$$\mathcal{D} \equiv \bigcup_{i=0}^{p-1}(\boldsymbol{w}_i + p^k\mathcal{E}_i) \pmod{p^{k+1}}$$

with $\mathcal{E}_i \in \mathcal{F}_{\mathcal{W}}$. Then $T(p, \mathcal{D})$ is a self-affine tile if $k \geq 1$, or if $k = 0$, and the $\mathcal{E}_i$'s are identical.

Proof. For $k = 0$ in the second case, let $\mathcal{E}$ denote the identical $\mathcal{E}_i$'s, then $\mathcal{D} = \mathcal{W} \oplus \mathcal{E}$. Hence $\mathcal{D}$ is a complete residue set modulus $p\mathbf{I_2}$, and is a tile digit set.

To prove the case $k \geq 1$, let $\mathcal{E}_j \in \mathcal{F}_{\mathcal{W}}$, then $\mathcal{D}_j := \mathcal{W} \oplus \mathcal{E}_j$ is a complete residue set modulus $p\mathbf{I}_2$, i.e., $(\mathcal{D}_j)_{res} = \{0, \cdots, p-1\} \times \{0, \cdots, p-1\}$. Then by (2.3)

$$m_{(\mathcal{D}_j)_{res}}(p^{-1}\boldsymbol{v}) = m_{\mathcal{D}_j}(p^{-1}\boldsymbol{v}) = m_{\mathcal{W}}(p^{-1}\boldsymbol{v})m_{\mathcal{E}_j}(p^{-1}\boldsymbol{v}), \quad \forall\ \boldsymbol{v} \in \mathbb{Z}^2.$$

Note that $\mathcal{Z}(m_{(\mathcal{D}_j)_{res}}) = p^{-1}\mathbb{Z}^2 \setminus \mathbb{Z}^2$, therefore for any $\mathcal{E}_j \in \mathcal{F}_{\mathcal{W}}$,

$$\mathcal{Z}(m_{\mathcal{W}}) \cup \mathcal{Z}(m_{\mathcal{E}_j}) = p^{-1}\mathbb{Z}^2 \setminus \mathbb{Z}^2. \tag{2.4}$$

Now, we check the Kenyon criterion (Theorem 2.4) holds on $\mathcal{D}$. In view of (2.3), we can assume without loss of generality, that $\mathcal{D} = \bigcup_{j=0}^{p-1}(\boldsymbol{w}_j + p^k\mathcal{E}_j)$. For any $\boldsymbol{v} \in \mathbb{Z}^2 \setminus \{\mathbf{0}\}$, let $n \geq 0$ be such that $\boldsymbol{v}' = p^{-n}\boldsymbol{v} \in \mathbb{Z}^2 \setminus p\mathbb{Z}^2$. Then by (2.4), either $p^{-1}\boldsymbol{v}' \in \mathcal{Z}(m_{\mathcal{W}})$ or $\in \mathcal{Z}(m_{\mathcal{E}_j})$ for all $\mathcal{E}_j \in \mathcal{F}_{\mathcal{W}}$. In the first case, $p^{-(n+1)}\boldsymbol{v} \in \mathcal{Z}(m_{\mathcal{W}})$, then

$$\begin{aligned} m_{\mathcal{D}}(p^{-(n+1)}\boldsymbol{v}) &= \sum_{j=0}^{p-1} e^{2\pi i\langle \boldsymbol{w}_j,\ p^{-1}\boldsymbol{v}'\rangle} m_{p^k\mathcal{E}_j}(p^{-1}\boldsymbol{v}') \\ &= \sum_{j=0}^{p-1} e^{2\pi i\langle \boldsymbol{w}_j,\ p^{-1}\boldsymbol{v}'\rangle} m_{\mathcal{E}_j}(p^{k-1}\boldsymbol{v}') \\ &= p\sum_{j=0}^{p-1} e^{2\pi i\langle \boldsymbol{w}_j,\ p^{-1}\boldsymbol{v}'\rangle} = pm_{\mathcal{W}}(p^{-1}\boldsymbol{v}') = 0 \end{aligned}$$

(we need $k \geq 1$ in the first identity of the last line). In the second case, $p^{-1}\boldsymbol{v}' \in \mathcal{Z}(m_{\mathcal{E}_j})$ for all $\mathcal{E}_j \in \mathcal{F}_{\mathcal{W}}$. Then $p^{-(n+k+1)}\boldsymbol{v} \in \mathcal{Z}(m_{p^k\mathcal{E}_j})$, and hence

$$m_{\mathcal{D}}(p^{-(n+k+1)}\boldsymbol{v}) = \sum\nolimits_{j=0}^{p-1} e^{2\pi i\langle \boldsymbol{w}_j, p^{-(n+k+1)}\boldsymbol{v}\rangle} m_{p^k\mathcal{E}_j}(p^{-(n+k+1)}\boldsymbol{v}) = 0.$$

By Theorem 2.4, $T(p, \mathcal{D})$ is a self-affine tile. □

3. **Directional projection of $\mathcal{D}$**

In this section, we will set up some preparation work for the proof of the necessity of Theorem 1.1. We assume that $\mathbf{0} \in \mathcal{D}$, and $\mathcal{D}$ is primitive with respect to $\mathbf{A} = p\mathbf{I}_2$. For a digit set $\mathcal{S} \subset \mathbb{Z}^+$, denote $P_{\mathcal{S}}(x) = \sum_{s\in\mathcal{S}} x^s$.

Let $\mathbb{Z}[x]$ ($\mathbb{Z}^+[x]$) denote the set of polynomials with integer (non-negative integer, respectively) coefficients. We use $a \mid b$ to denote a divides b, and $a \nmid b$ means a does not divide b; the notations apply to both integers and polynomials. Let $\Phi_d(x)$ be the *d-th cyclotomic polynomial*, the minimal polynomial of the primitive d-th root of unity, i.e., $\Phi_d(e^{2\pi i/d}) = 0$. Then for a prime p, $\Phi_p(x) = 1 + x + \cdots + x^{p-1}$, and $\Phi_{p^s}(x) = 1 + x^{p^{s-1}} + \cdots + x^{p^{s-1}(p-1)}$.

Lemma 3.1. *Let p be a prime. Suppose $f(x) \in \mathbb{Z}^+[x]$ and has degree less than p^s. If $\Phi_{p^s}(x)|f(x)$, then there exists a polynomial $Q(x) \in \mathbb{Z}^+[x]$ such that*

$$f(x) = \Phi_{p^s}(x)Q(x).$$

Proof. We only need to show that $Q(x)$ has non-negative coefficients. Since by assumption $f(x)$ has degree $\leq p^s - 1$ and $\Phi_{p^s}(x)$ has degree $p^{s-1}(p-1)$, $Q(x)$ has degree $\leq p^{s-1} - 1$. Write

$$f(x) = \sum_{n=0}^{p^s-1} a_n x^n, \quad Q(x) = \sum_{n=0}^{p^{s-1}-1} b_n x^n, \quad a_n \in \mathbb{Z}^+, b_n \in \mathbb{Z}.$$

Then

$$\sum_{n=0}^{p^s-1} a_n x^n = \Phi_{p^s}(x)Q(x) = \sum_{i=0}^{p-1}\sum_{n=0}^{p^{s-1}-1} b_n x^{n+ip^{s-1}}.$$

Note that for any $0 \leq n_1, n_2 \leq p^{s-1} - 1,\ 0 \leq i_1, i_2 \leq p-1$, we have

$$n_1 + i_1p^{s-1} = n_2 + i_2p^{s-1} \iff n_1 = n_2,\ i_1 = i_2.$$

It follows that $a_{n+ip^{s-1}} = b_n \in \mathbb{Z}^+$. This proves $Q(x) \in \mathbb{Z}^+[x]$. □

Assume that $\mathcal{D} \subset \mathbb{Z}^2$ (and $\mathbf{0} \in \mathcal{D}$ by convention). For any $\boldsymbol{v} \in \mathbb{R}^2$, denote

$$\pi_{\boldsymbol{v}}(\mathcal{D}) := \{\langle \boldsymbol{d}, \boldsymbol{v}\rangle : \boldsymbol{d} \in \mathcal{D}\},$$

and call it the *projection of $\mathcal{D}$ in the $\boldsymbol{v}$-direction*, or in short, the *$\boldsymbol{v}$-projection of $\mathcal{D}$*. If $\boldsymbol{v} = \boldsymbol{e}_1 = (1,0)^t$, then we denote $\pi_{\boldsymbol{v}}(\mathcal{D})$ by $\pi_1(\mathcal{D})$.

Proposition 3.2. *Let $\mathcal{D} \subset \mathbb{Z}^2$ be a primitive digit set with respect to $p\mathbf{I}_2$, then $m_{\mathcal{D}}(p^{-(k+1)}\boldsymbol{v}) = 0$ if and only if*

$$\pi_{\boldsymbol{v}}(\mathcal{D}) \equiv \{0 = \eta_0, \eta_1, \cdots, \eta_{s-1}\} + p^k\{0, 1, \cdots, p-1\} \ (mod\ p^{k+1}), \tag{3.1}$$

where $s \geq 1$ and $0 \leq \eta_i \leq p^k - 1$.

Remark. Note that the $\langle \boldsymbol{d}, \boldsymbol{v}\rangle$ can be positive or negative, but the entries on the right side are always nonnegative; also note that the η_i's can be identical.

Proof. Let $\mathcal{A} \equiv \pi_{\boldsymbol{v}}(\mathcal{D}) \pmod{p^{k+1}}$ with $\mathcal{A} \subset \{0, 1, \cdots, p^{k+1} - 1\}$. Then

$$P_{\mathcal{A}}(e^{2\pi i/p^{k+1}}) = \sum_{d\in\mathcal{A}} e^{2\pi i p^{-(k+1)}d} = \sum_{d\in\pi_{\boldsymbol{v}}(\mathcal{D})} e^{2\pi i p^{-(k+1)}d} = m_{\mathcal{D}}(p^{-(k+1)}\boldsymbol{v}) = 0.$$

This implies $\Phi_{p^{(k+1)}}(x)|P_{\mathcal{A}}(x)$. By Proposition 3.1, there is a polynomial $Q(x) \in \mathbb{Z}^+[x]$ such that

$$P_{\mathcal{A}}(x) = \Phi_{p^{k+1}}(x)Q(x).$$

Since $s := Q(1)$ is a positive integer, we can write $Q(x) = \sum_{i=0}^{s-1} x^{\eta_i}, \eta_0 = 0$ (η_i may be repeated); furthermore $0 \leq \eta_i \leq p^k - 1$ (as $P_{\mathcal{A}}$ has degree $\leq p^{k+1} - 1$ and $\Phi_{p^{k+1}}(x) = \sum_{j=0}^{p-1} x^{jp^k}$). We conclude that

$$\mathcal{A} = \{0, \eta_1, \cdots, \eta_{s-1}\} + p^k\{0, 1, \cdots, p-1\}.$$

For the sufficiency, we observe that the expression of $\pi_{\boldsymbol{v}}(\mathcal{D})$ in (3.1) implies that $P_{\mathcal{A}}(x) = \Phi_{p^{k+1}}(x)Q(x)$ where $Q(x) = \sum_{i=0}^{s-1} x^{\eta_i}$. It follows that $p^{-(k+1)}$ is a root of $P_{\mathcal{A}}(x)$, so that $p^{-(k+1)}\boldsymbol{v}$ is a root of $m_{\mathcal{D}}(\boldsymbol{\xi})$. □

