Analysis Math., **44 (4)** (2018), 433–449
DOI: 10.1007/s10476-018-0606-1
First published online October 17, 2018

TILING, CIRCLE PACKING AND EXPONENTIAL SUMS OVER FINITE FIELDS

C. D. HAESSIG[1], A. IOSEVICH[1,*,†], J. PAKIANATHAN[1,†], S. ROBINS[2] and L. VAICUNAS[3]

[1]Department of Mathematics, University of Rochester, Rochester, NY, U. S. A.
e-mails: c.d.haessig@rochester.edu, iosevich@gmail.com, jonathan.pakianathan@rochester.edu

[2]Institute of Mathematics and Statistics, University of São Paulo,
São Paulo, SP, 05508-090, Brazil
e-mail: sinai.robins@gmail.com

[3]Department of Mathematics, Michigan State University, , East Lansing, MI 48824, U. S. A.
e-mail: vaicunas@msu.edu

(Received August 11, 2016; revised April 27, 2017; accepted May 29, 2017)

Abstract. We study the problem of tiling and packing in vector spaces over finite fields and its connections with zeroes of classical exponential sums. In particular, we study tilings mostly in two and three dimensions and packings in dimension two. A combination of Fourier analytic and algebraic methods is employed.

1. Introduction

1.1. Tiling characterization in $\mathbb{F}_p^2$ and $\mathbb{F}_p^3$. Tiling is one of the most diverse and ubiquitous concepts of modern mathematics. In Euclidean space, we say that a domain $\Omega \subset \mathbb{R}^d$ tiles by $A \subset \mathbb{R}^d$ if

$$\sum_{a \in A} \Omega(x-a) = 1 \quad \text{a.e.},$$

where $\Omega(x)$ denotes the characteristic function of Ω. Much work has been done over the years on this subject matter in a variety of contexts. See for example, [1], [3], [10] and the references contained therein.

* Corresponding author.

† The work of the second and third authors was partially supported by the NSA grant H98230-15-1-0319

Key words and phrases: tiling, circle packing, exponential sum, finite field, algebraic tiling, multiple packing, polynomial method, Jacobian conjecture.

Mathematics Subject Classification: primary 43A46, secondary 43A85, 65T50.

The purpose of this paper is to study tiling in vector spaces over finite fields. Let $E \subset \mathbb{F}_q^d$, the d-dimensional vector space over the finite field with q elements.

DEFINITION 1.1. Let $A \subset \mathbb{F}_q^d$. We say that E k-tiles $\mathbb{F}_q^d$ by A if

$$\sum_{a \in A} E(x-a) = k \quad \text{for every } x \in \mathbb{F}_q^d.$$

Note that k-tiling means that each point in $\mathbb{F}_q^d$ is covered exactly k times by some translate of the set E. There is an immediate duality here that follows from the definition: E k-tiles $\mathbb{F}_q^d$ by A if and only if A k-tiles $\mathbb{F}_q^d$ by E. For some of the historical perspectives and the growing body of work on multiple tilings, we refer the reader to [5], [6], [7], and [11].

We first provide a simple characterization of k-tiling in terms of the coefficients of the Fourier transform. Given $U \subset \mathbb{F}_q^d$, $|U|$ denotes the number of elements in U.

LEMMA 1.2 (Fourier characterization). *The set $E \subset \mathbb{F}_q^d$ multi-tiles $\mathbb{F}_q^d$ by $A \subset \mathbb{F}_q^d$ at level k if and only if*

$$|A| \cdot |E| = kq^d$$

and

$$\widehat{E}(m) \cdot \widehat{A}(m) = 0 \quad \textit{for every } m \neq \vec{0}.$$

Here and throughout, given $f\colon \mathbb{F}_q^d \to \mathbb{C}$, we recall the discrete Fourier transform

$$\widehat{f}(m) \equiv q^{-d} \sum_{x \in \mathbb{F}_q^d} \chi(-x \cdot m) f(x),$$

where χ is a non-trivial additive character on $\mathbb{F}_q$.

PROOF. If E and A k-tile $\mathbb{F}_q^d$, then $E \star A = k$. After taking the Fourier transform, this equation yields $q^d \cdot \widehat{E} \cdot \widehat{A} = k\delta_0$, where δ_0 is the Kronecker delta function. The conclusion of the lemma follows. □

In order to illustrate Lemma 1.2, let's consider the following examples.

EXAMPLE 1.3. Suppose that $E = \{(t, f(t)) : t \in \mathbb{F}_q\}$, where $f\colon \mathbb{F}_q \to \mathbb{F}_q$ is arbitrary. Then it is clear that E tiles by $A = \{(0,c) : c \in \mathbb{F}_q\}$. To see how this fits in with Theorem 1.2, observe that

$$\widehat{A}(m) = q^{-2} \sum_{c \in \mathbb{F}_q} \chi(-cm_2).$$

It follows directly from the orthogonality relations for characters that this quantity is 0 if $m_2 \neq 0$ and q^{-1} if $m_2 = 0$. In other words, $\widehat{A}(m)$ is non-zero on $\{(t,0) : t \in \mathbb{F}_q\}$ and 0 everywhere else. On the other hand,

$$\widehat{E}(m_1,0) = q^{-2} \sum_{x_1 \in \mathbb{F}_q} \chi(-x_1 m_1) = 0 \quad \text{if } m_1 \neq 0.$$

Therefore $\widehat{E}(m) \cdot \widehat{A}(m) = 0$ if $m \neq \vec{0}$.

This example easily generalizes to sets in $\mathbb{F}_q^d$ of the form

$$E = \big\{(x_1, x_2, \dots, x_j, f_1(\vec{x}), \dots, f_{d-j}(\vec{x})\big\},$$

where $\vec{x} = (x_1, \dots, x_j)$.

