Discrete Mathematics and Theoretical Computer Science DMTCS vol. **8**, 2006, 129–140

Tiling $\mathbb{Z}^2$ with translations of one set

Hui Rao[1†] and Yu-Mei Xue[2]

[1] *Mathematical Department, Tsinghua university, Beijing 100084, China*
E-mail: hrao@math.tsinghua.edu.cn
[2]*Mathematical Department, Tsinghua university, Beijing 100084, China*
E-mail: YXue@math.tsinghua.edu.cn

received 6 Aug 2005, *revised 28 Mar 2006*, *accepted 19 Apr 2006*.

Let A be a finite subset of $\mathbb{Z}^2$. We say A tiles $\mathbb{Z}^2$ with the translation set C, if any integer $z \in \mathbb{Z}^2$ can be represented as $z_1 + z_2$, $z_1 \in A$, $z_2 \in C$ in a unique way. In this case we call A a $\mathbb{Z}^2$-tile and write $A \oplus C = \mathbb{Z}^2$. A tile A is said to be a normal $\mathbb{Z}^2$-tile if there exists a periodic set C such that $A \oplus C = \mathbb{Z}^2$. We characterize all normal $\mathbb{Z}^2$-tiles with prime cardinality.

Keywords: *tiling*, *periodicity*

1 Introduction

Let A be a finite subset of $\mathbb{Z}^n$. We denote by $\#A$ the cardinality of A. We say A is a $\mathbb{Z}^n$-*tile* (or *tile* in short), if there is a set $C \subseteq \mathbb{Z}^n$ such that any element $z \in \mathbb{Z}^n$ can be represented uniquely in the form

$$z = z_A + z_C, \quad z_A \in A,\ z_C \in C.$$

In this case, we say the pair (A, C) is a *translation tiling* of $\mathbb{Z}^n$ and write $A \oplus C = \mathbb{Z}^n$.

An infinite subset C of $\mathbb{Z}^n$ is *periodic*, if there is a vector λ such that $C = C + \lambda$; λ is said to be a period of C. A set C is k-*periodic* if it has k linearly independent periods.

The $\mathbb{Z}$-tiles have been studied by many authors ([New], [Sands], [Szabo], [Tij1], [Coven]). It is well known that if A is finite and $A \oplus C = \mathbb{Z}$, then the translation set C must be periodic ([Fuchs],[New]). Hence tiling problems are translated to problems of decompositions of the finite cyclic group $\mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n-1\}$. Newman [New] determined all $\mathbb{Z}$-tiles such that $\#A$ is a prime power. Particularly, when $\#A$ is a prime number, it is shown that

Proposition 1.1 *([New],[Sands]) Let p be a prime number and $A = \{s_0, s_1, \ldots, s_{p-1}\}$ be a subset of $\mathbb{Z}$. Then A is a $\mathbb{Z}$-tile if and only if*

$$\{\frac{s_0}{d}, \frac{s_1}{d}, \ldots, \frac{s_{p-1}}{d}\} \equiv \{0, 1, \ldots, p-1\} \pmod p$$

where $d = \gcd\{s_0, s_1, \ldots, s_{p-1}\}$ is the greatest common divisor.

[†] Supported by the German Research Foundation (DFG).

Remark 1.2 The above result can be expressed in terms of cyclotomic polynomials as follows ([Coven]: Lemma 1.1). Let $\Phi_n(z)$ denote the n-th cyclotomic polynomial. Then

A is a $\mathbb{Z}$-tile if and only if there exists an integer $k \geq 1$ such that $\Phi_{p^k}(z)$ divides the polynomial $A(z) = z^{s_0} + z^{s_1} + \cdots + z^{s_{p-1}}$.

Recently, based on works of Sands [Sands] and Tijdeman [Tij1], Coven and Meyerowitz [Coven] characterized all the $\mathbb{Z}$-tiles A such that $\#A$ has at most two prime factors.

However, the study of $\mathbb{Z}^n$-tiles seems to be untouched except the work of Beauquier and Nivat [BN]. [BN] gives an elegant characterization of the polyominoe tiles which are disk-like. This is a special case of $\mathbb{Z}^2$-tiles.

For the study of $\mathbb{Z}^n$-tiles, the first difficulty is the periodicity. We call a tile A a *normal* tile, if there is a periodic translation set C such that $A \oplus C = \mathbb{Z}^n$. Namely, a tile is normal if it can tile $\mathbb{Z}^n$ periodically. It has been conjectured that any translation tile of $\mathbb{Z}^n$ is normal.

Periodic Tiling Conjecture. (Lagarias and Wang [LW]) *Any $\mathbb{Z}^n$-tile is normal.*

This conjecture is true for $\mathbb{Z}$-tiles as we have mentioned, but it is widely open for higher dimensions. For more details we refer to Tijdeman [Tij2].