Note that Proposition 3.2 implies that if the zero set of $m_{\mathcal{D}}(\boldsymbol{\xi})$ is nonempty, then $p|\#\mathcal{D}$. Let $\boldsymbol{v} = (n, m)^t$ be such that $m_D(p^{-(k+1)}\boldsymbol{v}) = 0$, and without loss of generality, we assume that $\#\mathcal{D} = ps$ where s is as in (3.1). Let $\mathbf{B} = \begin{bmatrix} n & m \\ 0 & 1 \end{bmatrix}$. Consider $\mathbf{B}\mathcal{D}$, it changes the first coordinate of $\mathcal{D}$, but keep the second coordinate unchanged, and

$$\pi_1(\mathbf{B}\mathcal{D}) = \pi_{\boldsymbol{v}}(\mathcal{D}) \equiv \{0 = \eta_0, \eta_1, \cdots, \eta_{s-1}\} + p^k\{0, 1, \cdots, p-1\} \pmod{p^{k+1}}.$$

Corollary 3.3. *Let $\mathcal{D} \subset \mathbb{Z}^2$ be as in Proposition 3.2. Suppose there is $\boldsymbol{v} = (1, m)^t$ such that $m_{\mathcal{D}}(p^{-(k+1)}\boldsymbol{v}) = 0$ for some $k \geq 1$, then $\eta_i \neq 0$ for some i.*

Proof. Let $\mathbf{B} = \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix}$ be the matrix defined by $\boldsymbol{v}$. By assumption, $\mathcal{D}$ is a primitive digit set with respect to $p\mathbf{I}_2$. Since $\det \mathbf{B} = 1$, $\mathbf{B}\mathcal{D}$ is also a primitive digit set with respect to $p\mathbf{I}_2$. If $\eta_i = 0$ for all i, then we have

$$\pi_1(\mathbf{B}\mathcal{D}) \equiv p^k\{0, 1, \cdots, p-1\} \pmod{p^{k+1}} \quad \text{with } k \geq 1.$$

Hence the first coordinate of $\mathbf{B}\mathcal{D}$ is contained in $p^k\mathbb{Z}$. This implies that $\mathbf{B}\mathcal{D}$ cannot be a primitive digit set with respect to $p\mathbf{I}_2$, a contradiction. □

By Proposition 3.2 and its proof, we obtain a preliminary decomposition of $\mathbf{B}\mathcal{D}$ through its first coordinate.

Corollary 3.4. *Let $\mathcal{D} \subset \mathbb{Z}^2$ be as in Proposition 3.2, and let $\mathbf{B}$ be defined by $\boldsymbol{v} = (n, m)^t$ as the above. Assume that $m_{\mathcal{D}}(p^{-(k+1)}\boldsymbol{v}) = 0, k \geq 0$. Then $\mathbf{B}\mathcal{D}$ admits a decomposition $\mathbf{B}\mathcal{D} = \bigcup_{i=1}^{s-1} \mathcal{D}_i$ where*

$$\mathcal{D}_i = \Big\{ \begin{bmatrix} \eta_i + p^{k+1}n_0 \\ d_{i,0} \end{bmatrix}, \begin{bmatrix} \eta_i + p^k + p^{k+1}n_1 \\ d_{i,1} \end{bmatrix}, \cdots, \begin{bmatrix} \eta_i + p^k(p-1) + p^{k+1}n_{p-1} \\ d_{i,p-1} \end{bmatrix} \Big\},$$

and $m_{\mathcal{D}_i}(p^{-(k+1)}\boldsymbol{e}_1) = 0$.

Let

$$V = \{(n, m)^t : n \in \mathbb{Z} \setminus p\mathbb{Z}, m \in \mathbb{Z}\}, \quad V_1 = \{(1, m)^t : m \in \mathbb{Z}\}.$$

Clearly, the condition in Kenyon's criterion is equivalent to $V \cup \widetilde{V} \subset \bigcup_{k\geq 0} \mathcal{Z}(m_{p^{-(k+1)}\mathcal{D}})$ for $\mathbf{A} = p\mathbf{I}_2$, where $\widetilde{V} = \{(m, n)^t : (n, m)^t \in V\}$.

Lemma 3.5. *For $\boldsymbol{v} \in V$, $p^{-(k+1)}\boldsymbol{v}$ is a root of $m_{\mathcal{D}}(\boldsymbol{\xi})$ if and only if $p^{-(k+1)}\boldsymbol{v}_1$ is a root $m_{\mathcal{D}}(\boldsymbol{\xi})$ for some $\boldsymbol{v}_1 \in V_1$.*

Proof. We only need to prove the necessity. For $\boldsymbol{v} = (n, m)^t \in V$, since n and p^{k+1} are co-prime, there exist integers t_1, t_2 such that $nt_1 + p^{k+1}t_2 = m$; hence $p^{-(k+1)}(0, nt_1 - m) \in \mathbb{Z}^2$. For $\boldsymbol{v}_1 = (1, t_1)^t$,

$$\begin{aligned} m_{\mathcal{D}}(p^{-(k+1)}n\boldsymbol{v}_1) &= m_{\mathcal{D}}(p^{-(k+1)}\boldsymbol{v} + p^{-(k+1)}(0, nt_1 - m)^t) \\ &= m_{\mathcal{D}}(p^{-(k+1)}\boldsymbol{v}) \\ &= 0. \end{aligned}$$

Since n is not a factor of p, we see that $p^{-(k+1)}\boldsymbol{v}_1$ is a root of $m_{\mathcal{D}}(\boldsymbol{\xi})$ as well. □

Hence to consider the zeros of $m_{\mathcal{D}}(\boldsymbol{\xi})$, we can use V and V_1 interchangeably. We define the following condition on $m_{\mathcal{D}}(\boldsymbol{\xi})$ which fulfils part of the condition in the Kenyon criterion.

$(*)$ *For every $\boldsymbol{v} \in V_1$, there exists $k > 0$ such that $m_{\mathcal{D}}(p^{-(k+1)}\boldsymbol{v}) = 0$.*

We use $k_{\boldsymbol{v}}$ to denote the smallest k such that $m_{\mathcal{D}}(p^{-(k+1)}\boldsymbol{v}) = 0$. Note that $k_{\boldsymbol{v}} = 0$ for all $\boldsymbol{v} \in V_1$ is equivalent to $m_{\mathcal{D}}(p^{-1}V_1) = 0$. Let

$$\mathcal{C} = \{\mathbf{0}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \cdots, \begin{bmatrix} p-1 \\ 0 \end{bmatrix}\}.$$

Then $m_{\mathcal{C}}(p^{-1}V_1) = 0$. In the following, we will discuss the relation of $m_{\mathcal{D}}(p^{-1}V_1) = 0$ and $\mathcal{C}$ is a direct summand in $\mathcal{D}_{res}$ (recall that $\mathcal{D}_{res}$ is defined as $\mathcal{D}(\text{mod } p) \subset \mathbb{Z}^2 \cap p[0,1)^2$).

Proposition 3.6. *Let $\mathcal{D} \subset \mathbb{Z}^2$ be a primitive digit set with respect to $p\mathbf{I}_2$, and by translation, assume that $\mathbf{0} \in \mathcal{D}_{res}$ has the largest number of repetition. Then the following are equivalent:*

(i) $k_{\boldsymbol{v}} = 0$ for all $\boldsymbol{v} \in V_1$ (or V);

(ii) $\mathcal{D}$ satisfies condition $(*)$, and $\mathcal{C} \subset \mathcal{D}_{res}$;

(iii) there are $0 \le d_i \le p-1$ (they may be equal) such that

$$\mathcal{D}_{res} = \left\{\mathbf{0}, \begin{bmatrix} 0 \\ d_1 \end{bmatrix} \cdots \begin{bmatrix} 0 \\ d_{s-1} \end{bmatrix}\right\} + \mathcal{C}. \tag{3.2}$$

Remark. The condition on $\mathcal{D}_{res}$ has no essential significance. Without that, we change the $\mathcal{D}_{res}$ in (ii), (iii) by a shift of the digits.

Proof. (i) $\Rightarrow$ (ii) We need only show the second part of (ii). Denote

$$\mathcal{D}_0 := \{\boldsymbol{d} \in \mathcal{D} : \langle \boldsymbol{d}, (1,m)^t \rangle \equiv 0 \text{ (mod } p) \text{ for some } 0 \le m \le p-1\}.$$

It is easy to check by definition that

$$(\mathcal{D}_0)_{res} = \{\mathbf{0}\} \cup \{\begin{bmatrix} x \\ y \end{bmatrix} \in \mathcal{D}_{res} : y \ne 0\}.$$

Let ℓ denote the number of repetition of $\mathbf{0} \in \mathcal{D}_{res}$, and is largest by assumption. As $m_{\mathcal{D}}(p^{-1}\boldsymbol{v}) = 0$, Proposition 3.2 implies that

$$\pi_{\boldsymbol{v}}(\mathcal{D}) \equiv \underbrace{\{0, \cdots, 0\}}_{s} + \{0, 1, \cdots, p-1\} \text{ (mod } p).$$

Therefore, each $0 \le m \le p-1$ corresponding to exactly s elements in $\mathcal{D}_0$: ℓ of them $\equiv \mathbf{0}$ (mod p), and $s-\ell$ of them do not. Hence $\#\mathcal{D}_0 = \ell + (s-\ell)p$. Let $\mathcal{D}_0^c = \mathcal{D} \setminus \mathcal{D}_0$, then

$$\pi_2((\mathcal{D}_0^c)_{res}) = \{0\}, \quad \#\mathcal{D}_0^c = sp - (\ell + (s-\ell)p) = \ell(p-1) > 0. \tag{3.3}$$

If $p = 2$, then it follows from the first part of (3.3) that $(\mathcal{D}_0^c)_{res} = \left\{\begin{bmatrix} 1 \\ 0 \end{bmatrix}\right\}$, and hence $\mathcal{C} = \left\{\mathbf{0}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}\right\} \subset \mathcal{D}_{res}$. For the case $p > 2$, we divide our consideration into two cases:

Case 1. $\ell = s$, then $\mathcal{D}_0 \equiv \{\mathbf{0}\} \pmod p$. Hence

$$\pi_2(\mathcal{D}) = \pi_2(\mathcal{D}_0) \cup \pi_2(\mathcal{D}_0^c) \equiv \{0\} \pmod p.$$

As $k_{\boldsymbol{e}_1} = 0$ (i.e., $m_{\mathcal{D}}(p^{-1}\boldsymbol{e}_1) = 0$), we have

$$\pi_1(\mathcal{D})(\text{mod } p) = \pi_1(\mathcal{D}_{res}) = \underbrace{\{0, \cdots, 0\}}_{s} + \{0, 1, \cdots, p-1\}.$$

The two identities imply $\mathcal{D}_{res} = \underbrace{\{\mathbf{0}, \cdots, \mathbf{0}\}}_{s} + \mathcal{C}$.

Case 2. $\ell < s$. Assume the contrary, $\mathcal{C} \nsubseteq \mathcal{D}_{res}$, we prove that there is a $\boldsymbol{d} \in \mathcal{D}$ such that $\mathcal{D} - \boldsymbol{d}$ contains at least $\ell + 1$ elements $\equiv \mathbf{0} \pmod p$, a contradiction.

As $\mathcal{C} \nsubseteq \mathcal{D}_{res}$, there is an $x_0 \in \{1, \cdots, p-1\}$ and $(x_0, 0)^t \notin \mathcal{D}_{res}$. This together with (3.3) yield

$$(\mathcal{D}_0^c)_{res} \subset \Big\{ \begin{bmatrix} x \\ 0 \end{bmatrix} : x \in \{1, \cdots, p-1\} \setminus \{x_0\} \Big\}.$$

As $\#\mathcal{D}_0^c = \ell(p-1)$ and $p > 2$ by assumption, the pigeon hole principle implies that there must be an $x \in \{1, \cdots, p-1\}$ such that $\mathcal{D}_0^c$ contains at least $\ell + 1$ elements $\equiv (x, 0)^t (\text{mod } p)$. Choose one from them, say $\boldsymbol{d}$. Then $\mathcal{D} - \boldsymbol{d}$ contains at least $\ell + 1$ elements $\equiv \mathbf{0} \pmod p$, and completes the proof.