EXAMPLE 1.4. Let H_j denote a j-dimensional affine subspace of $\mathbb{F}_q^d$, $1 \leq j \leq d-1$. By elementary linear algebra, H_j tiles by $H_j^{\perp}$ at level 1. Let us see how this fits in with Theorem 1.2. We have

$$\widehat{H}_j(m) = q^{-(d-j)} H_j^{\perp}(m), \tag{1.1}$$

where $H_j^{\perp}$ is the orthogonal subspace. It follows that

$$\widehat{H}_j(m)\widehat{H_j}^{\perp}(m) = q^{-(d-j)} \cdot q^{-j} \cdot H_j^{\perp}(m) \cdot H_j(m) = 0 \quad \text{if } m \neq \vec{0}.$$

EXAMPLE 1.5. Let p be a prime and let $E = \{0, 1, 2, \dots, k-1\}$, $k \geq 2$. Let $A = \mathbb{Z}_p$. Then E k-tiles $\mathbb{Z}_p$ by A and does not j-tile $\mathbb{Z}_p$ for any $j < k$. It is instructive to note here that since $A = \mathbb{Z}_p$ and A is viewed as a subset of $\mathbb{Z}_p$, $\widehat{A}$ vanishes identically away from 0.

The examples above give us some hints about characterization of 1-tilings, which we now proceed to classify.

DEFINITION 1.6. Suppose that E 1-tiles $\mathbb{F}_q^d$ by A. We say that $E \subset \mathbb{F}_q^d$ is a *graph* if there is a coordinate decomposition

$$\mathbb{F}_q^d = \mathbb{F}_q^s \oplus \mathbb{F}_q^{d-s} = \big\{(x_1, \dots, x_s, y_1, \dots, y_{d-s})\big\}$$

such that

$$E = \big\{(\widehat{x}, f(\widehat{x}) : \widehat{x} \in \mathbb{F}_q^s\big\} = \text{Graph}(f)$$

for some function $f \colon \mathbb{F}_q^s \to \mathbb{F}_q^{d-s}$ with respect to these coordinates.

Note given such an $E = \text{Graph}(f)$, we can come up with sets E, A such that E 1-tiles $\mathbb{F}_q^d$ by A. Here

$$A = \vec{0} \oplus \mathbb{F}_q^{d-s} = \big\{(\vec{0}, \widehat{y}) : \widehat{y} \in \mathbb{F}_q^{d-s}\big\},$$

so all such graphs give 1-tilings.

As some of our results only apply for prime fields $\mathbb{F}_p$ where p is a prime, we should point out that any tiling pair (E, A) in $\mathbb{F}_q^d$ with $q = p^\ell$ can also be viewed as a tiling pair in $\mathbb{F}_p^{d\ell}$ as $\mathbb{F}_q \cong \mathbb{F}_p^\ell$ as additive groups. Thus as tiling only uses the additive structure of the ambient space, it is more informative to work only in vector spaces V over the prime fields $\mathbb{F}_p$, as the dimension of V over $\mathbb{F}_p$ more accurately characterizes structural questions regarding tilings than the dimension of V over other finite fields.

The following is a characterization of 1-tilings in $\mathbb{F}_p^2$ when p is a prime.

THEOREM 1.7 (classification of 1-tilings of the plane). *Let $q = p$, a prime and suppose that E 1-tiles $\mathbb{F}_p^2$ by A. Then E is a graph. Thus either $|E| = 1$ and $A = \mathbb{F}_p^2$, $E = \mathbb{F}_p^2$ and $|A| = 1$, or there is a function $f\colon \mathbb{F}_p \to \mathbb{F}_p$ such that $E = \mathrm{Graph}(f)$ with respect to some choice of coordinate axis decomposition for $\mathbb{F}_p^2$. Note the function f can always be given by a polynomial of degree at most $p - 1$.*

A similar argument yields a characterization of k-tilings for $\mathbb{F}_p^2$ when p is a prime.

THEOREM 1.8 (classification of k-tilings of the plane $\mathbb{F}_p^2$). *Let $q = p$, a prime and suppose that E k-tiles $\mathbb{F}_p^2$. Then either $|E| = k$ and $A = \mathbb{F}_p^2$, $E = \mathbb{F}_p^2$ and $|A| = k$, or $|E| = sp$ for some $1 \le s \le p - 1$ such that s divides k and E is the union of s disjoint graphs* $\mathrm{Graph}(f_1), \ldots, \mathrm{Graph}(f_s)$.

Theorem 1.7 gives much more structural information about tiling sets than the simple divisibility condition on their order, i.e., $|E| = 1$, p or p^2 in the case when $|E| = p$. This is because most sets of size p are not graphs as the next example explains.

EXAMPLE 1.9. We give an example of p points in $\mathbb{F}_p^2$ which cannot be expressed as $\mathrm{Graph}(f)$ for any f or equivalently do not equidistribute on any collection of p parallel lines. To construct an example of p points that do not equidistribute on p parallel lines in any direction, it is necessary and sufficient to construct collection of points whose pairwise differences generate all possible directions. This is sometimes referred to as the "vertical line test" (in every direction). Note there are $p + 1$ directions in $\mathbb{F}_p^2$ which can be encoded by the slopes of the corresponding lines $\{0, 1, \ldots, p - 1, \infty\}$.

For $p = 5$ a collection of 5 points in $\mathbb{F}_5^2$ which do not equidistribute in any direction is given by

$$\big\{(0,0),\, (1,1),\, (2,3),\, (3,1),\, (2,4)\big\}$$

since their pairwise differences generate every possible slope (direction) as the reader can easily check.