In the present paper, our main purpose is to characterize the normal $\mathbb{Z}^2$-tiles A with $\#A$ a prime number. Our main result is the following theorem.

Theorem 1.3 *Let $A = \{(s_0, t_0), \ldots, (s_{p-1}, t_{p-1})\}$ be a subset of $\mathbb{Z}^2$ where p is a prime number. Then A is a normal $\mathbb{Z}^2$-tile if and only if there exist two integers a and b, such that $as_0 + bt_0, \ldots, as_{p-1} + bt_{p-1}$ are distinct and $\{as_0 + bt_0, \ldots, as_{p-1} + bt_{p-1}\}$ is a $\mathbb{Z}$-tile.*

Roughly speaking, A is a normal tile with prime cardinality if and only if a projection of A is a $\mathbb{Z}$-tile.

This paper is organized as follows. In Section 2, we give several interesting results on periodicity of tilings of normal tiles. In Section 3, we prove Theorem 1.3 by using cyclotomic polynomials. An algorithm is given in Section 4 to check whether a set A with prime cardinality is a normal tile.

The referee pointed out to us that Szegedy [Sze] has proved a more general result as follows.

Theorem 1.4 *(Szegedy [Sze]) Let A be a $\mathbb{Z}^n$-tile with $\#A$ prime or $\#A = 4$, then A is normal.*

He gives in both cases an algorithm to decide the tiling problem, and our result Theorem 1.3 is covered by Szegedy's algorithm. However, while Szegedy's approach is primarily group-theoretic, we use elementary congruences and cyclotomic polynomials, which have been used successfully to study $\mathbb{Z}$-tiles by previous authors. We hope that our method can give a clue how to tackle $\mathbb{Z}^2$-tiles A with $\#A = pq$, where p, q are prime numbers.

2 Periodicity

In this section, we give some lemmas on the periodicity of tilings of normal tiles. Lemma 2.4 is an interesting generalization of a result of Tijdeman [Tij1].

Let $A \oplus C = \mathbb{Z}^2$, and let ϕ be an invertible linear transformation from $\mathbb{Z}^2$ to $\mathbb{Z}^2$. We may regard ϕ as an integral 2×2 matrix with determinant ± 1. It is obvious that $A \oplus C = \mathbb{Z}^2$ if and only if $\phi(A) \oplus \phi(C) = \mathbb{Z}^2$.

Proposition 2.1 *If A is a normal $\mathbb{Z}^2$-tile, then there is a 2-periodic set C such that $A \oplus C = \mathbb{Z}^2$.*

Proof: Suppose $A \oplus C' = \mathbb{Z}^2$ and C' is periodic. By applying a linear transformation, we may assume that a period of C' is $(c, 0)$, and further we assume that c is larger than the diameter of A. We divide the plane into squares of size $c \times c$, and denote by $S_{[a,b]}$ the square

$$S_{[a,b]} := [ac, (a+1)c] \times [bc, (b+1)c].$$

Let us consider the intersection of the translation set C' and $S_{[a,b]}$, and define

$$\mathcal{P}(a, b) = \{(s, t) - (ac, bc);\ (s, t) \in C' \cap S_{[a,b]}\}.$$

Now $(c, 0)$ is a period of C' implies that $\mathcal{P}(a, b) = \mathcal{P}(0, b)$.

Let b_1 and b_2 be two integers such that $\mathcal{P}(0, b_1) = \mathcal{P}(0, b_2)$, this must happen since the number of the patterns $\mathcal{P}(0, b)$, $b \in \mathbb{Z}$, is finite. Let

$$C = \bigcup_{m \in \mathbb{Z}} (C' \cap (\mathbb{Z} \times [b_1 c, b_2 c)) + m\vec{v}) \tag{1}$$

where $\vec{v} = (0, (b_2 - b_1)c)$. Then C is 2-periodic with periods $(c, 0)$ and $(0, (b_2 - b_1)c)$.

It remains to show that $A \oplus C = \mathbb{Z}^2$. By the above construction,

$$\{(s, t) \in C';\ b_1 c \leq t < b_2 c)\} + A$$

covers a strip of the plane. We shall show that this patch can be extended to a tiling. Notice that the configurations of C' in $\mathbb{Z} \times [b_1 c, (b_1 + 1)c]$ and $\mathbb{Z} \times [b_2 c, (b_2 + 1)c]$ are the same. Let $\mathbb{Z} \times [b_2 c, (b_2 + 2)c]$ have the same configuration as $\mathbb{Z} \times [b_1 c, (b_1 + 2)c]$, then the patch is extended with neither gap nor overlap. Repeating this procedure, the patch is extended to a tiling of the upper half plane. We can do the same for the lower half plane. Therefore we obtain a tiling and the translation set is C in (1). □