(ii) $\Rightarrow$ (iii) We show that $\mathcal{D}_{res}$ has the form in (3.2) by induction on s. It is trivial for $s = 1$. Suppose the statement is true for $k \le s-1$. For the case s. By assumption, there is a subset $\mathcal{D}_1$ of $\mathcal{D}$ satisfies $(\mathcal{D}_1)_{res} = \mathcal{C}$. Denote $\mathcal{D}_2 := \mathcal{D} \setminus \mathcal{D}_1$, then $\#\mathcal{D}_2 = (s-1)p$. For any $\boldsymbol{v} \in V_1$,

$$\begin{aligned} 0 &= m_{\mathcal{D}}(p^{-1}\boldsymbol{v}) \\ &= m_{\mathcal{D}_1}(p^{-1}\boldsymbol{v}) + m_{\mathcal{D}_2}(p^{-1}\boldsymbol{v}) \\ &= m_{\mathcal{C}}(p^{-1}\boldsymbol{v}) + m_{\mathcal{D}_2}(p^{-1}\boldsymbol{v}) \\ &= m_{\mathcal{D}_2}(p^{-1}\boldsymbol{v}). \end{aligned}$$

By translating a $\boldsymbol{d} \in \mathcal{D}_2$ with $\mathbf{0} \in \mathcal{D}_2 - \boldsymbol{d}$ and by induction, we have $m_{\mathcal{D}_2 - \boldsymbol{d}}(p^{-1}\boldsymbol{v}) = 0$. By induction,

$$(\mathcal{D}_2)_{res} = \Big\{ \begin{bmatrix} 0 \\ d_1 \end{bmatrix}, \cdots \begin{bmatrix} 0 \\ d_{s-1} \end{bmatrix} \Big\} + \mathcal{C},$$

for some $d_i \in \{0, 1, \cdots, p-1\}$, and

$$\mathcal{D}_{res} = (\mathcal{D}_1)_{res} \cup (\mathcal{D}_2)_{res} = \Big\{ \mathbf{0}, \begin{bmatrix} 0 \\ d_1 \end{bmatrix}, \cdots \begin{bmatrix} 0 \\ d_{s-1} \end{bmatrix} \Big\} + \mathcal{C}.$$

(iii) $\Rightarrow$ (i) It follows from a direct check. $\square$

In Proposition 3.8, we show that the condition in Proposition 3.6(i) is implied by $k_{\boldsymbol{e}_1} = 0$ where $\boldsymbol{e}_1 = (1, 0)^t$. We need a lemma.

Lemma 3.7. *Suppose $\mathcal{D}$ satisfies condition $(*)$, and $\#\mathcal{D} = p$, then $\mathcal{D}_{res} = \mathcal{C}$ if and only if $k_{\boldsymbol{e}_1} = 0$.*

Proof. The necessity follows directly check of $m_{\mathcal{C}}(p^{-1}\boldsymbol{e}_1)$. For the sufficiency, we observe that if $\#\mathcal{D} = p$, then by condition $(*)$ and Proposition 3.2, we have for any $\boldsymbol{v} \in V$, there is $k > 0$ such that

$$\pi_{\boldsymbol{v}}(\mathcal{D}) \equiv p^k\{0, 1, \cdots, p-1\} \pmod{p^{k+1}}.$$

Note that $\#\pi_{\boldsymbol{v}}(\mathcal{D}) = p$. In particular, for $k_{\boldsymbol{e}_1} = 0$, we have

$$\pi_1(\mathcal{D}) \equiv \{0, 1, \cdots, p-1\} \pmod{p}.$$

If $\mathcal{D}_{res} \neq \mathcal{C}$, then there is $0 \leq j \leq p-1$ such that $\begin{bmatrix} j \\ 0 \end{bmatrix} \notin \mathcal{D}_{res}$. Therefore there is $\begin{bmatrix} d_1 \\ d_2 \end{bmatrix} \in \mathcal{D}$ with $d_1 = j + pn$ and $d_2 \in \mathbb{Z} \setminus p\mathbb{Z}$. Then $\boldsymbol{v} = (d_2, -d_1)^t \in V$ and $\langle \boldsymbol{v}, \begin{bmatrix} d_1 \\ d_2 \end{bmatrix} \rangle = 0$. Hence $\#\pi_{\boldsymbol{v}}(\mathcal{D}) < p$, a contradiction. Hence $\mathcal{D}_{res} = \mathcal{C}$. □

Proposition 3.8. *Suppose $\mathcal{D}$ with $\#\mathcal{D} = sp < p^2$ satisfies property $(*)$, and $k_{\boldsymbol{e}_1} = 0$, then condition (i) in Proposition 3.6 is satisfied, i.e., $k_{\boldsymbol{v}} = 0$ for all $\boldsymbol{v} \in V_1$.*

Proof. In view of Proposition 3.6, it suffices to prove $\mathcal{C} \subset \mathcal{D}_{res}$ here. When $s = 1$, the conclusion follows from Lemma 3.7. For $s > 1$, we prove that if $\mathcal{C} \nsubseteq \mathcal{D}_{res}$, then there is a $\widetilde{\mathcal{D}}$ satisfies the conditions in Lemma 3.7, and $\mathcal{C} \nsubseteq \widetilde{\mathcal{D}}_{res}$. It is impossible.

By Proposition 3.6, if $\mathcal{C} \nsubseteq \mathcal{D}_{res}$, then there exists $\boldsymbol{v}_0 = (1, m_0)$ such that $k_0 := k_{\boldsymbol{v}_0} \geq 1$. Corollary 3.3 implies that there exist i such that $\eta := \eta_i^{(\boldsymbol{v}_0)} \neq 0$. Let $\mathbf{B} = \begin{bmatrix} 1 & m_0 \\ 0 & 1 \end{bmatrix}$ and consider $\mathbf{B}\mathcal{D}$, then we can use

$$\pi_1(\mathbf{B}\mathcal{D}) = \pi_{\boldsymbol{v}_0}(\mathcal{D}) \equiv \{0 = \eta_0, \eta_1, \cdots, \eta_{s-1}\} + p^{k_0}\{0, 1, \cdots, p-1\} \pmod{p^{k_0+1}}$$

to partition $\mathbf{B}\mathcal{D}$ according to its first coordinate (see Corollary 3.4):

$$\mathbf{B}\mathcal{D} = \begin{bmatrix} p^{k_0} & 0 \\ 0 & 1 \end{bmatrix}\mathcal{D}'_0 \cup \cdots \cup \left(\begin{bmatrix} \eta_{s-1} \\ 0 \end{bmatrix} + \begin{bmatrix} p^{k_0} & 0 \\ 0 & 1 \end{bmatrix}\mathcal{D}'_{s-1} \right), \tag{3.4}$$

and $m_{\mathcal{D}'_i}(p^{-1}\boldsymbol{e}_1) = 0$. Let $\mathcal{D}'$ be the union of those $\mathcal{D}'_i$ with $\eta_i = 0$. Then $\#\mathcal{D}' = s'p$ with $s' < s$. Then we have

(i) $\mathcal{D}'$ satisfies condition $(*)$. Indeed for any $\boldsymbol{v} = (1, m) \in V_1$, let $\boldsymbol{v}' = (1, m_0 + p^{k_0}m)^t$. Because $\boldsymbol{v}' \equiv \boldsymbol{v}_0 \pmod{p^{k_0}}$, we have, for $k \leq k_0$,

$$m_{\mathcal{D}}(p^{-k}\boldsymbol{v}') = m_{\mathcal{D}}(p^{-k}\boldsymbol{v}_0) \neq 0$$

(by the statement after (2.3)). This implies $k_{\boldsymbol{v}'} \geq k_0$. In view of Corollary 3.4 and the expression of $\mathcal{D}'_i$, we have $m_{\mathcal{D}'}(p^{-(k_{\boldsymbol{v}'}-k_0+1)}\boldsymbol{v}) = 0$.

(ii) $\mathcal{C} \nsubseteq \mathcal{D}'_{res}$. For otherwise, $\mathcal{C} \subseteq \mathcal{D}'_{res}$. Consider

$$\mathbf{B}^{-1}\begin{bmatrix} p^{k_0} & 0 \\ 0 & 1 \end{bmatrix}\mathcal{C} \subset \mathbf{B}^{-1}\begin{bmatrix} p^{k_0} & 0 \\ 0 & 1 \end{bmatrix}\mathcal{D}'_{res}.$$

It follows from (3.4) that there is a subset of p elements in $\mathbf{B}^{-1}\begin{bmatrix} p^{k_0} & 0 \\ 0 & 1 \end{bmatrix}\mathcal{D}'$ $(\subseteq \mathcal{D})$ such that the first coordinates are 0 modulus p. But $k_{\boldsymbol{e}_1} = 0$ implies

$$\pi_1(\mathcal{D}) \equiv \underbrace{\{0, \cdots, 0\}}_{s} + \{0, \cdots, p-1\} \pmod{p},$$

and $s < p$ by assumption. It is impossible.

It follows that $\mathcal{D}'$ satisfies condition $(*)$ and $\mathcal{C} \nsubseteq \mathcal{D}'_{res}$. Then we reduce s to s'. By applying the same discussion on $\mathcal{D}'$, and repeat, we can eventually get a digit set $\mathcal{D}'' \subseteq \mathcal{D}$ with $\#\mathcal{D}'' = p$ with condition $(*)$, and $\mathcal{C} \nsubseteq \mathcal{D}''_{res}$, a contradiction to Lemma 3.7. □

Proposition 3.8 does not hold if we remove the condition $\#\mathcal{D} < p^2$.

Example 3.9. *Let $\mathcal{W}$ and $\mathcal{E}_1$ be defined as in Example 2.2 and $\mathcal{D} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}(\mathcal{W} + 5\mathcal{E}_1)$. Then $\mathcal{D}$ is a product-form, hence it is a tile digit and has property $(*)$ (Theorem 2.4). Observe that*

$$m_{\mathcal{D}}(5^{-1}\boldsymbol{e}_1) = m_{\mathcal{W}}(5^{-1}(1,-1)^t) = 0, \quad \textit{but} \quad m_{\mathcal{D}}(5^{-1}(1,1)^t) = m_{\mathcal{W}}(5^{-1}\boldsymbol{e}_1) \neq 0.$$

Hence, the conclusion in Proposition 3.8 does not hold. □

If we replace V and V_1 by $\widetilde{V}$ and $\widetilde{V}_1$ respectively, then the above results also hold by adjusting to the second coordinate. As a direct consequence of Proposition 3.6, we have

Corollary 3.10. *Suppose $\mathcal{D}$ is a primitive tile digit set with respect to $p\mathbf{I}_2$ Then $\mathcal{D}$ is a complete residue set (mod p) if and only if $k_{\boldsymbol{v}},\ k_{\boldsymbol{v}'} = 0$ for all $\boldsymbol{v} \in V_1$, $\boldsymbol{v}' \in \widetilde{V}_1$.*

The following proposition shows that when the tile digit set is not a complete residue set (mod p), then by a suitable linear transform of the tile digit set $\mathcal{D}$, we have $k_{\boldsymbol{e}_i} \geq 1$ for $i = 1, 2$.

Proposition 3.11. *Let $\mathcal{D}$ be a primitive tile digit set with respect to $\mathbf{A} = p\mathbf{I}_2$, and is not a complete residue set (mod p). Then there is an invertible matrix $\mathbf{B} \in M_2(\mathbb{Z})$ with $|\det \mathbf{B}| = 1$ such that $\boldsymbol{e}_1 = (1,0)^t$ and $\boldsymbol{e}_2 = (0,1)^t$ are the zeros of $m_{p^{-k_i-1}\mathbf{B}\mathcal{D}}$ for some $k_i \geq 1, i = 1, 2$ respectively.*

Proof. By assumption and Corollary 3.10, there is a $\boldsymbol{v}_1 \in V_1$ (or $\widetilde{V}_1$) which is a zero of $m_{p^{-(k_1+1)}\mathcal{D}}$ for some $k_1 \geq 1$. Without loss of generality, we assume $\boldsymbol{v}_1 = (1, n_1) \in V_1$. Let $\mathbf{B}_1 = \begin{bmatrix} 1 & n_1 \\ 0 & 1 \end{bmatrix}$. Then $\mathbf{B}_1\mathcal{D}$ is also a primitive digit set, and

$$\begin{aligned} \pi_1(\mathbf{B}_1\mathcal{D}) &= \pi_{\boldsymbol{v}_1}(\mathcal{D}) \\ &\equiv \{0, \eta_1, \cdots, \eta_{p-1}\} + p^{k_1}\{0, 1, \cdots, p-1\} \pmod{p^{k_1+1}}, \end{aligned} \tag{3.5}$$

with $0 \le \eta_i \le p^{k_1} - 1$, and p is not a common factor of $\{\eta_i\}_{i=0}^{p-1}$ by primitive and $k_1 \ge 1$.