Note in general, the number of directions in $\mathbb{F}_p^2$ is $p+1$ while a set of p points has $\binom{p}{2} = \Theta(p^2)$ pairs of distinct points so one expects this last example to be "generic" amongst subsets of size p in $\mathbb{F}_p^2$, i.e., that most subsets of size p determine all directions and hence are not graphs. Indeed there are $\binom{p^2}{p} = \frac{p^2(p^2-1)\cdots(p^2-p+1)}{p!}$ sets of size p in $\mathbb{F}_p^2$ while at most $(p+1)p^p$ of these are graphs (choose a direction and then one point per hyperplane in the family of hyperplanes perpendicular to that direction). One can compute

$$\frac{\binom{p^2}{p}}{(p+1)p^p} = \frac{p(p-\frac{1}{p})(p-\frac{2}{p})\cdots(p-\frac{p-1}{p})}{(p+1)!} \geq \frac{(p-1)^p}{(p+1)!} \to \infty \quad \text{as } p \to \infty.$$

The proof of Theorem 1.7 carries over to 3-dimensions as long as we weaken the conclusion slightly by showing that either E or A is a graph and hence the tiling is graphical.

THEOREM 1.10 (classification of 1-tilings in 3-space). *Let $q = p$ a prime and suppose E 1-tiles $\mathbb{F}_p^3$ by A. Then (E, A) is a graphical tiling i.e., either E or A is a graph. More generally, if (E, A) is a tiling pair in $\mathbb{F}_p^d$ with $|E| = p$ or p^{d-1} then the tiling is graphical.*

In higher dimensions, the results of Theorems 1.7 and 1.10 seemingly fail, i.e., not every tiling pair is graphical at least over cyclic groups of non-prime order. For example in [9], a tiling of $\mathbb{Z}_6^5 \times \mathbb{Z}_{15}$ which is not spectral is constructed. Such a tiling cannot be graphical as all graphs are spectral sets. However it is not clear exactly in which dimension the graphical structure of tilings breaks down if we consider only vector spaces over prime fields $\mathbb{Z}_p$. The first possibility not covered by our methods of a non-graphical tiling would be $(E, A) \subseteq \mathbb{F}_p^4$ with $|E| = |A| = p^2$ but we have not found any such explicit example.

1.2. A polynomial approach to multi-tiling over finite fields. An alternate approach to the main problem may be taken by associating polynomials (in d variables) to the sets A and E. We begin by associating to each point $m \in \mathbb{F}_q^d$ the monomial $z^m := z_1^{m_1} \cdots z_d^{m_d}$. We notice that if we form the multivariate polynomial that encodes all of the information about the set E by forming $\sum_{e \in E} z^e$, and then we translate the set E by any element $a \in A$, this encoding corresponds to the multiplication $z^a \sum_{e \in E} z^e$. But in order to respect the additive structure of the abelian group $(\mathbb{Z}/q\mathbb{Z})^d$ inside the exponents of these monomials, we will need to work in the ring

$$(\mathbb{Z}/q\mathbb{Z})[z_1, \ldots, z_d] \,/\, \big((z_1^q - 1), \ldots, (z_d^q - 1)\big).$$

Note that when $q = p^\ell$, p a prime, the finite field $\mathbb{F}_q$ has additive group isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\ell$ so when applying results in this section to fields, $q = p$ a prime should be assumed.

For example, for $d=2$, $q=7$, we have $z_1^4 z_2^5 = z_1^{11} z_2^5 \bmod ((z_1^7-1),(z_2^7-1))$. We note that although we could work with $\mathbb{F}_q[z_1,\dots,z_d]$ and its relevant quotients, we are here simply ignoring the multiplicative structure of the field and focusing on its additive structure. To simplify notation, we define the ideal

$$\mathcal{I} := \big((z_1^q-1),\dots,(z_d^q-1)\big)$$

in our ring $(\mathbb{Z}/q\mathbb{Z})[z_1,\dots,z_d]$ and work with multivariate polynomials mod $\mathcal{I}$. We note that when we write $\frac{z_1^q-1}{z_1-1}$, we mean the polynomial

$$1+z_1+z_1^2+\cdots+z_1^{q-1},$$

so there are no rational functions here and hence we do not need to worry about singularities. Another advantage of this polynomial approach is that we may differentiate as many times as we like with respect to each variable, obtaining many moment identities for each d and q.

THEOREM 1.11. *A set $E \subset \mathbb{F}_q^d$ multi-tiles by a set of translation vectors $A \subset \mathbb{F}_q^d$, at level $k \geq 1$, if and only if*

$$\Big(\sum_{e\in E} z^e\Big)\Big(\sum_{a\in A} z^a\Big) = k\prod_{i=1}^{d}\frac{z_i^q-1}{z_i-1} \mod \mathcal{I}. \tag{1.2}$$

We note that the Fourier result follows immediately from Theorem (1.11) by specializing all of the coordinates of $z \in \mathbb{C}^d$ to be roots of unity

$$z_j := e^{2\pi i k_j/q},$$

and in this case all elements of the ideal $\mathcal{I}$ vanish identically, considering everything over $\mathbb{C}$ now. Furthermore, letting each $z_j = 1$ in Theorem (1.11) retrieves the arithmetic constraint of Theorem 1.2, namely that $|A||E| = kq^d$.

With the same notation of tiling at level k, we have the following consequence of the polynomial identity given by Theorem 1.11, using differentiation.

COROLLARY 1.12.

$$|A|\Big(\sum_{e\in E} e\Big) + |E|\Big(\sum_{a\in A} a\Big) = 0 \quad \textit{in } (\mathbb{Z}/q\mathbb{Z})^d. \tag{1.3}$$

We may also obtain higher moment identities by further differentiation of the identity of Theorem 1.11, and here is the next such moment identity.

COROLLARY 1.13.

$$\Big(\sum_{e\in E} e_j^2\Big)|A| + \Big(\sum_{a\in A} a_j^2\Big)|E| + 2\Big(\sum_{e\in E} e_j\Big)\Big(\sum_{a\in A} a_j\Big) = 0 \mod q, \tag{1.4}$$

for each $1 \le j \le d$.