Lemma 2.2 *If a set C is 2-periodic, then it has two periods $(M, 0)$ and $(0, N)$ for some integers M and N.*

Proof: Suppose λ_1 and λ_2 are two linear independent periods of C. Then $a\lambda_1 + b\lambda_2$ is also a period of C. Clearly we can choose a, b properly to have periods of the form $(M, 0)$ and $(0, N)$. □

For a finite set A, we define a polynomial $A(x, y)$ as

$$A(x, y) := \sum_{(s,t) \in A} x^s y^t.$$

For a polynomial $P(x, y) = \sum x^s y^t$, define

$$P(x, y) \pmod{x^M - 1, y^N - 1} = \sum x^{s \pmod{M}} y^{t \pmod{N}}.$$

Then as a corollary of Proposition 2.1 and Lemma 2.2, we have

Corollary 2.3 *A finite set $A \subset \mathbb{Z}^2$ is a normal tile if and only if there exists a finite set $B \subset \mathbb{Z}^2$ and positive integers M, N such that $\#A\#B = MN$ and*

$$A(x, y)B(x, y) \equiv (1 + x + \cdots + x^{M-1})(1 + y + \cdots + y^{N-1}) \pmod{x^M - 1, y^N - 1}. \tag{2}$$

The following lemma is a generalization of a result of Tijdeman [Tij1], which concerns the $\mathbb{Z}$-tilings. Coven and Meyerowitz ([Coven]: Lemma 3.1) gave a nice proof of Tijdeman's Lemma. Our proof is a generalization of the proof in [Coven].

Lemma 2.4 *Let A and B be finite subsets of $\mathbb{Z}^2$ with non-negative coordinates with corresponding polynomials $A(x, y)$ and $B(x, y)$ and let $MN = \#A\#B$. If equation (2) holds and p is a prime which is not a factor of $\#A$, then*

$$A(x^p, y^p)B(x, y) \equiv (1 + x + \cdots + x^{M-1})(1 + y + \cdots + y^{N-1}) \pmod{x^M - 1, y^N - 1}.$$

Proof: Since p is prime, $A(x^p, y^p) \equiv (A(x, y))^p \pmod p$, *i.e.*, when the coefficients are reduced modulo p. Let $G_{M,N}(x, y) = (1 + x + \cdots + x^{M-1})(1 + y + \cdots + y^{N-1})$. Then

$$A(x^p, y^p)B(x, y) \equiv (A(x, y))^{p-1}A(x, y)B(x, y) \equiv (A(x, y))^{p-1}G_{M,N}(x, y),$$

where $\equiv$ means the exponents of x and y are reduced modulo M and N respectively, and then the coefficients are reduced modulo p. Since

$$x^i y^j G_{M,N}(x, y) \equiv G_{M,N}(x, y) \pmod{x^M - 1, y^N - 1}$$

holds for any i, j, we have

$$(A(x, y))^{p-1}G_{M,N}(x, y) \equiv (A(1, 1))^{p-1}G_{M,N}(x, y) \pmod{x^M - 1, y^N - 1}.$$

Since p does not divide $\#A$, Fermat's Little Theorem yields $(A(1, 1))^{p-1} \equiv 1 \pmod p$. Therefore

$$A(x^p, y^p)B(x, y) \equiv G_{M,N}(x, y),$$

where the exponents of x and y are reduced modulo M and N respectively, and then the coefficients are reduced modulo p.

Since $A(1, 1)B(1, 1) = G_{M,N}(1, 1) = MN$, both $A(x^p, y^p)B(x, y)$ and $G_{M,N}(x, y)$ have nonnegative coefficients whose sum is MN. Consider the following reductions.

(R1) $A(x^p, y^p)B(x, y)$ is reduced modulo $x^M - 1, y^N - 1$, yielding a polynomial $G^*(x, y)$.
(R2) The coefficients of $G^*(x, y)$ are reduced modulo p, yielding $G_{M,N}(x, y)$.

Reduction (R1) preserves the sum of the coefficients, but (R2) reduces the sum by some nonnegative multiple of p. Because the sum of the coefficients of both $G^*(x, y)$ and $G_{M,N}(x, y)$ is MN, that multiple is 0. Therefore $G^*(x, y) = G_{M,N}(x, y)$. □

The following theorem is a two dimensional generalization of Lemma 2.3 in [Coven]. We have shown that if A is a normal tile, then there is a translation set with periods $(M, 0)$ and $(0, N)$. Theorem 2.5 says further that we may assume that M and N have the same prime factors as $\#A$.