We claim that there is a $\boldsymbol{v}_2 \in \widetilde{V}_1 = \{(m, 1)^t : m \in \mathbb{Z}\}$ such that $k_2 \ge 1$. If otherwise, $\widetilde{V}_1$ is a zero set of $m_{p^{-1}\mathbf{B}_1\mathcal{D}}$. According to Proposition 3.6 (apply to the second coordinate), $\mathbf{B}_1\mathcal{D}$ has the form

$$\mathbf{B}_1\mathcal{D} \equiv \left\{\mathbf{0}, \begin{bmatrix} \eta_1 \\ 0 \end{bmatrix}, \cdots \begin{bmatrix} \eta_{p-1} \\ 0 \end{bmatrix}\right\} + \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\mathcal{C} \pmod{p}. \tag{3.6}$$

On the other hand, we can write $\mathbf{B}_1\mathcal{D}$ according to its first coordinate in (3.5),

$$\mathbf{B}_1\mathcal{D} = \begin{bmatrix} p^{k_1} & 0 \\ 0 & 1 \end{bmatrix}\mathcal{D}_0 \cup \cdots \cup \left(\begin{bmatrix} \eta_{p-1} \\ 0 \end{bmatrix} + \begin{bmatrix} p^{k_1} & 0 \\ 0 & 1 \end{bmatrix}\mathcal{D}_{p-1}\right).$$

Let $\mathcal{D}'$ be the union of those $\mathcal{D}_i$ with $\eta_i = 0$. Then $\mathcal{C} \nsubseteq \mathcal{D}'_{res}$ (by (3.6)), and $\mathcal{D}'$ satisfies (*) (by the proof of Proposition 3.8). As $m_{\mathbf{B}_1\mathcal{D}}(p^{-(k_1+1)}\boldsymbol{e}_1) = 0$, by Corollary 3.4,

$$m_{\mathcal{D}_i}(p^{-1}\boldsymbol{e}_1) = 0.$$

Hence $k_1^{(\mathcal{D}')} = 0$, and $\mathcal{C} \subseteq \mathcal{D}'_{res}$ (by Proposition 3.6) a contradiction. Hence, there is a $\boldsymbol{v}_2 = (n_2, 1)^t$ such that $k_2 \ge 1$. Let

$$\mathbf{B} = \begin{bmatrix} 1 & 0 \\ n_2 & 1 \end{bmatrix}\mathbf{B}_1.$$

It follows that $\boldsymbol{e}_1 = (1, 0)^t$ and $\boldsymbol{e}_2 = (0, 1)^t$ are the zeros of $m_{p^{-k_i-1}\mathbf{B}\mathcal{D}}$ as asserted in the proposition. □

Our main task if to use the expression of $\pi_i(\mathbf{B}\mathcal{D}), i = 1, 2$ to reduce $\mathbf{B}\mathcal{D}$ into the vector form of Theorem 1.1.

4. **Decomposition of $\mathcal{D}$**

In this section, we consider a decomposition of $\mathcal{D}$ as a key step in the proof of the necessity in Theorem 1.1. As before, we assume $\mathbf{0} \in \mathcal{D}$ is a primitive tile digit with respect to $\mathbf{A} = p\mathbf{I}_2$ (hence $\#\mathcal{D} = p^2$). According to Propostion 3.11 and the remark at the end of Section 2, we assume, without loss of generality, that

$$m_{\mathcal{D}}(p^{-(k_1+1)}\boldsymbol{e}_1) = 0, \quad m_{\mathcal{D}}(p^{-(k_2+1)}\boldsymbol{e}_2) = 0,$$

and $k_1 \ge k_2 \ge 1$. Hence by Proposition 3.2, the first coordinates and the second coordinates of the digits in $\mathcal{D}$ can be expressed separately as (the ordering are rearranged)

$$\pi_1(\mathcal{D}) \equiv \{0, \alpha_1, \cdots, \alpha_{p-1}\} + p^{k_1}\{0, 1, \cdots, p-1\} \pmod{p^{k_1+1}}, \tag{4.1}$$

$$\pi_2(\mathcal{D}) \equiv \{0, \beta_1, \cdots, \beta_{p-1}\} + p^{k_2}\{0, 1, \cdots, p-1\} \pmod{p^{k_2+1}}, \tag{4.2}$$

where $0 \le \alpha_i \le p^{k_1} - 1$, $0 \le \beta_i \le p^{k_2} - 1$. Our main effort is to investigate the relation of the two projections to match up the α_i and β_j, and show that $k_1 = k_2$ (Proposition 5.1).

For an integer b, we say that it has *p-exponent* t if $p^t | b$ but $p^{t+1} \nmid b$; the p-exponent of a subset $E \subset \mathbb{Z}$ is the p-exponent of the g.c.d. of E. We use $\Delta(E)$ to denote the difference set $E - E$.

Lemma 4.1. *For any subset E of $\pi_2(\mathcal{D})$ in (4.2) with $\#E = p$, then $\Delta(E) \neq \{0\}$. Furthermore, if we let t be the p-exponent of $\Delta(E)$, then $t \le k_2$, and $E (mod\ p^t)$ is a singleton $\{\gamma\}$ with $0 \le \gamma \le p^t - 1$ (if $t = 0$, we take $\gamma = 0$).*

Proof. For $E \subseteq \pi_2(\mathcal{D})$, the elements in $E (\mathrm{mod}\ p^{k_2+1})$ are of the form $\beta_i + p^{k_2} j$ for some β_i and $0 \le j \le p-1$ in (4.2). Since $\mathcal{D}$ is primitive and $k_2 \ge 1$, the β_i's are not all equal. Hence for $\#E = p$, E must contains some distinct β_i or j, therefore $\Delta(E) := E - E \not\equiv \{0\} (\mathrm{mod}\ p^{k_2+1})$.

Suppose for each element in $E (\mathrm{mod}\ p^{k_2+1})$, the corresponding β_i are equal, then there are $0 \le j_1 \neq j_2 \le p-1$ such that

$$\{\beta_i + p^{k_2} j_1,\ \beta_i + p^{k_2} j_2\} \subset E (\mathrm{mod}\ p^{k_2+1}).$$

Hence the p-exponent of $\Delta(E)$ is k_2. Suppose there are $\beta_{i_1} \neq \beta_{i_2}$, then by

$$\{\beta_{i_1} + p^{k_2} j_1,\ \beta_{i_2} + p^{k_2} j_2\} \subset E (\mathrm{mod}\ p^{k_2+1}),\ \text{for some } 0 \le j_1, j_2 \le p-1,$$

and $0 \le \beta_{i_1}, \beta_{i_2} \le p^{k_2} - 1$, we see that

$$p^t \mid \gcd(\Delta(E)) \implies p^t \mid \gcd(\beta_{i_1} - \beta_{i_2} + p^{k_2}(j_1 - j_2)).$$

Hence $t < k_2$ for t the p-exponent of $\Delta(E)$.

For the last part, that $t = 0$ is trivial. For $t > 0$, we observe that $\beta_i \equiv \beta_j (\mathrm{mod}\ p^t)$. Hence we can take γ to be any $\beta_i (\mathrm{mod}\ p^t)$. $\square$

The decomposition: Let $\mathcal{D}$ be a tile digit set satisfies (4.1) and (4.2), we will use the α_i in $\pi_1(\mathcal{D})$ in (4.1) to make a decomposition of $\mathcal{D}$. For each α_i, there is a subset $\mathcal{D}_i \subset \mathcal{D}$ of p elements such that its first coordinates are $\alpha_i + p^{k_1} j + p^{k_1+1} n_j$; for the second coordinates of $\mathcal{D}_i$, we use Lemma 4.1 to write them as $\gamma_i + p^{t_i} n_{i,j} + p^{t_i+1} m_j$. Hence we have a decomposition $\mathcal{D} = \bigcup_{i=0}^{p-1} \mathcal{D}_i$ where

$$\mathcal{D}_i \equiv \{ \begin{bmatrix} \alpha_i \\ \gamma_i + p^{t_i} n_{i,0} \end{bmatrix}, \cdots, \begin{bmatrix} \alpha_i + p^{k_1}(p-1) \\ \gamma_i + p^{t_i} n_{i,p-1} \end{bmatrix} \} \quad (\mathrm{mod} \begin{bmatrix} p^{k_1+1} & 0 \\ 0 & p^{t_i+1} \end{bmatrix}), \tag{4.3}$$

the t_i and γ_i are defined as in Lemma 4.1.

If all the α_i are distinct, then the $\mathcal{D}_i$'s are uniquely defined, and so are the t_i's. If some of the $\alpha_i' s$ are equal, say $\alpha_i = \cdots = \alpha_{i+k}$, and are distinct from the others, then for each j, the digits associated with first coordinates $\alpha_i + p^{k_1} j, \cdots, \alpha_{i+k} + p^{k_1} j$ (they are equal) in the $\mathcal{D}_i, \cdots, \mathcal{D}_{i+k}$ can be rearrange among themselves, and the resulting

$\gamma_i, \cdots \gamma_{i+k}$ and $t_i, \cdots, t_{i+k}$ can be different. Because of this, we rearrange them so that t_i is the maximum among all these rearrangements. We then perform the same procedure to the remaining $p(k-1)$ digits of the $\mathcal{D}_i, \cdots, \mathcal{D}_{i+k}$ and obtain t_{i+1} as the next maximum, and so on inductively. Consequently, we have $t_i \geq \cdots \geq t_{i+k} \geq 0$ (they are bounded by k_2 by Lemma 4.1) and have the maximum property as stated.

From the above discussion, we give a temporal definition for the convenience of referral in the rest of the proof.

Definition 4.2. *Following the above construction, we can partition $\mathcal{D}$ as*

$$\mathcal{D} = \bigcup_{i=0}^{p-1} \mathcal{D}_i = \bigcup_{i=0}^{p-1} \left(\begin{bmatrix} \alpha_i \\ \gamma_i \end{bmatrix} + \mathbf{A}_i \mathcal{E}_i \right) \tag{4.4}$$

where

$$\mathbf{A}_i = \begin{bmatrix} p^{k_1} & 0 \\ 0 & p^{t_i} \end{bmatrix}, \quad \mathcal{E}_i \equiv \left\{ \begin{bmatrix} 0 \\ n_{i,0} \end{bmatrix}, \cdots, \begin{bmatrix} p-1 \\ n_{i,p-1} \end{bmatrix} \right\} \pmod{p},$$

with $0 \leq n_{i,k} \leq p-1$, and the p-exponents $\{t_i\}_{i=0}^{p-1}$ are set up as in last paragraph. We call (4.4) *an* admissible decomposition *of $\mathcal{D}$.*

Remark 1. A direct check shows that $m_{\mathcal{D}_i}(p^{-(k_1+1)}\boldsymbol{e}_1) = 0$.

Remark 2. By a translation of $\mathcal{D}$, we can assume all the entries $\alpha_i, \gamma_i \geq 0$. Also with a rearrangement of the indices, we can assume $t_0 \geq t_1 \cdots \geq t_{p-1}$.