We note that higher moment formulas continue to exist, using similar methods, albeit they get more messy. We've given here an analogue of the 'mean' and of the 'second moment' for any finite tiling sets E and A.

1.3. Packings. When tiling or multi-tiling is not possible, we can still ask for the largest proportion of $\mathbb{F}_q^d$ that various disjoint translates of $E \subset \mathbb{F}_q^d$ can cover.

DEFINITION 1.14. We say that E packs $\mathbb{F}_q^d$ by A if $A \subset \mathbb{F}_q^d$ with the property that

$$(E + a) \cap (E + a') = \emptyset \quad \text{for all } a \neq a',\ a, a' \in A.$$

DEFINITION 1.15. We say that A is an optimal packing set for E if A is a set of largest possible size such that E packs $\mathbb{F}_q^d$ by A.

DEFINITION 1.16. The density of packing of $E \subset \mathbb{F}_q^d$ by $A \subset \mathbb{F}_q^d$ is the ratio $\frac{|E||A|}{q^d}$.

We start out with a very negative result.

THEOREM 1.17. *Let* $E = S_t = \{x \in \mathbb{F}_q^d : \|x\| = t\}$, *where* $\|x\| = x_1^2 + \cdots + x_d^2$. *If* $d \ge 4$ *and* $t \neq 0$, *then the optimal packing of* S_t *has size* 1.

For proof, see [8, Lemma 8.1]. In particular, this means that the sphere packing problem is only interesting in dimensions two and three.

We now specialize to the two-dimensional case.

DEFINITION 1.18. A circle of "radius" R and center $(u, v) \in \mathbb{F}_q^2$ is the affine variety given by

$$\begin{aligned} C_R((u,v)) &= \big\{(x,y) \in \mathbb{F}_q^2 : (x-u)^2 + (y-v)^2 = R\big\} \\ &= \big\{(x,y) \in \mathbb{F}_q^2 : \|(x,y) - (u,v)\| = R\big\}. \end{aligned}$$

Note that this notion of radius is the square of the usual one but is more suitable for work in general fields. The packing number $P(q, c)$ is defined as the maximum number of pairwise disjoint circles of radius c that you can fit into the plane $\mathbb{F}_q^2$. Scaling by $M \neq 0$ shows that $P(q, M^2c) = P(q, c)$. We will often abbreviate $P(q, 1) = P(q)$ when referring to the packing number of unit circles.

In [2], the following lemma about completing line segments into triangles in the plane was proven. It will be very useful in our study of circle packings:

LEMMA 1.19. *Fix a field $\mathbb{F}$ of characteristic not equal to two and let P be the plane $\mathbb{F}^2$. Let (x_1, x_2) be a line segment of length $\|x_1 - x_2\| = (x_1 - x_2) \cdot (x_1 - x_2) = \ell_1 \neq 0$ in the plane P. This segment can be extended into exactly μ triangles (x_1, x_2, x_3) with $\|x_2 - x_3\| = \ell_2$ and $\|x_3 - x_1\| = \ell_3$ given, where*

$$\mu = \begin{cases} 2 & \text{if } 4\sigma_2 - \sigma_1^2 \text{ is a nonzero square in } \mathbb{F}, \\ 1 & \text{if } 4\sigma_2 - \sigma_1^2 \text{ is zero}, \\ 0 & \text{if } 4\sigma_2 - \sigma_1^2 \text{ is a nonsquare in } \mathbb{F}, \end{cases}$$

and $\sigma_1 = \ell_1 + \ell_2 + \ell_3$, $\sigma_2 = \ell_1\ell_2 + \ell_2\ell_3 + \ell_3\ell_1$.

This lemma immediately leads to a criterion for when two circles intersect in the plane:

COROLLARY 1.20. *Let C_1 be a circle of radius ℓ_1 and C_2 be a circle of radius ℓ_2 and let $\ell_3 = \|x_1 - x_2\| \neq 0$ be the distance between their centers x_1 and x_2. Then C_1 and C_2 intersect in μ points, where*

$$\mu = \begin{cases} 2 & \text{if } 4\sigma_2 - \sigma_1^2 \text{ is a nonzero square in } \mathbb{F}, \\ 1 & \text{if } 4\sigma_2 - \sigma_1^2 \text{ is zero}, \\ 0 & \text{if } 4\sigma_2 - \sigma_1^2 \text{ is a nonsquare in } \mathbb{F}, \end{cases}$$

and $\sigma_1 = \ell_1 + \ell_2 + \ell_3$, $\sigma_2 = \ell_1\ell_2 + \ell_2\ell_3 + \ell_3\ell_1$. When $\ell_1 = \ell_2 = c$ and $\ell_3 = R \neq 0$ we find two circles of radius c and distance R between their centers intersect in μ points, where

$$\mu = \begin{cases} 2 & \text{if } R(4c - R) \text{ is a nonzero square in } \mathbb{F}, \\ 1 & \text{if } R(4c - R) \text{ is zero i.e., } R = 4c, \\ 0 & \text{if } R(4c - R) \text{ is a nonsquare in } \mathbb{F}. \end{cases}$$

The proof is very simple, so we give it here. The first part is clear and the second follows from the following computation. Setting $\ell_1 = \ell_2 = c$ and $\ell_3 = R \neq 0$ yields $\sigma_1 = 2c + R$ and $\sigma_2 = 2cR + c^2$. Thus

$$4\sigma_2 - \sigma_1^2 = 4(2cR + c^2) - (2c + R)^2 = 4cR - R^2 = R(4c - R).$$

EXAMPLE 1.21 (packing of circles in $\mathbb{F}_3^2$). The function $f\colon \mathbb{F}_3 \to \mathbb{F}_3$ given by $f(R) = R(4 - R) = R(1 - R)$ takes only the values $\{0, 1\}$ and so is always a square. Thus any two unit circles in the plane $P = \mathbb{F}_3^2$ intersect. Thus the unit packing number $P(3) = P(3, 1)$ is equal to 1 as you can pack at most 1 unit circle into the plane $\mathbb{F}_3^2$. The function $g : \mathbb{F}_3 \to \mathbb{F}_3$ given by $g(R) = R(4(2) - R) = R(-1 - R)$ takes only the values $\{0, 1\}$ also so $P(3, 2) = 1$ also.