Theorem 2.5 *If $A \subset \mathbb{Z}^2$ is a normal tile, then there exists a finite set $B \subset \mathbb{Z}^2$ and two integers M and N, M and N are products of prime factors of $\#A$, such that*

$$A(x, y)B(x, y) \equiv (1 + x + \cdots + x^{M-1})(1 + y + \cdots + y^{N-1}) \pmod{x^M - 1, y^N - 1}.$$

Proof: If $A \oplus C = \mathbb{Z}^2$ is a tiling of periods $(M, 0)$ and $(0, N)$ and $r > 1$ is a prime factor of M which does not divides $\#A$, then by Lemma 2.4, $rA \oplus C = \mathbb{Z}^2$. Therefore $rA \oplus C_0 = r\mathbb{Z}^2$ where $C_0 = \{(s,t) \in C;\ s \equiv 0, t \equiv 0 \pmod r\}$.

Since the periods $(M, 0)$ and $(0, rN)$ of C are also periods of C_0, we conclude that $A \oplus C_0/r = \mathbb{Z}^2$ is a tiling with periods $(M/r, 0)$ and $(0, N)$. Continuing this procedure, we may remove any prime factor r from M which does not divide $\#A$. $\square$

3 Tiles with prime cardinality

In this section, we prove Theorem 1.3, the main result of this paper.

Proposition 3.1 *Let $A = \{(s_0, t_0), (s_1, t_1), \dots (s_{n-1}, t_{n-1})\}$ be a subset of $\mathbb{Z}^2$. If there exist two integers a and b such that $as_0 + bt_0, as_1 + bt_1, \dots, as_{n-1} + bt_{n-1}$ are distinct and $\{as_0 + bt_0, as_1 + bt_1, \dots, as_{n-1} + bt_{n-1}\}$ is a $\mathbb{Z}$-tile, then A is a normal $\mathbb{Z}^2$-tile.*

Proof: Let $k \in \mathbb{Z}$ and $k \neq 0$, then obviously E is a $\mathbb{Z}$-tile if and only if kE is a $\mathbb{Z}$-tile ([Coven]: Lemma 1.4).

Case 1. $a \neq 0$ and $b = 0$ (or, vice versa, $a = 0$ and $b \neq 0$). By assumption $\{as_0, \dots, as_{n-1}\}$ is a $\mathbb{Z}$-tile, so $\{s_0, \dots, s_{n-1}\}$ is also a $\mathbb{Z}$-tile. Hence there is a translation set F such that

$$\{s_0, \dots, s_{n-1}\} \oplus F = \mathbb{Z}. \tag{3}$$

Let $C = F \times \mathbb{Z}$. Clearly $A \oplus C = \mathbb{Z}^2$ and C is periodic.

Case 2. $ab \neq 0$. We may assume that a and b are coprime. Let u, v be two integers such that $au - bv = 1$, and let

$$\phi = \begin{pmatrix} a & b \\ v & u \end{pmatrix}.$$

In the following, we will regard ϕ as a linear operator from $\mathbb{Z}^2$ to $\mathbb{Z}^2$. Then ϕ gives a one-to-one map from $\mathbb{Z}^2$ to $\mathbb{Z}^2$. Since

$$\phi(A) = \{(as_0 + bt_0, vs_0 + ut_0), \dots, (as_{n-1} + bt_{n-1}, vs_{n-1} + ut_{n-1})\}$$

and $\{as_0 + bt_0, as_1 + bt_1, \dots, as_{n-1} + bt_{n-1}\}$ is a $\mathbb{Z}$-tile, so by the conclusion of Case 1 (by choosing $a = 1, b = 0$ there), $\phi(A)$ is a normal tile. Hence A is also a normal tile. $\square$

From now on, we prove the other direction of Theorem 1.3. Suppose A is a normal tile and $\#A = p$ is a prime. Then by the discussion of Section 2, there is a translation set C with periods $(p^m, 0)$ and $(0, p^m)$ for some positive integer m. Let

$$D_1 = \{(1, b);\ b = 0, 1, \dots, p^m - 1\}, \ \ D_2 = \{(a, 1);\ a = 0, p, 2p, \dots, p^m - p\},$$

and set $D = D_1 \cup D_2$. If p^k divides x but p^{k+1} does not divide x, then we write $v_p(x) = k$. For two integers s, t we denote $v_p(s,t) := v_p(\gcd\{s,t\})$. First we establish two lemmas.

Lemma 3.2 *Let (s,t) be a point of $\mathbb{Z}^2$ with $v_p(s,t)=k$. Then the constant term of*

$$\sum_{(a,b)\in D} z^{as+bt} \pmod{z^{p^m}-1} \tag{4}$$

is p^k when $k<m$, is $p^m(1+\frac{1}{p})$ when $k\geq m$.

Proof: When $v_p(s,t)\geq m$, each term in (4) is 1, and hence the constant term of (4) is $\#D=p^m(1+\frac{1}{p})$. So let us assume that $v_p(s,t)<m$.