Remark 3. Note that in the above decomposition, it is possible that different pairs of $\left(\begin{bmatrix} \alpha_i \\ \gamma_i \end{bmatrix}, \mathbf{A}_i \right)$ are identical (the associated $\mathcal{E}_i$'s can be identical or distinct). We let I_j denote such indices, and let $\widetilde{\mathcal{D}}_j = \bigcup_{i \in I_j} \mathcal{D}_i$, $\widetilde{\mathcal{E}}_j = \bigcup_{i \in I_j} \mathcal{E}_i$; this gives a further decomposition.

In the following, we give a special property on the zero set of the mask polynomial of the above $\widetilde{\mathcal{D}}_j$, which will be used in next section (Lemma 5.4). Let $t_{\min} = \min_{0 \leq j \leq p-1} t_j$. Then by assumption and Lemma 4.1, $t_{\min} \leq t_j \leq k_2 \leq k_1$. For $\boldsymbol{v}_n = (1, p^{k_1 - t_{\min}} n)$, let

$$\mathcal{Z}_j = \{ n \in \mathbb{Z} : \ m_{\widetilde{\mathcal{D}}_j}(p^{-(k_{\boldsymbol{v}_n}+1)} \boldsymbol{v}_n) = 0 \}.$$

Note that $0 \in \mathcal{Z}_j$, following from $\boldsymbol{v}_0 = (1,0) = \boldsymbol{e}_1$ and Remark 1 above. Hence $\mathcal{Z}_j \neq \emptyset$.

Lemma 4.3. *For each j, $t_j = t_{\min}$ if and only if $\mathcal{Z}_j \neq \mathbb{Z}$. In particular there is some j such that $\mathcal{Z}_j \neq \mathbb{Z}$.*

Proof. Without loss of generality, we assume that $\widetilde{\mathcal{D}}_j = \mathcal{D}_j$, and $\mathcal{D}_j$ has the expression in (4.4). Let $\boldsymbol{v}_n = (1, p^{k_1 - t_{\min}} n)^t$. For the sufficiency, we observe that if otherwise, $t_j > t_{\min}$, then

$$\begin{aligned} \pi_{\boldsymbol{v}_n}(\mathcal{D}_j) &= \langle \boldsymbol{v}_n, \left[\begin{smallmatrix} \alpha_j \\ \gamma_j \end{smallmatrix} \right] \rangle + \langle \boldsymbol{v}_n, \mathbf{A}_j \mathcal{E}_j \rangle \\ &\equiv \langle \boldsymbol{v}_n, \left[\begin{smallmatrix} \alpha_j \\ \gamma_j \end{smallmatrix} \right] \rangle + p^{k_1} \{0, \cdots, p-1\} \pmod{p^{k_1+1}} \end{aligned}$$

(that $t_j > t_{\min}$ is used to absorb the term from the second coordinate in the (mod p^{k_1+1})). Hence by Proposition 3.2, $n \in \mathcal{Z}_j$ and $\mathcal{Z}_j = \mathbb{Z}$, a contradiction.

To prove the necessity, assume $t_j = t_{\min}$, then $\boldsymbol{v}_n = (1, n)$. If $\mathcal{Z}_j = \mathbb{Z}$, then for any $n \in \mathbb{Z}$,

$$0 = m_{\mathcal{D}_j}(p^{-(k_{\boldsymbol{v}_n}+1)} \boldsymbol{v}_n) = e^{2\pi i \langle p^{-(k_{\boldsymbol{v}_n}+1)} \boldsymbol{v}_n, (\alpha_j, \gamma_j)^t \rangle} m_{\mathcal{E}_j}(p^{-(k_{\boldsymbol{v}_n} - k_1 + 1)} (1, n)^t).$$

This implies $\mathcal{E}_j$ satisfies condition $(*)$. Note that for $n = 0$, $m_{\mathcal{E}_j}(p^{-1}(1,0)^t) = 0$ (by a direct check), we can use Proposition 3.8 to conclude that $m_{\mathcal{E}_j}(p^{-1}(1,n)^t) = 0$ for all $n \in \mathbb{Z}$. Then Proposition 3.6 apply to $\mathcal{E}_j$ implies

$$\mathcal{E}_j \equiv \left[\begin{smallmatrix} 0 \\ d_j \end{smallmatrix} \right] + \mathcal{C} \pmod{p} \tag{4.5}$$

for some $0 \le d_j \le p-1$. On the other hand, by Lemma 4.1, we can write $\mathcal{E}_j$ as

$$\mathcal{E}_j = \left[\begin{smallmatrix} 0 \\ d_j \end{smallmatrix} \right] + \left[\begin{smallmatrix} 1 & 0 \\ 0 & p^{s_j} \end{smallmatrix} \right] \left\{ \left[\begin{smallmatrix} 0 \\ n_0 \end{smallmatrix} \right], \cdots, \left[\begin{smallmatrix} p-1 \\ n_{p-1} \end{smallmatrix} \right] \right\}.$$

where p^{s_j} is the g.c.d. of the second coordinates of $\mathcal{E}_j$. Note that $s_j \ge 1$ (if $s_j = 0$, then $\mathcal{E}_j$ cannot be written as in (4.5)), and the n_k's are not all equal (otherwise, $\Delta(\mathcal{E}_j) = 0$, contradicting to Lemma 4.1). Then

$$\mathcal{D}_j = \left[\begin{smallmatrix} \alpha_j \\ \gamma_j \end{smallmatrix} \right] + \mathbf{A}_j \mathcal{E}_j = \left[\begin{smallmatrix} \alpha_j \\ \gamma_j + p^{t_j} d_j \end{smallmatrix} \right] + \mathbf{A}'_j \mathcal{E}'_j,$$

where

$$\mathbf{A}'_j = \left[\begin{smallmatrix} p^{k_1} & 0 \\ 0 & p^{t_j + s_j} \end{smallmatrix} \right], \quad \mathcal{E}' \equiv \left\{ \left[\begin{smallmatrix} 0 \\ n'_0 \end{smallmatrix} \right], \cdots, \left[\begin{smallmatrix} p-1 \\ n'_{p-1} \end{smallmatrix} \right] \right\} \pmod{p}.$$

This means that there is another rearrangement of $\mathcal{D}_j$ such that $t'_j = t_j + s_j \ge t_j + 1$. It contradicts the maximality of t_j on $\mathcal{D}_j$. □

5. **Proof of the main theorem**

We know in last section $t_{\min} \le t_j \le k_2 \le k_1$. Our final effort is to that they are all equal.

Proposition 5.1. *For the admissible decomposition in Definition 4.2, we have* $t_{\min} = k_2 = k_1 := k$. *Hence we can improve the expression in* (4.4) *as*

$$\mathcal{D} = \bigcup_{j=0}^{p-1} \mathcal{D}_j = \bigcup_{j=0}^{p-1} \left(\left[\begin{smallmatrix} \alpha_j \\ \beta_j \end{smallmatrix} \right] + p^k \mathcal{E}_j \right). \tag{5.1}$$

For this we will need a few technical lemmas

Lemma 5.2. *Let* $\boldsymbol{v}_n = (1, p^{k_1 - t_{\min} n})^t$, *and assume that* $k_1 \geq 1$, *then either* $k_{\boldsymbol{v}_n} \geq k_1$ *or* $k_{\boldsymbol{v}_n} = 0$.

Proof. Write $\boldsymbol{v} = \boldsymbol{v}_n$. Since $m_{\mathcal{D}}(p^{-(k_{\boldsymbol{v}}+1)}\boldsymbol{v}) = 0$, by Proposition 3.2, we have

$$\pi_{\boldsymbol{v}}(\mathcal{D}) \equiv \{0, \eta_1, \cdots, \eta_{p-1}\} + p^{k_{\boldsymbol{v}}}\{0, 1, \cdots, p-1\} \pmod{p^{k_{\boldsymbol{v}}+1}} \tag{5.2}$$

for some $0 \leq \eta_i \leq p^{k_{\boldsymbol{v}}} - 1$. From the decomposition (4.4), we also have

$$\pi_{\boldsymbol{v}}(\mathcal{D}) = \bigcup_{i=0}^{p-1} \left(\langle \boldsymbol{v}, \left[\begin{smallmatrix} \alpha_i \\ \gamma_i \end{smallmatrix} \right] \rangle + p^{k_1} \langle (1, p^{t_i - t_{\min}} n)^t, \mathcal{E}_i \rangle \right).$$

If $k_{\boldsymbol{v}} < k_1$, then $k_{\boldsymbol{v}} + 1 \leq k_1$, and the above equation reduces to

$$\pi_{\boldsymbol{v}}(\mathcal{D}) \equiv \{\alpha_i + p^{k_1 - t_{\min}} n \gamma_i\}_{i=0}^{p-1} + \{0, \cdots, 0\} \pmod{p^{k_{\boldsymbol{v}}+1}}.$$

Comparing with (5.2), we have $k_{\boldsymbol{v}} = 0$. □

Remark. Note that in the case $k_{\boldsymbol{v}_n} = 0$, that $0 \leq \eta_i \leq p^{k_{\boldsymbol{v}_n}} - 1$ implies η_i is identically zero, hence $\pi_{\boldsymbol{v}_n}(\mathcal{D}) = \{0, 1, \cdots, p-1\} \pmod{p}$.

We let

$$\mathcal{D}^{(n)} := \mathbf{B}_n \mathcal{D} \quad \text{where} \quad \mathbf{B}_n = \begin{bmatrix} 1 & p^{k_1 - t_{\min} n} \\ 0 & 1 \end{bmatrix}.$$

Then

$$m_{\mathcal{D}^{(n)}}(p^{-(k_{\boldsymbol{v}_n}+1)}\boldsymbol{e}_1) = m_{\mathcal{D}}(p^{-(k_{\boldsymbol{v}_n}+1)}\boldsymbol{v}_n) = 0,$$

and the exponent $k_1^{(n)}$ in $\pi_1(\mathcal{D}^{(n)})$ equals $k_{\boldsymbol{v}_n}$. Let $\{\mathcal{D}_\ell^{(n)}\}_{\ell=0}^{p-1}$ be a decomposition of $\mathcal{D}^{(n)}$ as in (4.4), and let $\{t_\ell^{(n)}\}_{\ell=0}^{p-1}$ be the associated sequence of p-exponents for the second coordinates. By Remark 1 of Definition 4.2,

$$m_{\mathcal{D}_\ell^{(n)}}(p^{-(k_{\boldsymbol{v}_n}+1)}\boldsymbol{e}_1) = 0. \tag{5.3}$$

Note that these $\mathcal{D}_\ell^{(n)}$ may not equal to $\mathbf{B}_n \mathcal{D}_i$ because of the rearrangement of the digits for the $t_\ell^{(n)}$ (see the paragraph "The decomposition" before Definition 4.2)

In view of Lemma 5.2, we consider $k_{\boldsymbol{v}_n} \geq k_1$. Let $\mathcal{D}_{\ell_i}^{(n)}$ be the component determined by the η_i(defined in (5.2)) in $\{\mathcal{D}_\ell^{(n)}\}_{\ell=0}^{p-1}$. Let

$$I = \{i : t_i = t_{\min}\} \quad \text{and} \quad I^c = \{i : t_i > t_{\min}\}.$$

(The I^c turns out to be empty eventually in the proof of Proposition 5.1.) For $i \in I^c$, we have $m_{\mathcal{D}_i}(p^{-(k_1+1)}\boldsymbol{v}_n) = 0$ (see the proof of the sufficiency in Lemma 4.3), and hence

$$\pi_1(\mathbf{B}_n\mathcal{D}_i) \equiv \eta_i + p^{k_1}\{0, \cdots, p-1\} \pmod{p^{k_1+1}}. \tag{5.4}$$

Lemma 5.3. *Suppose $k_{\boldsymbol{v}_n} \geq k_1$, then for $i \in I^c$, $t_{\ell_i}^{(n)} > t_{\min}$, and $\mathcal{D}_{\ell_i}^{(n)} \subset \bigcup_{j\in I^c}\mathbf{B}_n\mathcal{D}_j$. Consequently,*

$$\bigcup\nolimits_{i\in I^c}\mathcal{D}_{\ell_i}^{(n)} = \bigcup\nolimits_{j\in I^c}\mathbf{B}_n\mathcal{D}_j\ .$$