Using the same results, we get a criterion for the existence of three disjoint circles of radius c in the plane:

PROPOSITION 1.22. *There is a packing of three disjoint circles of radius c in $\mathbb{F}_q^2$ whose centers make a triangle with nonzero sidelengths ℓ_1, ℓ_2, ℓ_3 if and only if*

$$\ell_1(4c-\ell_1), \quad \ell_2(4c-\ell_2), \quad \ell_3(4c-\ell_3)$$

are non squares in $\mathbb{F}_q$ and $4\sigma_2-\sigma_1^2$ is a square where $\sigma_2=\ell_1\ell_2+\ell_2\ell_3+\ell_3\ell_1$, $\sigma_1=\ell_1+\ell_2+\ell_3$.

Once again, the proof is straightforward. It follows from the previously mentioned results since such a packing exists in $\mathbb{F}_q^2$ if and only if the triangle made by the centers exists in $\mathbb{F}_q^2$ and the circles of radius c centered at the vertices of the triangle are pairwise disjoint.

This generalizes immediately using the same argument, to a brute force algorithm to determine whether one can pack k disjoint circles of radius c in a finite plane:

THEOREM 1.23 (Primitive Circle Packing Algorithm). *Fix a finite field $\mathbb{F}_q$ of odd characteristic and nonzero $c\in\mathbb{F}_q$. Let $f\colon \mathbb{F}_q\to\mathbb{F}_q$ be given by $f(R)=R(4c-R)$ and let $S=\{R\in\mathbb{F}_q \mid f(R) \text{ is not a square in } \mathbb{F}_q\}$. Note $0\notin S$. Then it is possible to pack k distinct circles of radius c in the plane $P=\mathbb{F}_q^2$ (with nonzero distance between centers) if and only if it is possible to find k distinct vertices in P that form a $(k-1)$-simplex whose edge lengths all lie in S. In the case this holds, the packing is achieved by placing the k-circles at the vertices of the $(k-1)$-simplex.*

REMARK 1.24. Note here and in the paragraphs to follow that the simplexes in question are necessarily degenerate when $k\geq 4$.

Note when $q=1 \bmod 4$, it is possible to have zero distance between centers of distinct circles and this must be excluded in the theorem. The theorem is a complete characterization of packing only when $q=3 \bmod 4$.

When searching for such a $(k-1)$ simplex as mentioned in the algorithm, one can assume the first vertex is the origin and hence consider only the $O((q^2)^{k-1})$ possible $(k-1)$ simplices pinned at the origin. For each of these, a calculation of $\binom{k}{2}$ distances will determine the edge lengths of this simplex and determine if it will work or not. Thus a brute force search will essentially use at most $O(k^2q^{2k-2})$ basic steps to determine if a k-packing of circles of radius c exists in the plane $P=\mathbb{F}_q^2$ or not, and if it does exist, will produce such a packing. This is a polynomial time algorithm for any fixed k. However as the only a priori upper bound on $P(q,c)$ is $\frac{q^2}{q-1}=O(q)$ as the size of a circle is at least $q-1$, using this algorithm to determine $P(q,c)$ is not feasible as it would have to check $1\leq k\leq q$ cases leading to $O(q^2q^{2q-2})=O(q^{2q})$ efficiency which is not feasible.

When the distance between the distinct circles in the packing is allowed to be zero, in fact larger packings can be achieved. This can be done only when $q = 1 \mod 4$. In this case there is a primitive 4th root of unity i in $\mathbb{F}_q$ and the two lines $\{(t, it) \mid t \in \mathbb{F}_q\}$ and $\{(t, -it) \mid t \in \mathbb{F}_q\}$ are isotropic ($\|v\| = 0$ for v on these lines) and together form the circle of radius zero about the origin. It turns out for any nonzero c, the q circles of radius c centered on the points of an isotropic line are all disjoint and hence form a "degenerate" isotropic packing of nearly optimal size.

THEOREM 1.25 (isotropic circle packing). *Let $q = 1 \mod 4$ and let $P = \mathbb{F}_q^2$ be the affine plane over $\mathbb{F}_q$. If i is a primitive 4th root of unity in $\mathbb{F}_q$ then the lines $\{(t, it) \mid t \in \mathbb{F}_q\}$ and $\{(t, -it) \mid t \in \mathbb{F}_q\}$ are the two isotropic lines in this plane. For any $c \neq 0$, we have*

$$q \leq P(q, c) \leq q + 1.$$

A packing of q circles of radius c can be achieved by taking the q circles of radius c centered at the q points on an isotropic line. The complement of this packing is nothing other than the isotropic line itself.

Note the isotropic packing of the last theorem is maximal as one can show that the complementary isotropic line cannot contain any circle of nonzero radius. However this does not necessary preclude the existence of a completely different maximum circle packing achieving $P(q, c) = q + 1$.

1.4. Algebraic tilings. In this section we discuss the algebraic 1-tilings of affine spaces over algebraically closed fields. We also explore the connections between some of these results and the well-known Jacobian conjectures (see e.g. [4]).

DEFINITION 1.26. Let k be a field and $\mathbb{A}^d$ denote d-dimensional affine space over k. By a regular automorphism of $\mathbb{A}^d$ we mean a bijective function $F\colon \mathbb{A}^d \to \mathbb{A}^d$ such that both F and F^{-1} have polynomial coordinate functions.