Without loss of generality, let us assume that $v_p(s)\geq v_p(t)$, which implies $v_p(t)=k$. There are exactly p^k elements (in sense of a multiple set) in $\{s+bt;\ 0\leq b\leq p^m-1\}$ which can be divided by p^m. Hence the constant term of

$$\sum_{(a,b)\in D_1} z^{as+bt} \pmod{z^{p^m}-1} = \sum_{0\leq b\leq p^m-1} z^{s+bt} \pmod{z^{p^m}-1}$$

is p^k. Clearly the constant term of

$$\sum_{(a,b)\in D_2} z^{as+bt} \pmod{z^{p^m}-1}$$

is 0. The lemma is proved. □

Lemma 3.3 is the key lemma in this paper.

Lemma 3.3 *Let B be a subset of $\mathbb{Z}^2$ with $\#B=p^n$, and let $B(x,y)$ be the corresponding polynomial. If for any non-negative coprime integers a,b, holds*

$$B(z^a,z^b)\equiv p^{n-m}(1+z+\cdots+z^{p^m-1}) \pmod{z^{p^m}-1},$$

then $n\geq 2m$ and

$$B(x,y)\equiv p^{n-2m}(1+x+\cdots+x^{p^m-1})(1+y+\cdots+y^{p^m-1}) \pmod{x^{p^m}-1, y^{p^m}-1}.$$

Proof: We say B is *equally-distributed* in $\{0,1,\ldots,p^m-1\}\times\{0,1,\ldots,p^m-1\}$ if

$$\#\{(g,h)\in B;\ g\equiv s, h\equiv t \pmod{p^m}\} = \#B/p^{2m}$$

for any $(s,t)\in\{0,1,\ldots,p^m-1\}\times\{0,1,\ldots,p^m-1\}$. Let c_i be the number of points (g,h) in B with $v_p(g,h)\geq i$; we shall call $c_0=c_0(B), c_1=c_1(B),\ldots,c_m=c_m(B)$ the *indices* of the set B. We claim that:

Claim. For a set $B\subset\mathbb{Z}^2$ with $\#B=p^n\geq p^{2m}$, there exists a translation $B^*=B+(s^*,t^*)$ such that

$$c_0(B^*)=p^n, c_1(B^*)\geq p^{n-2}, c_2(B^*)\geq p^{n-4},\ldots,c_m(B^*)\geq p^{n-2m}. \tag{5}$$

Moveover, if B is not equally-distributed in $\{0,1,\ldots,p^m-1\}\times\{0,1,\ldots,p^m-1\}$, then at least one of the inequalities is strict.

We prove this claim by induction on m. When $m = 1$, the claim is obviously true.

Clearly $c_0(B + (s,t)) = \#B = p^n$ for any (s,t).

When (s,t) runs over $\{0, 1, \ldots, p-1\} \times \{0, 1, \ldots, p-1\}$, we have

$$\sum c_1(B + (s,t)) = \#B = p^n,$$

hence there exists $(s_1, t_1) \in \{0, 1, \ldots, p-1\} \times \{0, 1, \ldots, p-1\}$ such that

$$c_1(B + (s_1, t_1)) \geq p^{n-2}$$

by the pigeon-hole principle. Let

$$B_1 := \{(g,h) \in B + (s_1, t_1);\ v_p(g,h) \geq 1\},$$

then $\#B_1 \geq p^{n-2}$. Let $\tilde{B}_1$ be any subset of B_1 with cardinality $\#B_1 = p^{n-2}$ and set $B_2 = \tilde{B}_1/p$.

By induction hypothesis, there exists (s_2, t_2) such that for $B_2^* = B_2 + (s_2, t_2)$, it holds that

$$c_0(B_2^*) = p^{n-2}, c_1(B_2^*) \geq p^{n-4}, c_2(B_2^*) \geq p^{n-6}, \ldots, c_{m-1}(B_2^*) \geq p^{n-2m}.$$

Set $(s^*, t^*) = (s_1, t_1) + p(s_2, t_2)$ and

$$B^* = B + (s^*, t^*) = B + (s_1, t_1) + p(s_2, t_2).$$

Then:

(i) $c_0(B^*) = p^n$ as we have mentioned before.

(ii) $c_1(B^*) = c_1\left(B + (s_1, t_1)\right) \geq p^{n-2}$ by the choice of (s_1, t_1).

(iii) For $i \geq 2$, notice that

$$B^* \supset B_1 + p(s_2, t_2) \supset \tilde{B}_1 + p(s_2, t_2) = pB_2 + p(s_2, t_2) = pB_2^*,$$

therefore $c_i(B^*) \geq c_{i-1}(B_2^*) \geq p^{n-2i}$. The first assertion of the claim is proved.