Proof. If $I^c = \emptyset$, the result is trivial, hence we assume that $I^c \neq \emptyset$. From the paragraph of "The decomposition" before Definition 4.2, we see that in the construction of $\mathcal{D}_{\ell_i}^{(n)}$, the p-exponent $t_{\ell_i}^{(n)}$ is taking maximum among the possible choices of digits associated with the η_i in (5.4), which includes $\mathbf{B}_n\mathcal{D}_i$. This implies that $t_{\ell_i}^{(n)} \geq t_i > t_{\min}$. If

$$\mathcal{D}_{\ell_i}^{(n)} \cap \bigcup\nolimits_{k\in I}\mathbf{B}_n\mathcal{D}_k \neq \emptyset,$$

then there is $j \in I^c, k \in I$ such that

$$\mathbf{B}_n\begin{bmatrix}\alpha_j\\ \gamma_j\end{bmatrix} + \mathbf{B}_n\mathbf{A}_j\boldsymbol{u}_j, \quad \mathbf{B}_n\begin{bmatrix}\alpha_k\\ \gamma_k\end{bmatrix} + \mathbf{B}_n\mathbf{A}_k\boldsymbol{u}_k \in \mathcal{D}_{\ell_i}^{(n)}$$

where $\boldsymbol{u}_j \in \mathcal{E}_j,\ \boldsymbol{u}_k \in \mathcal{E}_k$. So

$$\{\gamma_j + p^{t_j}\pi_1(\boldsymbol{u}_j),\ \gamma_k + p^{t_{\min}}\pi_1(\boldsymbol{u}_k)\} \subset \pi_2(\mathcal{D}_{\ell_i}^{(n)}).$$

It implies that $t_{\ell_i}^{(n)}$ is less than or equal to $t_{\min}$, a contradiction. Therefore, $\mathcal{D}_{\ell_i}^{(n)} \subset \bigcup_{j\in I^c}\mathbf{B}_n\mathcal{D}_j$, and hence

$$\bigcup\nolimits_{i\in I^c}\mathcal{D}_{\ell_i}^{(n)} \subseteq \bigcup\nolimits_{j\in I^c}\mathbf{B}_n\mathcal{D}_j\ .$$

As the cardinality of the two sets are equal, the inclusion is actually equality. □

Lemma 5.4. *Suppose $n \notin \mathcal{Z}_j$ for some j, and $k_{\boldsymbol{v}_n} \geq k_1$. Then $t_{\min}^{(n)} := \min\{t_{\ell_i}^{(n)} : t_i = t_{\min}\} < t_{\min}$.*

Proof. We write $\mathcal{D}_i^{(n)}$ to replace $\mathcal{D}_{\ell_i}^{(n)}$ for brevity, we also refer the reader to Figure 1 for some illustration of the notations defined in the following. By Lemma 5.3, $\bigcup_{i\in I^c}\mathcal{D}_i^{(n)} = \bigcup_{i\in I^c}\mathbf{B}_n\mathcal{D}_i$, and $\bigcup_{i\in I}\mathcal{D}_i^{(n)} = \bigcup_{i\in I}\mathbf{B}_n\mathcal{D}_i$. Let I_j denote those i such that

$$\left(\begin{bmatrix}\alpha_i\\ \gamma_i\end{bmatrix}, \mathbf{A}_i\right) = \left(\begin{bmatrix}\alpha_j\\ \gamma_j\end{bmatrix}, \mathbf{A}_j\right)$$

and let $\widetilde{\mathcal{D}}_j = \bigcup_{i\in I_j}\mathcal{D}_i$ (see Remark 2 after Definition 4.2).

As $n \notin \mathcal{Z}_j$, Lemma 4.3 implies $t_j = t_{\min}$, we have $I_j \subset I$, and $\mathbf{B}_n\widetilde{\mathcal{D}}_j \subseteq \bigcup_{i\in I}\mathcal{D}_i^{(n)}$. Let $\mathcal{F}_j = \{i \in I : \mathcal{D}_i^{(n)} \cap \mathbf{B}_n\widetilde{\mathcal{D}}_j \neq \emptyset\}$. Then

$$\mathbf{B}_n\widetilde{\mathcal{D}}_j \subsetneqq \bigcup\nolimits_{i\in\mathcal{F}_j}\mathcal{D}_i^{(n)},$$

because $m_{\mathbf{B}_n\widetilde{\mathcal{D}}_j}(p^{-(1+k_{\boldsymbol{v}_n})}\boldsymbol{e}_1) \neq 0$ (as $n \notin \mathcal{Z}_j$), but according to (5.3),

$$m_{\cup_{i\in\mathcal{F}_j}\mathcal{D}_i^{(n)}}(p^{-(1+k_{\boldsymbol{v}_n})}\boldsymbol{e}_1) = \sum\nolimits_{i\in\mathcal{F}_j} m_{\mathcal{D}_i^{(n)}}(p^{-(1+k_{\boldsymbol{v}_n})}\boldsymbol{e}_1) = 0.$$

Hence there is an index $\tau \in \mathcal{F}_j$ such that $\mathcal{D}_\tau^{(n)} \setminus \mathbf{B}_n\widetilde{\mathcal{D}}_j \neq \emptyset$. Choose

$$\begin{aligned}
\boldsymbol{x} &= \mathbf{B}_n\Big(\begin{bmatrix}\alpha_j\\ \gamma_j\end{bmatrix} + \mathbf{A}_j\boldsymbol{u}\Big) \in \mathcal{D}_\tau^{(n)} \cap \mathbf{B}_n\widetilde{\mathcal{D}}_j,\\
\boldsymbol{y} &= \mathbf{B}_n\Big(\begin{bmatrix}\alpha_k\\ \gamma_k\end{bmatrix} + \mathbf{A}_k\boldsymbol{u}'\Big) \in \mathcal{D}_\tau^{(n)} \setminus \mathbf{B}_n\widetilde{\mathcal{D}}_j \ \Big(\subseteq \bigcup\nolimits_{i\in I\setminus I_j}\mathbf{B}_n\mathcal{D}_i\Big).
\end{aligned}$$

From the definition of I_j, we have $(\begin{bmatrix}\alpha_j\\ \gamma_j\end{bmatrix}, \mathbf{A}_j) \neq (\begin{bmatrix}\alpha_k\\ \gamma_k\end{bmatrix}, \mathbf{A}_k)$. But $\mathbf{A}_j = \mathbf{A}_k = \begin{bmatrix}p^{k_1} & 0\\ 0 & p^{t_{\min}}\end{bmatrix}$, we must have

$$\begin{bmatrix}\alpha_j\\ \gamma_j\end{bmatrix} \neq \begin{bmatrix}\alpha_k\\ \gamma_k\end{bmatrix}. \tag{5.5}$$

Note that $\pi_1(\mathcal{D}_\tau^{(n)}) \equiv \eta_i + p^{k_{\boldsymbol{v}_n}}\{0, \cdots, p-1\} \pmod{p^{k_{\boldsymbol{v}_n}+1}}$ and $k_{\boldsymbol{v}_n} \geq k_1$, we have

$$\pi_1(\boldsymbol{x}) \equiv \pi_1(\boldsymbol{y}) \equiv \eta_i \pmod{p^{k_1}}.$$

It follows that $(\alpha_j - \alpha_k) + p^{k_1-t_{\min}}n(\gamma_j - \gamma_k) = \pi_1(\boldsymbol{x}) - \pi_1(\boldsymbol{y}) \in p^{k_1}\mathbb{Z}$. This together with (5.5) and $0 \leq \alpha_j, \alpha_k \leq p^{k_1} - 1$ implies that $\gamma_j \neq \gamma_k (\leq p^{t_{\min}} - 1)$.

Since

$$\gamma_j + p^{t_{\min}}\pi_2(\boldsymbol{u}),\ \gamma_k + p^{t_{\min}}\pi_2(\boldsymbol{u}') \in \pi_2(\mathcal{D}_\tau^{(n)}),$$

we see that $t_\tau^{(n)}$, the p-exponent of $\Delta(\pi_2(\mathcal{D}_\tau^{(n)}))$, is less than $t_{\min}$. That is to say, there is a $\tau \in I = \{i : t_i = t_{\min}\}$ such that $t_\tau^{(n)} < t_{\min}$. One the other hand, for $i \in I^c$, from Lemma 5.3, we have $t_i^{(n)} > t_{\min}$. Therefore

$$t_{\min}^{(n)} = \min_{0\leq i\leq p-1} t_i^{(n)} = \min_{i\in I^c} t_i^{(n)} < t_{\min},$$

which completes the proof of the lemma. □

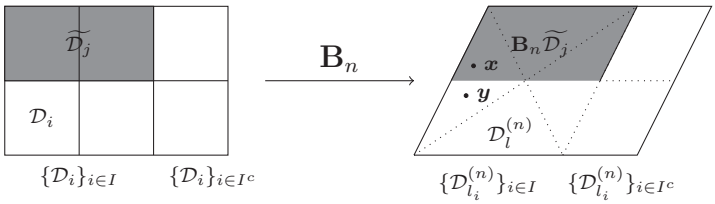

FIGURE 1. Illustration of Lemma 5.4

Proof of Proposition 5.1. Suppose otherwise, $t_{\min} < k_1$. As $k_1 \geq 1$, we have

$$0 \neq m_{\mathcal{D}}(p^{-1}\boldsymbol{v}_n) = m_{\mathcal{D}}(p^{-1}\boldsymbol{e}_1),$$

and hence $k_{\boldsymbol{v}_n} \neq 0$. By Lemma 5.2, $k_{\boldsymbol{v}_n} \geq k_1$ for all n .

Let $\{\widetilde{\mathcal{D}}_j\}_{j=0}^{N-1}$ be an admissible decomposition of $\mathcal{D}$ be defined as in the remark 2 after Definition 4.2. For $t_j = t_{\min}$, we have $\mathcal{Z}_j \neq \mathbb{Z}$ (Lemma 4.3). Let $\mathbf{B}_1 = \left[\begin{smallmatrix} 1 & p^{k_1-t_{\min}}n_1 \\ 0 & 1 \end{smallmatrix}\right]$ with $n_1 \notin \mathcal{Z}_j$. Lemma 5.4 implies $t_{\min}^{(1)} < t_{\min}$. Note that $k_1^{(1)} = k_{\boldsymbol{v}_{n_1}} \geq k_1$. By the same argument as in the first paragraph, $k_{\boldsymbol{v}_n}^{(1)} \geq k_1^{(1)}$.

Consider the matrix $\mathbf{B}_2 = \left[\begin{smallmatrix} 1 & p^{k_1^{(1)}-t_{\min}^{(1)}}n_2 \\ 0 & 1 \end{smallmatrix}\right]$. Let $\mathcal{D}^{(2)} = \mathbf{B}_2\mathcal{D}_1 (= \mathbf{B}_2\mathbf{B}_1\mathcal{D})$, then the same argument shows that

$$k_1^{(2)} \geq k_1^{(1)}, \quad t_{\min}^{(2)} < t_{\min}^{(1)} < t_{\min}.$$

Here,

$$\mathbf{B}_2\mathbf{B}_1 = \left[\begin{smallmatrix} 1 & p^{k_1-t_{\min}}m_1 \\ 0 & 1 \end{smallmatrix}\right], \quad m_1 = n_1 + p^{(k_1^{(1)}-t_{\min}^{(1)})-(k_1-t_{\min})}n_2 \in \mathbb{Z}.$$

This procedure can only continuous for finitely many steps, and the last step gives a contradiction to Lemma 4.3.

For the last statement, we note that $\gamma_j \in \{0, \beta_1, \cdots, \beta_{p-1}\}$ (see (4.2) and Lemma 4.1), and by a rearrangement, we write $\gamma_j = \beta_j$. □

Finally, we proof the necessity of Theorem 1.1.