The study of regular automorphisms of affine space has a long history, and a useful criterion in determining whether a polynomial function $F\colon \mathbb{A}^d \to \mathbb{A}^d$ has a polynomial inverse is given conjecturally (over algebraically closed fields) via the famous Jacobian conjecture.

To state this conjecture, notice if F^{-1} exists and is polynomial then both Jacobian matrices DF and DF^{-1} have polynomial entries, and taking determinants we see that $JF \cdot JF^{-1} = 1$ where JF and JF^{-1} are polynomials. Hence JF has to be a nonzero constant as the only units in a polynomial ring are nonzero constants. The Jacobian conjecture is that this necessary condition is also sufficient:

CONJECTURE 1.27 (Jacobian conjecture). *Let k be an algebraically closed field and $\mathbb{A}^d$ be d-dimensional affine space over k. A polynomial function $F\colon \mathbb{A}^d \to \mathbb{A}^d$ has a polynomial inverse if and only if the Jacobian determinant JF is a nonzero constant (that is, $JF \in k^*$).*

The Jacobian conjecture reduces to the case over $\mathbb{C}$ in characteristic zero but is still open in all dimensions $d \geq 2$.

DEFINITION 1.28. An algebraic set is a subset of $\mathbb{A}^d$, which is a common zero set of a finite collection of polynomials.

DEFINITION 1.29. Fix a field k. Let X and Y be algebraic sets in d-dimensional affine space $\mathbb{A}^d_k$. Then (X, Y) is an *algebraic* 1*-tiling* if the map $\theta\colon X \times Y \to \mathbb{A}^d_k$ given by $\theta(x, y) = x + y$ is an isomorphism of algebraic sets.

THEOREM 1.30. *Let k be an algebraically closed field, and suppose (X, Y) algebraically 1-tiles $\mathbb{A}^d_k$. Then $\dim X + \dim Y = d$.*

PROOF. By definition, the map

$$\theta\colon X \times_k Y \to \mathbb{A}^d_k \quad \text{via} \quad (x, y) \mapsto x + y$$

is an isomorphism. Denote by $k[X]$ and $k[Y]$ the coordinate rings of X and Y, respectively. By Noether's normalization lemma, there exist algebraically independent elements $x_1, \ldots, x_i \in k[X]$ and $y_1, \ldots, y_j \in k[Y]$ such that $k[X]$ and $k[Y]$ are finitely generated modules over the polynomial rings $k[x_1, \ldots, x_i]$ and $k[y_1, \ldots, y_j]$, respectively. Thus $k[X] \otimes k[Y] = k[\mathbb{A}^d]$ is a finitely generated module over

$$k[x_1, \ldots, x_i] \otimes k[y_1, \ldots, y_j] = k[x_1, \ldots, x_i, y_1, \ldots, y_j].$$

Comparing Krull dimensions we find $i + j = d$ as claimed. □

In the graphical classification of tilings over finite fields (e.g. Theorem 1.7), either X or Y is isomorphic to a linear subspace of $\mathbb{A}^2$. While this may not occur for general $\mathbb{A}^d$, we expect considerable restrictions on what type of X and Y may occur since the algebraic sets X and Y must behave well under the ambient vector addition in $\mathbb{A}^d$. For instance, it may be the case that the coordinate rings $k[X]$ and $k[Y]$ are isomorphic to polynomial rings, say $k[X] \cong k[f_1, \ldots, f_i]$ and $k[Y] \cong k[g_1, \ldots, g_j]$; that is, X and Y are isomorphic to affine spaces $\mathbb{A}^i$ and $\mathbb{A}^j$, respectively. If we express the generators f_s and g_t as polynomials in the coordinates $z_1, \ldots z_d$ of $\mathbb{A}^d$, then the function

$$F(z_1, \ldots, z_d)$$

$$= \big(f_1(z_1, \ldots, z_d), \ldots, f_i(z_1, \ldots, z_d), g_1(z_1, \ldots, z_d), \ldots, g_j(z_1, \ldots, z_d)\big)$$

is a polynomial function $F\colon \mathbb{A}^d \to \mathbb{A}^d$ which is an isomorphism by construction. Thus it is a regular automorphism of $\mathbb{A}^d$. Note that F takes X in the original coordinate system to the set $\{(f_1, \dots, f_i, 0, \dots, 0)\}$ and Y to $\{(0, \dots 0, g_1, \dots, g_j)\}$ in the new coordinate system, which is analogous to the classification in Theorem 1.7.

2. Proofs of Theorems 1.7, 1.8 and 1.10: tiling characterization in $\mathbb{F}_p^2$ and $\mathbb{F}_p^3$

In this section, p is a prime.

LEMMA 2.1. *Suppose that E k-tiles $\mathbb{F}_p^d$ by A. Then $\widehat{E}(m)$ is nonzero for all m if and only if $|E| = k$ and $A = \mathbb{F}_p^d$. Furthermore $1 \le k \le p^d$.*

PROOF. To see this, observe that since $\widehat{E}(m)\widehat{A}(m) = 0$ for all nonzero m and $\widehat{E}(m)$ is assumed nonzero, we conclude $\widehat{A}(m) = 0$ for all $m \neq \vec{0}$. Since $A(x) = \sum_{m \in \mathbb{F}_p^d} \chi(x \cdot m)\widehat{A}(m)$, we conclude that A is a constant function and hence that A must be the whole space since A cannot be the empty set. This forces E to consist of k distinct points since E k-tiles $\mathbb{F}_p^d$ by A. Since $E \subset \mathbb{F}_p^d$, we also conclude that $1 \le k \le p^d$. $\square$

PROPOSITION 2.2. *Let E be a subset of $\mathbb{F}_p^d$ and m a fixed nonzero vector of $\mathbb{F}_p^d$. Then the following are equivalent*:

(1) $\widehat{E}(m) = 0$.