Suppose B is not equally distributed in $\{0, 1, \ldots, p^m - 1\} \times \{0, 1, \ldots, p^m - 1\}$. If $c_1(B + (s,t)) > p^{n-2}$, then the claim already holds. So we assume that $c_1(B + (s,t)) = p^{n-2}$ for all $(s,t) \in \{0, 1, \ldots, p-1\} \times \{0, 1, \ldots, p-1\}$. Choose (s_1, t_1) such that $B_2 = \left(B + (s_1, t_1)\right)/p$ is not equally-distributed in $\{0, 1, \ldots, p^{m-1} - 1\} \times \{0, 1, \ldots, p^{m-1} - 1\}$. Again we get the desired inequality by the induction hypothesis. Our claim is proved.

Now we return to the proof of the lemma. Let us first assume that $p^n \geq p^{2m}$.

If B is equally-distributed in $\{0, 1, \ldots, p^m - 1\} \times \{0, 1, \ldots, p^m - 1\}$, then obviously the lemma holds. Let us assume that B is not equally-distributed in $\{0, 1, \ldots, p^m - 1\} \times \{0, 1, \ldots, p^m - 1\}$.

Notice that if B satisfies the conditions of the lemma, then any translation of B, particularly B^* in the Claim, also satisfies the conditions of the lemma. Let us consider the polynomial

$$\sum_{(a,b) \in D} B^*(z^a, z^b) = \sum_{(a,b) \in D} \sum_{(s,t) \in B^*} z^{as+bt} = \sum_{(s,t) \in B^*} \sum_{(a,b) \in D} z^{as+bt}.$$

Under the assumptions of the lemma, an easy calculation shows that the constant term of

$$\sum_{(a,b)\in D} B^*(z^a, z^b) \pmod{z^{p^m} - 1} \tag{6}$$

is $p^n(1+\frac{1}{p})$. On the other hand, by Lemma 3.2, the constant term of (6) is

$$\begin{aligned} & (c_0^* - c_1^*) + (c_1^* - c_2^*)p + \cdots + (c_{m-1}^* - c_m^*)p^{m-1} + c_m^*(p^m + p^{m-1}) \\ = \quad & c_0^* + c_1^*(p-1) + \cdots + c_{m-1}^*(p^{m-1} - p^{m-2}) + c_m^* p^m, \end{aligned}$$

where $c_i^* = c_i(B^*)$ are the indices of B^*. This together with (5) implies that

$$c_0^* = p^n, c_1^* = p^{n-2}, c_2^* = p^{n-4}, \ldots, c_m^* = p^{n-2m}.$$

This contradicts the second assertion of the Claim. The lemma is proved in the case $n \geq 2m$.

Finally we show that $n \geq 2m$ must hold. Otherwise, let $\tilde{B}$ be a multi-set which has the same elements as B, but the multiplicity of each element multiplied by a factor $p^{n'}$ so that $\#\tilde{B} = p^{n+n'} \geq p^{2m}$. It is seen that $\tilde{B}$ also satisfies the conditions of the lemma. Therefore, $\tilde{B}$ is equally-distributed in $\{0,1,\ldots,p^m-1\} \times \{0,1,\ldots,p^m-1\}$ and so that B is also equally-distributed. It follows that $n \geq 2m$. The lemma is proved. □

Proof of Theorem 1.3. One direction is proved by Proposition 3.1, we prove the other direction in the following.

Let $A = \{(s_0,t_0),(s_1,t_1),\ldots(s_{p-1},t_{p-1})\}$ be a normal tile of $\mathbb{Z}^2$ with $\#A = p$. We may assume that $(s_0,t_0) = (0,0)$. Then according to Theorem 2.5, there exist a set B and $M = p^m$, such that

$$A(x,y)B(x,y) \equiv (1+x+\cdots+x^{M-1})(1+y+\cdots+y^{M-1}) \pmod{x^M - 1, y^M - 1}. \tag{7}$$

Note that $\#B = p^{2m-1}$. Suppose for any non-negative coprime integers a, b the set

$$\{as_0 + bt_0, as_1 + bt_1, \ldots, as_{p-1} + bt_{p-1}\}$$

is not a $\mathbb{Z}$-tile. Then by Remark 1.2, for any integer $k \geq 1$, $\Phi_{p^k}(z) = 1 + z^{p^{k-1}} + \cdots + z^{(p-1)p^{k-1}}$ does not divide

$$A(z^a, z^b) = z^{as_0+bt_0} + z^{as_1+bt_1} + \cdots + z^{as_{p-1}+bt_{p-1}},$$

where $\Phi_n(x)$ denotes the n-th cyclotomic polynomial. From (7), we have

$$A(z^a, z^b)B(z^a, z^b) \equiv p^m(1+z+\cdots+z^{p^m-1}) \pmod{z^{p^m} - 1}.$$

Hence $\Phi_{p^k}(z)$ $(1 \leq k \leq m)$ must be factors of $B(z^a, z^b)$, which implies that $B(z^a, z^b)$ is a multiple of $\Phi_p(z)\Phi_{p^2}(z)\cdots\Phi_{p^m}(z) = 1 + z + \cdots + z^{p^m-1}$. Hence for any non-negative coprime integers a, b,

$$B(z^a, z^b) \equiv p^{m-1}(1+z+\cdots+z^{p^m-1}) \pmod{z^{p^m} - 1}.$$

Now by Lemma 3.3, we have that $\#B \geq p^{2m}$ which contradicts with $\#B = p^{2m-1}$. This contradiction proves the theorem. □