Theorem 5.5. *Let $\mathcal{D}$ be a primitive tile digit with respect to $p\mathbf{I}_2$. Then there is an invertible matrix $\mathbf{B} \in M_2(\mathbb{Z})$ with $|\det \mathbf{B}| = 1$ and a $\mathbb{Z}_p^2$-summand $\mathcal{W} = \{\boldsymbol{w}_i\}_{i=0}^{p-1}$ such that*

$$\mathbf{B}\mathcal{D} \equiv \bigcup_{i=0}^{p-1} \left(\boldsymbol{w}_i + p^k\mathcal{E}_i\right) \quad (mod\ p^{k+1}), \tag{5.6}$$

for some $k \geq 0$, where $\mathcal{E}_i \in \mathcal{F}_{\mathcal{W}}$. In particular, when $k = 0$, the $\mathcal{E}_i$'s are all equal.

Proof. If $\mathcal{D}$ is a complete residue set modulus $p\mathbf{I}_2$, then $\mathcal{D} \equiv \mathbb{Z}_p^2 \pmod p$ which obviously has the form as in (5.6) for $k = 0$.

Suppose $\mathcal{D}$ is not a complete residue set modulus $p\mathbf{I}_2$, let $\mathbf{B}$ be an invertible matrix defined as in Proposition 3.11 such that $m_{\mathcal{D}}(p^{-(k+1)}\boldsymbol{e}_1) = 0$ and $m_{\mathcal{D}}(p^{-(k+1)}\boldsymbol{e}_2) = 0$ (see (4.1), (4.2)). Denote $\mathcal{W} = \{\boldsymbol{w}_j\}_{j=0}^{p-1} := \{\left[\begin{smallmatrix} \alpha_j \\ \beta_j \end{smallmatrix}\right]\}_{j=0}^{p-1}$ as in Proposition 5.1. In the following we show that elements in $\mathcal{W}$ are distinct, $\mathcal{W}$ is a $\mathbb{Z}_p^2$-summand, and the $\mathcal{E}_i$ are complementary $\mathbb{Z}_p^2$-summand. Then the theorem follows.

For any $n \in \mathbb{Z}$, we claim that either $k_{\boldsymbol{v}_n} = 0$ or $k_{\boldsymbol{v}_n} = k$. Indeed consider $\mathcal{D}_n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}\mathcal{D}$, we have for the first coordinate,

$$m_{\mathcal{D}_n}(p^{-(k_{\boldsymbol{v}_n}+1)}\boldsymbol{e}_1) = m_{\mathcal{D}}(p^{-(k_{\boldsymbol{v}_n}+1)}\boldsymbol{v}_n) = 0,$$

and for the second coordinate

$$m_{\mathcal{D}_n}(p^{-(k+1)}\boldsymbol{e}_2) = m_{\mathcal{D}}(p^{-(k+1)}\boldsymbol{e}_2) = 0.$$

These together with Proposition 5.1 apply to $\mathcal{D}_n$ imply $k_{\boldsymbol{v}_n} = k\ (= t_{\min})$ when $k_{\boldsymbol{v}_n} \geq 1$. The claim follows by Lemma 5.2.

Next we consider the two cases separately.

(i) For the $\boldsymbol{v}_n$ with $k_{\boldsymbol{v}_n} = 0$, we have, by (5.1) and $k \geq 1$,

$$\begin{aligned} 0 = m_{\mathcal{D}}(p^{-1}\boldsymbol{v}_n) &= \sum\nolimits_{j=0}^{p-1} e^{2\pi i\langle \boldsymbol{w}_j, p^{-1}\boldsymbol{v}_n\rangle} m_{p^k\mathcal{E}_j}(p^{-1}\boldsymbol{v}_n) \\ &= p\sum\nolimits_{j=0}^{p-1} e^{2\pi i\langle \boldsymbol{w}_j, p^{-1}\boldsymbol{v}_n\rangle} \\ &:= pP(e^{2\pi i/p}), \end{aligned}$$

where $P(x) = \sum_{j=0}^{p-1} x^{k_j}, k_j \equiv \langle \boldsymbol{v}_n, \boldsymbol{w}_j\rangle (\mathrm{mod}\ p)$ and $0 \leq k_j \leq p-1$. So $\Phi_p(x)|P(x)$. Note that $P(x)$ is polynomial of degree $\leq p-1$, it follows that $P(x)$ is a constant multiple of $\Phi_p(x)$. Hence all the k_j are distinct, i.e., the $\boldsymbol{w}_j$'s are distinct. This implies $m_{\mathcal{W}}(p^{-1}\boldsymbol{v}_n) = 0$.

(ii) For the $\boldsymbol{v}_n$ with $k_{\boldsymbol{v}_n} = k$, we have $n \in \mathcal{Z}_j\ (= \{n' : m_{\mathcal{D}_j}(p^{-(k+1)}\boldsymbol{v}_{n'}) = 0\})$ for each j. Hence for any $\mathcal{D}_i$,

$$0 = m_{\mathcal{D}_i}(p^{-(k+1)}\boldsymbol{v}_n) = e^{2\pi i\langle \boldsymbol{w}_i, p^{-(k+1)}\boldsymbol{v}_n\rangle} m_{\mathcal{E}_i}(p^{-1}\boldsymbol{v}_n).$$

Then $m_{\mathcal{E}_i}(p^{-1}\boldsymbol{v}_n) = 0$.

It follows from the claim and (i), (ii) that for any $\boldsymbol{v}_n = (1, n)^t$, either $m_{\mathcal{W}}(p^{-1}\boldsymbol{v}_n) = 0$ or $m_{\mathcal{E}_i}(p^{-1}\boldsymbol{v}_n) = 0$. If we consider the second coordinate, namely, for any $\boldsymbol{v}_m = (m, 1)$, again we have either $m_{\mathcal{W}}(p^{-1}\boldsymbol{v}_m) = 0$ or $m_{\mathcal{E}_i}(p^{-1}\boldsymbol{v}_m) = 0$ for all $m \in \mathbb{Z}$. By Lemma 3.5, we have

$$\mathbb{Z}^2 \setminus p\mathbb{Z}^2 \subset \mathcal{Z}(m_{p^{-1}\mathcal{W}}) \cup \mathcal{Z}(m_{p^{-1}\mathcal{E}_i}).$$

It means $\mathbb{Z}_p^2$ is a zero set of $m_{p^{-1}(\mathcal{W}+\mathcal{E}_i)}$. Hence $\mathcal{W} + \mathcal{E}_i$ is a complete residue set modulus $p\mathbf{I}_2$ for each i. □

6. **Remarks**

Note that if $\mathcal{W}_{res} = \left\{\mathbf{0}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \cdots, \begin{bmatrix} p-1 \\ 0 \end{bmatrix}\right\}$ for some matrix $\mathbf{B}$ in (5.6), the primitivity of $\mathbf{B}\mathcal{D}$ implies $k = 0$ and $\mathcal{D}$ is a complete residue set modulus $p\mathbf{I}_2$. For the special case $p = 2$, unlike the other odd primes, the tile digit set for $2\mathbf{I}_2$ is always a complete residue set. This can be proved directly.

Proposition 6.1. *Let $\mathcal{D} \subset \mathbb{Z}^2$ is a primitive digit with respect to $2\mathbf{I}_2$. Then $\mathcal{D}$ is a tile digit set if and only if $\mathcal{D}$ is a complete residue set modulus $2\mathbf{I}_2$.*

Proof. We just need to prove the necessity. Assume $\mathcal{D}$ is a tile digit set, then by Proposition 3.2,

$$\pi_1(\mathcal{D}) \equiv \{0, \alpha\} + 2^{k_1}\{0, 1\} \pmod{2^{k_1+1}},$$

where $k_1 \geq 0,\ 0 \leq \alpha \leq 2^{k_1} - 1$. Since $\mathcal{D}$ is primitive, α must be odd, or 0 when $k_1 = 0$. It follows from a direct check that in both cases, $m_{\mathcal{D}}(2^{-1}\boldsymbol{e}_1) = 0$. Similarly, we have $m_{\mathcal{D}}(2^{-1}\boldsymbol{e}_2) = 0$, and by observing the first coordinate of $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\mathcal{D}$, we have $m_{\mathcal{D}}(2^{-1}(1,1)^t) = 0$.

Note that for any $\boldsymbol{v} \in \mathbb{Z}^2 \setminus 2\mathbb{Z}^2$, $\boldsymbol{v}(\text{mod } 2)$ equals one of $\boldsymbol{e}_1, \boldsymbol{e}_2, (1,1)^t$. So, we always have

$$m_{\mathcal{D}}(2^{-1}\boldsymbol{v}) = 0.$$

Hence, $\mathcal{D}$ is a complete residue set modulo 2. □

For $p = 3$, the characterization of the tile digit sets in Theorem 1.1 can be reduced to be the product-forms. First we prove a lemma.

Lemma 6.2. *Let $\mathcal{W}$ be a $\mathbb{Z}_3^2$-summand, and let $\mathcal{W} \oplus \mathcal{E} = \mathbb{Z}_3^2$. Then there exists $\mathbf{B} \in M_2(\mathbb{Z})$ with $|\det \mathbf{B}| = 1$ such that $\mathcal{W}' = \mathbf{B}\mathcal{W}$, $\mathcal{E}' = \mathbf{B}\mathcal{E}$, and*

$$\mathcal{W}'_{res} = \left\{\mathbf{0}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 2 \\ 0 \end{bmatrix}\right\}, \qquad \mathcal{E}'_{res} = \left\{\mathbf{0}, \begin{bmatrix} a \\ 1 \end{bmatrix}, \begin{bmatrix} b \\ 2 \end{bmatrix}\right\}, \quad a, b \in \{0, 1, 2\},$$

or interchange the role of $\mathcal{W}'$ and $\mathcal{E}'$.

Proof. In terms of the zeros of the mask polynomial, the direct sum $\mathcal{W} \oplus \mathcal{E} = \mathbb{Z}_3^2$ is equivalent to (see Section 2)

$$\mathcal{Z}(m_{\mathcal{W}}) \cup \mathcal{Z}(m_{\mathcal{E}}) = 3^{-1}\mathbb{Z}^2 \setminus \mathbb{Z}^2. \tag{6.1}$$

This together with Lemma 3.5 imply that there is a $\boldsymbol{v} = (1, n)^t$ (or $(n, 1)^t$) such that

$$m_{\mathcal{W}}(3^{-1}\boldsymbol{v}) = m_{\mathbf{B}_1\mathcal{W}}(3^{-1}\boldsymbol{e}_1) = 0,$$

where $\mathbf{B}_1 = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$(or $\begin{bmatrix} n & 1 \\ 1 & 0 \end{bmatrix}$, respectively). Then Proposition 3.2 implies $\pi_1(\mathcal{W}_1) \equiv \{0, 1, 2\} \pmod 3$, i.e.,

$$\mathbf{B}_1\mathcal{W} \equiv \left\{\mathbf{0}, \begin{bmatrix} 1 \\ \ell \end{bmatrix}, \begin{bmatrix} 2 \\ m \end{bmatrix}\right\} \pmod 3, \quad \ell,\ m \in \{0, 1, 2\}.$$

Let $\mathbf{B}_2 := \begin{bmatrix} 1 & 0 \\ -\ell & 1 \end{bmatrix}$ and let $\mathcal{W}' = \mathbf{B}_2(\mathbf{B}_1\mathcal{W})$, $\mathcal{E}' = \mathbf{B}_2(\mathbf{B}_1\mathcal{E})$. Then

$$\mathcal{W}'_{res} = \left\{\mathbf{0}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 2 \\ i \end{bmatrix}\right\}, \quad i = 0, 1, 2.$$