(2) *E is equidistributed on the hyperplanes H_0, H_1, …, H_{p-1} where*

$$H_j = \{x : x \cdot m = j\}.$$

(3) $\widehat{E}(rm) = 0$ *for all* $r \in \mathbb{F}_p^*$.

PROOF. Suppose that (1) holds. Then $0 = \widehat{E}(m) = \frac{1}{p^d} \sum_{x \in E} \chi(-m \cdot x)$ where χ is a nontrivial additive character of $\mathbb{F}_p$. We may assume $\chi(-t) = \xi^t$ where ξ is a primitive pth root of unity.

Then we have $0 = \sum_{k=0}^{p-1} a_k \xi^k$ where a_k is the number of elements of E on the hyperplane H_k. This implies ξ is a zero of the polynomial $a_0 + a_1 x + a_2 x^2 + \cdots + a_{p-1}x^{p-1}$ with rational coefficients a_j. However it is well known the minimal polynomial (over $\mathbb{Q}$) of ξ is $1 + x + x + \cdots + x^{p-1} = \frac{x^p - 1}{x - 1}$ which is irreducible by Eisenstein's criterion. Thus $a_0 + a_1 x + a_2 x^2 + \cdots a_{p-1}x^{p-1}$ is a $\mathbb{Q}$-multiple of $1 + x + x^2 + \cdots + x^{p-1}$ and so $a_0 = a_1 = a_2 = \cdots = a_{p-1}$. In other words, E is equidistributed over the hyperplanes H_0, …, H_{p-1}. Thus (2) holds. As all the steps in the argument are reversible (1) and (2) are equivalent.

Finally noting that replacing m with rm, r a nonzero scalar, does not change the corresponding set of hyperplanes, we see that (2) and (3) are equivalent. □

Note that this last proposition is not true for Fourier transforms of general complex valued functions over prime fields. Indeed one can create a complex function with any prescribed set of zeros on the Fourier space side and then use the inverse Fourier transform to get an example of a complex function where the equivalences of Proposition 2.2 don't hold. However it is true for rational-valued functions such as characteristic functions, as the interested reader can check.

Proof of Theorem 1.7. Note that $|E||A| = p^2$, so $|E| = 1$, p or p^2. If $|E| = 1$ then E is a point and we are done. If $|E| = p^2$ then E is the whole plane and we are done, so without loss of generality $|E| = p$.

If $\widehat{E}(m)$ never vanishes then by Lemma 2.1, E is a point and we are done. On the other hand if $\widehat{E}(m) = 0$ for some nonzero m, then it vanishes on L, the line passing through the origin and $m \neq \vec{0}$. Thus if we set $L^\perp$ to be the line through the origin, perpendicular to m, we see that

$$\widehat{L^\perp}(s)\,\widehat{E}(s) = 0$$

for all nonzero s. This is because by (1.1) $\widehat{L^\perp}(s) = q^{-(d-1)}L(s)$. Since $|L^\perp| = p = |E|$ we then see that E 1-tiles $\mathbb{F}_p^2$ by $L^\perp$.

Since $\widehat{E}(m) = 0$ we see that E is equidistributed on the set of p lines $H_t = \{x \mid x \cdot m = t\}, t \in \mathbb{F}_p$. Since $|E| = p$ this means there is exactly one point of E on each of these lines.

We will now choose a coordinate system in which E will be represented as a graph of a function. The coordinate system will either be an orthogonal system or an isotropic system depending on the nature of the vector m.

Case 1: $m \cdot m \neq 0$. We may set $e_1 = m$ and e_2 a vector orthogonal to m. $\{e_1, e_2\}$ is an orthogonal basis because e_2 does not lie on the line throough m as this line is not isotropic. If we take a general vector $\widehat{x} = x_1e_1 + x_2e_2$ we see that $\widehat{x} \cdot m = x_1(m \cdot m)$ and so the lines H_t, $t \in \mathbb{F}_p$ are the same as the lines of constant x_1 coordinate with respect to this orthogonal basis $\{e_1, e_2\}$. Thus there is a unique value of x_2 for any given value of x_1 so that $x_1e_1 + x_2e_2 \in E$. Thus $E = \{x_1e_1 + f(x_1)e_2 : x_1 \in \mathbb{F}_p\} = \mathrm{Graph}(f)$ for some function $f\colon \mathbb{F}_p \to \mathbb{F}_p$.

Case 2: $m \cdot m = 0$. We may set $e_1 = m$. In this case any vector orthogonal to e_1 lies on the line generated by e_1 and so cannot be part of a basis with e_1. Instead we select e_2 off the line generated by e_1 and scale it so that $e_1 \cdot e_2 = 1$. Then by subtracting a suitable multiple of e_1 from e_2 one can also ensure $e_2 \cdot e_2 = 0$. Thus $\{e_1, e_2\}$ is a basis consisting of two linearly in-

dependent isotropic vectors. With respect to this basis, the dot product is represented by the matrix

$$\mathbb{A} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

which exhibits the plane as the hyperbolic plane. This case can only occur when $p = 1 \bmod 4$. Note when we express a general vector $\widehat{x} = x_1 e_1 + x_2 e_2$ with respect to this basis we have $\widehat{x} \cdot m = x_2$ thus the lines $\{H_t : t \in \mathbb{F}_p\}$ are the same as the lines of constant x_2 coordinate with respect to this basis and E has a unique point on each of these lines. Thus $E = \{f(x_2)e_1 + x_2 e_2 : x_2 \in \mathbb{F}_p\} = \text{Graph}(f)$ is a graph with respect to this isotropic coordinate system.