4 Algorithm

In this section, we give an algorithm to check the conditions of Theorem 1.3. We note that our algorithm is essentially identical with the algorithm given by Szegedy [Sze].

4.1 Span of A.

Let $\mathcal{L}(A)$ be the set of $\mathbb{Z}$-linear combinations of vectors in A, which is a sublattice of $\mathbb{Z}^2$. If the rank of $\mathcal{L}(A)$ is 1, then $A = \{a_0v, a_1v, \ldots, a_{p-1}v\}$ for some vector $v \in \mathbb{Z}^2$; in this case, A is a tile if and only if $\{a_0, a_1, \ldots, a_{p-1}\}$ is a $\mathbb{Z}$-tile. So we assume that $\mathcal{L}(A)$ is a full-rank lattice. Then there is an integral matrix ϕ such that

$$\mathcal{L}(A) = \phi(\mathbb{Z}^2).$$

The matrix ϕ can be obtained in the following way. All the vectors in A form a $p \times 2$ matrix

$$\begin{pmatrix} s_0 & t_0 \\ s_1 & t_1 \\ \vdots & \vdots \\ s_{p-1} & t_{p-1} \end{pmatrix}$$

By applying elementary row operators, the matrix can be reduced to the form

$$\begin{pmatrix} s & t \\ 0 & t' \\ 0 & 0 \\ \vdots & \vdots \\ 0 & 0 \end{pmatrix}$$

Clearly $\mathcal{L}(A) = \mathcal{L}\{(s,t), (0,t')\} = \phi(\mathbb{Z}^2)$ where

$$\phi = \begin{pmatrix} s & 0 \\ t & t' \end{pmatrix}.$$

The linear span $\mathcal{L}(A) \neq \mathbb{Z}^2$ if and only if $|\det \phi| > 1$.

Let $A' = \phi^{-1}(A)$. We claim that *A tiles $\mathbb{Z}^2$ if and only if A' tiles $\mathbb{Z}^2$*. Suppose A tiles $\mathbb{Z}^2$, i.e., $A \oplus C = \mathbb{Z}^2$. Let $C_0 = C \cap \phi(\mathbb{Z}^2)$. Then $A \oplus C_0 = \phi(\mathbb{Z}^2)$, $A' \oplus \phi^{-1}(C_0) = \mathbb{Z}^2$ and so that A' tiles $\mathbb{Z}^2$. On the other hand, suppose A' tiles $\mathbb{Z}^2$, *i.e.*, $A' \oplus C' = \mathbb{Z}^2$. Let R be a complete representative system of residues $\mathbb{Z}^2/\phi(\mathbb{Z}^2)$. Then $A \oplus \phi(C') = \phi(\mathbb{Z}^2)$, and so that $A \oplus C = \mathbb{Z}^2$ where $C = \phi(C') \oplus R$.

4.2 Algorithm

So, to check whether A is a normal tile, it suffices to check whether A' is a normal tile. Hence, from now on, we assume that $\mathcal{L}(A) = \mathbb{Z}^2$.

Proposition 4.1 *If $\mathcal{L}(A) = \mathbb{Z}^2$, then there exist integers a, b satisfying the conditions of Theorem 1.3, if and only if there exist integers $a, b \in \{0, 1, \ldots, p-1\}$ satisfying these conditions.*

Proof: As we have pointed out, we may assume that $(a, b) = 1$. Hence at least one of a, b is coprime to p, let us say, $(a, p) = 1$. The integers a, b satisfying the conditions of Theorem 1.3 means that there exists an integer m such that

$$as_i + bt_i \equiv l_i p^m \pmod{p^{m+1}}$$

and $\{l_0, \dots, l_{p-1}\}$ is a complete representative system modulo p. If $m = 0$, we may choose $a \pmod p, b \pmod p$ instead of a, b, and the proposition is proved.