Note that for $i = 0$, $m_{\mathcal{W}'}(3^{-1}\boldsymbol{v}) \neq 0$ for any $\boldsymbol{v} = (0, n)^t$. By $\mathcal{W}' \oplus \mathcal{E}' = \mathbb{Z}_3^2$ and (6.1), we have $m_{\mathcal{E}'}(3^{-1}(0, n)^t) = 0$. Hence

$$\mathcal{E}'_{res} = \left\{\mathbf{0}, \begin{bmatrix} a \\ 1 \end{bmatrix}, \begin{bmatrix} b \\ 2 \end{bmatrix}\right\}, \quad a, b \in \{0, 1, 2\},$$

as stated in the lemma. On the other hand, for $i = 1$ or 2, we have by $\mathcal{W}' \oplus \mathcal{E}' = \mathbb{Z}_3^2$ and (6.1) again,

$$\widetilde{V}_1 = \{(n, 1)^t : n \in \mathbb{Z}\} \subset \mathcal{Z}(m_{3^{-1}\mathcal{E}'}).$$

Applying Proposition 3.6 to the second coordinate of $\mathcal{E}'$, then we have

$$\mathcal{E}'_{res} = \left\{\mathbf{0}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 2 \end{bmatrix}\right\}.$$

□

Proposition 6.3. *Suppose $\mathcal{D}$ is a primitive digit set with respect to $3\mathbf{I}_2$, then $\mathcal{D}$ is a tile digit set if and only if there is a $\mathbf{B} \in M_2(\mathbb{Z})$ with $|\det \mathbf{B}| = 1$ such that*

$$\mathbf{B}\mathcal{D} \equiv \mathcal{W} \oplus 3^k\mathcal{E} \ (mod\ 3^{k+1}),$$

which is a product-form. In this case $\mathcal{W}_{res} = \left\{\mathbf{0}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 2 \\ i \end{bmatrix}\right\}, i = 0, 1, 2.$

Proof. According to Theorem 1.1, $\mathcal{D}$ is a primitive tile digit set with respect to $3\mathbf{I}_2$ if and only if $\mathbf{B} \in M_2(\mathbb{Z})$ with $|\det \mathbf{B}| = 1$ such that

$$\mathbf{B}\mathcal{D} \equiv \bigcup_{i=0}^{2}(\boldsymbol{w}_i + 3^k\mathcal{E}_i) \ (\text{mod } 3^{k+1}),$$

where $\mathcal{W} = \{\mathbf{0} = \boldsymbol{w}_0, \boldsymbol{w}_1, \boldsymbol{w}_2\} \oplus \mathcal{E}_i = \mathbb{Z}_3^2$. By Lemma 6.2, we can choose $\mathbf{B}$ such that

$$\mathcal{W}_{res} = \left\{\mathbf{0}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 2 \\ i \end{bmatrix}\right\}, \quad i = 0, 1, 2.$$

That $\mathbf{B}\mathcal{D}$ is primitive implies $\gcd(\pi_2(\mathbf{B}\mathcal{D}) \setminus \{0\}) = 1$. So when $i = 0$, we have $k = 0$ and all $\mathcal{E}_i$ are equal to $\mathcal{E}$ (by Theorem 1.1). When $i = 1, 2$, we have proved $\mathcal{E}_i = \mathcal{E} = \left\{\mathbf{0}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 2 \end{bmatrix}\right\}$. Hence in either cases

$$\mathbf{B}\mathcal{D} \equiv \mathcal{W} \oplus 3^k\mathcal{E} \ (\text{mod } 3^{k+1}).$$

□

We remark that for the primes $p \neq 2, 3$, we cannot reduce the expression (5.6) to be a product-form as in the above proposition. This is because when $p \geq 5$ and $k \geq 1$ in (5.6), the complementary summands $\mathcal{E}_i$ of $\mathcal{W}$ ($\neq \left\{\mathbf{0}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \cdots, \begin{bmatrix} p-1 \\ 0 \end{bmatrix}\right\}$ (mod p)) may not equal (see Example 2.2 for $p = 5$).

Note that in the proof of Theorem 1.1, one of the main techniques is the decomposition in Section 4. It is likely that this method can be further improved to consider matrix of the form $\mathbf{A} = p\mathbf{I}_s$ with $s \geq 3$. It is a classical theorem in abstract algebra that that $\mathbb{Z}_p \times \mathbb{Z}_q$ is isomorphic as a group to $\mathbb{Z}_{pq}$ where p, q are distinct prime integers. Since the tile digit with respect to pq has been characterized([LR]). Is the tile digit with respect to $\mathbf{A} = \begin{bmatrix} p & 0 \\ 0 & q \end{bmatrix}$ can be get from one-dimension?

Q1: Characterize the tile digit sets for $\mathbf{A} = \begin{bmatrix} p & 0 \\ 0 & q \end{bmatrix}$ or $\mathbf{A} = p\mathbf{I}_s$ respectively.

If $\mathbf{A}$ is not a diagonal matrix, the problem is much harder. Indeed even for the case when $|\mathbf{A}| = p$ for p a prime, one needs additional condition (e.g., $\mathcal{D}$ spans $\mathbb{R}$ [HL1]) to characterize the tile digit sets $\mathcal{D}$ as complete residue set. It will be nice to remove the condition in the characterization. Specifically,

Q2: For any expanding integral matrix $\mathbf{A}$ in $\mathbb{R}^s, s \geq 2$ with $|\det \mathbf{A}| = p$, a prime, prove that $\mathcal{D}$ is a tile digit set if and only if $\mathcal{D}$ is a complete residue set modulus $\mathbf{A}$.

In the study of tiles, there is a fascinating class of multi-tiles (tile by more than one tile) arisen in the theory of substitutions and finite automata ([R], [Th]), which has received a lot of attention recently ([AB1,2], [BS], [RWY]). It seems that there is no characterization of such tile digit sets analogous to the self-affine tiles under consideration, and it is worthwhile to explore if the present technique can be apply to that situation.

One of the very interesting connection of tiles to analysis is the so called Fuglede problem; the originally conjecture was a compact set $K \subset \mathbb{R}^s$ is a tile if and only it is a spectral sets K, i.e., $L^2(K)$ admits an exponential orthonormal basis $\{e^{2\pi i\langle\lambda,\mathbf{x}\rangle} : \lambda \in \Lambda\}$ ([F]). While there are examples in $\mathbb{R}^s, s \geq 3$, showing that spectral sets and tiles are different ([T], [KoM]), there are many positive results with additional assumption on the sets (e.g., convexity, self-similarity, p-adic field), and connections to the geometry of numbers. As a directly related question in our investigation, we ask

Q3: What is the relation of the tile property and spectral property of the self-affine set $T(p\mathbf{I}_2, \mathcal{D})$?

Acknowledgement. The authors are indebted to Professor Chun-Kit Lai for some valuable discussions, and directly them to the relevant references.

References

[AB1] S. Akiyama, T. Borbély, H. Brunotte, A. Petho, J. Thuswaldner, *Generalized radix representations and dynamical systems I.* Acta Math. Hungar. 108(2005), 207-238.

[AB2] S. Akiyama, H. Brunotte, A. Petho, J. Thuswaldner, *Generalized radix representations and dynamical systems II.* Acta Arith. 121(2006), 21-61.

[B] C. Bandt, *Self-similar sets 5. Integer matrices and fractal tilings of* $\mathbb{R}^n$, Proc. Amer. Math. Soc., 112(1991), 549-562.

[BS] G. Berthé, A. Siegel, W. Steiner, P. Surer, J. Thuswaldner, *Fractal tiles associated with shift radix systems*, Adv. Math. 226(2011), 139-175.

[CT] G. Conner and J. Thuswaldner, *Self-affine manifolds*, Adv. Math. 289(2016), 725-783.

[FHL] X.Y. Fu, X.G. He and K.S. Lau, *Spectrality of self-similar tiles*, Constr. Approx. 42(2015), 519-541.

[F] B. Fuglede, *Commuting self-adjoint partial differential operators and a group theoretic problem*, J. Funct. Anal. 16(1974), 101-121.

[GaY] J. Gabardo, and X.J. Yu, *Natural tiling, lattice tiling and Lebesgue measure of integral self-affine tiles*, J. Lond. Math. Soc. 74(2006), 184-204.

[HL1] X.G. He and K.S. Lau, *Characterization of tile digit sets with prime determinants*, Appl. Comput. Harmon. Anal. 16(2004), 159-173.

[HL2] X.G. He and K.S. Lau, *Height reducing property of polynomials and self-affine tiles*, Geom. Dedicata 152(2011), 153-164.

[IMP] A. Iosevich, A. Mayeli and J. Pakianathan, *The Fuglede Conjecture holds in* $Z_p \times Z_p$, arXiv:1505.00883v1.

[K] R. Kenyon, *Self-replicating tilings*, Symbolic Dynamics and its applications, (ed. P.Walters, Amer. Math. Soc., Prividence, RI, 1992, 239-264.

[KiL1] I. Kirat and K.S. Lau, *On the connectedness of self-affine tiles*, J. London Math. Soc. 62 (2000), 291-304.

[KiL2] I. Kirat and K.S. Lau, *Classification of integral expanding matrices and self-affine tiles*, Discrete Comput. Geom. 28(2002), 49-73.

[Ko] M. Kolounzakis, *The study of translation tiling with Fourier analysis*, Fourier Analysis and convexity, App. Numer. Harmon. Anal., Birkhauser, Boston, 2004, 131-187.

[KoM] M. N. Kolountzakis and M. Matolcsi, *Tiles with no spectra*, Forum Math. 18(2006), 519-528.

[LgW1] J. Lagarias and Y. Wang, *Tiling the line by translates of one tile*, Invent. Math. 124(1996), 341-365.

[LgW2] J. Lagarias and Y. Wang, *Self-affine tiles in* $\mathbb{R}^n$, Adv. Math. 121(1996), 21-49.

[LgW3] J. Lagarias and Y. Wang, *Integral self-affine tiles in* $\mathbb{R}^n$ *I. Standard and non-standard digit sets*, J. London Math.Soc. 53(1996), 161-179.

[LgW4] J. Lagarias and Y. Wang, *Integral self-affine tiles, Part II. Lattice tilings*, J. Fourier Anal. Appl. 3(1997), 84-102.

[LR] K.S. Lau and H. Rao, *On one-dimensional self-similar tilings and pq-tiles*, Trans. Amer. Math. Soc., 355(2003), 1401-1414.

[LLR1] C.K. Lai, K.S. Lau and H. Rao, *Spectral structure of digit sets of self-similar tiles on* $\mathbb{R}^1$, Trans. Amer. Math. Soc. 365(2013), 3831-3850.

[LLR2] C.K. Lai, K.S. Lau and H. Rao, *Classification of tile digit sets as product-forms*, Tran. Amer. Math. Soc. (2016).

[LL] K.S. Leung and K.S. Lau, *Disklikeness of planar self-affine tiles*, Trans. Amer. Math. Soc. 359(2007), 3337-3355.

[O] A. Odlyzko, *Non-negative digit sets in positional number systems*, Proc. London Math. Soc. 37(1978), 213-229.

[RWY] H.Rao, Z.Y Wen and Y.M. Yang *Dual systems of algebraic iterated function systems*, Adv. Math. 253(2014), 63-85.

[R] G. Rauzy *Nombres algébriques et substitutions*, Bull. Soc.Mah. France 110(1982), 147-178.

[SW] R. Strichartz and Y. Wang, *Geometry of self-affine tiles I*, Indiana Univ. Math. J. 48(1999), 1-23.

[T] T. Tao, *Fuglede's conjecture is false in 5 or higher dimensions*, Math. Res. Letters 11(2004), 251-258.

[Th] W. Thurston, *Groups, tilings and finite state automata*, AMS Colloquium Lecture Notes, 1989.

School of Mathematics and Statistics, Central China Normal University, Wuhan;
Department of Mathematics, The Chinese University of Hong Kong, Hong Kong
E-mail address: anlixianghai@163.com

Department of Mathematics, The Chinese University of Hong Kong, Hong Kong,
School of Mathematics and Statistics, Central China Normal University, Wuhan
E-mail address: kslau@math.cuhk.edu.hk