Suppose $m \geq 1$. Let c be an integer such that $ac \equiv 1 \pmod{p^{m+1}}$. Then

$$acs_i + bct_i \equiv l_i cp^m \pmod{p^{m+1}},$$

$$s_i + bct_i \equiv l_i cp^m \pmod{p^{m+1}},$$

where $\{cl_0, \dots, cl_{p-1}\}$ is still a complete representative system modulo p. Write $s_i + bct_i = L_i p^m$, let ϕ be the matrix

$$\phi = \begin{pmatrix} p & -bc \\ 0 & 1 \end{pmatrix}.$$

Then $(s_i, t_i) = \phi(L_i p^{m-1}, t_i)$ and $\det \phi = p$, which contradicts with $\mathcal{L}(A) = \mathbb{Z}^2$. □

Algorithm:

Step 1. Find the matrix ϕ such that $\mathcal{L}(A) = \phi(\mathbb{Z}^2)$. If $\det \phi = 0$, then the problem is reduced to a $\mathbb{Z}$-tiling problem; otherwise set

$$A' = \phi^{-1}(A) = \{(s'_0, t'_0), (s'_1, t'_1), \dots, (s'_{p-1}, t'_{p-1})\}.$$

Step 2. Check whether there exist integers $a, b \in \{0, 1, \dots, p-1\}$ such that $as'_0 + bt'_0, as'_1 + bt'_1, \dots, as'_{p-1} + bt'_{p-1}$ are distinct and form a $\mathbb{Z}$-tile.

4.3 $\#A$ is a prime power.

We remark that the conclusion of Theorem 1.3 is false even for normal tiles A with $\#A = p^2$. For example, let $p = 3$ and

$$A = \{(0,0), (0,2), (1,1), (1,2), (1,3), (2,0), (2,1), (2,2), (3,1)\}.$$

Clearly the only translation set is $C = 3\mathbb{Z} \times 3\mathbb{Z}$ and so that A is a normal tile. The periods of C are $(3x, 3y)$ where $x, y \in \mathbb{Z}$. See Figure 1.

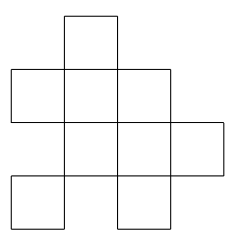

Figure 1.

We show that that A does not satisfy the condition of Theorem 1.3. Suppose not, then there are integers a, b such that $as_0+bt_0, as_1+bt_1, \ldots, as_{n-1}+bt_{n-1}$ are distinct and $\{as_0+bt_0, as_1+bt_1, \ldots, as_{n-1}+bt_{n-1}\}$ is a $\mathbb{Z}$-tile. We may assume that a and b are coprime. Let u, v be two integers such that $au-bv=1$, and let

$$\phi = \begin{pmatrix} a & b \\ v & u \end{pmatrix}.$$

Since

$$\phi(A) = \{(as_0+bt_0, vs_0+ut_0), \ldots, (as_{n-1}+bt_{n-1}, vs_{n-1}+ut_{n-1})\}$$

and $\{as_0+bt_0, as_1+bt_1, \ldots, as_{n-1}+bt_{n-1}\}$ is a $\mathbb{Z}$-tile, we infer that $\phi(C)$, the unique translation set of $\phi(A)$, has a period $(0,1)$. So there exist $x, y \in \mathbb{Z}$ such that $\phi(3x, 3y) = (0,1)$, which is impossible.

Acknowledgements

The authors thank Professor S. Akiyama, M. Nivat and J. Tamura for many valuable discussions. The authors would like to thank the anonymous referees for leading us to the work of Szegedy and for helping us to improve the paper.

References

[BN] Beauquier D. and Nivat M., On translating one polyomino to tile the plane, *Discrete Comput. Geom.,* **6** (1991), 575–592.

[Coven] Coven E. and Meyerowitz A., Tiling the integers with translates of one finite set, *Journal of Algebra*, **212** (1999), 161–174.

[Fuchs] Fuchs L., Abelian groups, Oxford-New York: Pergamon Press, 3rd edition, 1960.

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

[New] Newman D. J., Tesselation of integers, *J. Number Theory*, **9** (1977), 107–111.

[Sands] Sands A. D., On Keller's conjecture for certain cyclic groups, *Proc. Edinburgh Math. Soc. (2)*, **22** (1979), 17–21.

[Szabo] Szabó S., A type of factorization of finite abelian groups, *Discrete Math.*, **54** (1985), 121–124.

[Sze] Szegedy, M., Algorithms to tile the infinite grid with finite clusters. *focs, 39th Annual IEEE Symposium on Foundations of Computer Science.* (1998). Preprint available at http://www.cs.rutgers.edu/∼szegedy/

[Tij1] Tijdeman R., Decomposition of the integers as a direct sum of two subsets, in "Number Theory (Paris, 1992-1993)", London Math. Soc. Lecture Note Ser., Vol 215, pp. 261-276. Cambridge Univ. Press, Cambridge, 1995.

[Tij2] Tijdeman, R., Perodicity and almost-periodicity. Preprint (2002) available at http://www.math.leidenuniv.nl/∼tijdeman/