Finally we note any function $f : \mathbb{F}_p \to \mathbb{F}_p$ is given by a polynomial of degree at most $p-1$, explicitly expressed in the form

$$f(x) = \sum_{k \in \mathbb{F}_p} f(k) \frac{\Pi_{j \neq k}(x - j)}{\Pi_{j \neq k}(k - j)}$$

expresses f as such a polynomial in x. □

Proof of Theorem 1.8. If $\widehat{E}(m)$ never vanishes then by Lemma 2.1 we are done so we may assume $\widehat{E}(m) = 0$ for some nonzero m. Then E vanishes on the nonzero elements of the line L through m and the origin. By proposition 2.2, E is equidistributed on the p lines parallel to $L^\perp$ with s elements per line. Note $1 \leq s \leq p-1$ as if $s = p$ then E is the whole plane which was already covered. Then $|E| = ps$ and we can partition E into s sets $E_1, \ldots, E_s$ each with exactly one element on each of the lines parallel to $L^\perp$.

As we argued above, this means $E_j = \text{Graph}(f_j)$ of some function $f_j : \mathbb{F}_p \to \mathbb{F}_p$ once we take coordinates x parallel to L and y parallel to $L^\perp$. Since $|E||A| = kp^2$ we have $sp|A| = kp^2$ and so $|A| = \frac{kp}{s}$ so s must divide kp. Since $s \leq p-1$, s is relatively prime to p and so s divides k. This completes the proof of Theorem 1.8. □

Proof of Theorem 1.10. We proceed as in the proof of Theorem 1.7. Let (E, A) be a tiling pair in $\mathbb{F}_p^d$ As $|E||A| = p^d$ then $|E| = p^{d-1}$ implies $|A| = p$ so at least one of $|E|, |A|$ is p. Without loss of generality we will assume $|E| = p$ as the argument when $|A| = p$ is similar with the roles of E and A swapped.

We know that $\widehat{E}(m)\widehat{A}(m) = 0$ for all nonzero m. If $\widehat{A}(m) = 0$ for all nonzero m then Fourier inversion shows that the characteristic function of A is a constant and hence that A is the whole space and $|E| = 1$ which contradicts our assumptions. Thus $\widehat{A}(m)$ is nonzero for some nonzero m and hence $\widehat{E}(m) = 0$ for some nonzero m. Thus E equidistributes on the p

hyperplanes perpendicular to m. Let $H = H_m$ be the hyperplane through the origin perpendicular to m and let L be a line such that $H \oplus L = \mathbb{F}_p^d$. Let $\{e_1, \dots, e_d\}$ be a basis such that e_1 lies in L and $\{e_2, \dots, e_d\}$ lie in H. Now E equdistributes on the p hyperplanes of constant e_1-coordinate and so has exactly one element per hyperplane as $|E| = p$. Thus there is a function $f = (f_2, \dots, f_d) \colon \mathbb{F}_p \to \mathbb{F}_p^{d-1}$ such that $E = \{x_1 e_1 + f_2(x_1)e_2 + \cdots + f_d(x_1)e_d \mid x_1 \in \mathbb{F}_p\} = \mathrm{Graph}(f)$ and so the tiling (E, A) is graphical as claimed.

Now in 3 dimensions, $d = 3$ and if (E, A) is a tiling pair then $|E| = 1$, p, p^2, p^3. The cases $|E| = 1$, p^3 are trivial and trivially graphical while the cases $|E| = p$, p^2 fall under the last argument. $\square$

3. Proof of Theorem 1.25: isotropic circle packings in the plane

Once we show that the q circles of radius $c \neq 0$ centered at the q points on an isotropic line $L \subseteq P$ are disjoint, we will have shown $q \leq P(q, c)$. Note that q circles would account for $q(q-1) = q^2 - q$ points as circles of nonzero radius have size $q - 1$ when $q = 1 \bmod 4$. Thus only q unused points remain allowing for at most one more circle to be packed. Thus $P(q, c) \leq q + 1$.

So it remains only to show the disjointness of two different c-circles centered on an isotropic line. Consider (u, v) and (s, t) two distinct elements on an isotropic line L. A point of intersection (x, y) of the circles of radius $c \neq 0$ about (u, v) and (s, t) must satisfy the two equations

$$(x-u)^2 + (y-v)^2 = c, \quad (x-s)^2 + (y-t)^2 = c$$

As L is isotropic we have $u^2 + v^2 = s^2 + t^2 = 0$ so expanding the two equations and subtracting we get $-2x(u-s) - 2y(v-t) = 0$ i.e.,

$$(x, y) \cdot (u - s, v - t) = 0.$$

As $(u - s, v - t)$ is a nonzero element of the isotropic line L which is its own perp, we conclude that $(x, y) \in L$ and so $x^2 + y^2 = 0$ and $(x, y) \cdot (u, v) = 0$. Plugging these into the first equation of the two above, we find $0 = c$ which gives a contradiction. Thus the two circles of radius c centered at different points of the isotropic line must be disjoint. This completes the proof of the theorem. $\square$

Note that any point on the isotropic line L has distance zero from any other point on the line L and hence does not lie on any circle of radius $c \neq 0$ centered on the line. Thus L lies in the complement of the union of the circles in this packing. As $|L| = q = q^2 - q(q-1)$ we conclude that L is the complement of this packing.

4. Polynomial method results

PROOF OF THEOREM 1.11. Translating the set E by all elements of the set A corresponds to the product of polynomials

$$\Big(\sum_{e\in E} z^e\Big)\Big(\sum_{a\in A} z^a\Big) \mod \mathcal{I}.$$

On the other hand, this corresponds to multi-tiling at level k if and only if the latter product equals $k\sum_{f\in\mathbb{F}_q^d} z^f$, which is the required identity. □

PROOF OF COROLLARY 1.12. Fixing an index j and focusing on the variable z_j, we differentiate both sides of (1.11) with respect to z_j, and then multiply by z_j (i.e. we apply the differential operator $z_j\frac{\partial}{\partial z_j}$), obtaining:

$$\begin{aligned}(4.1)\qquad &\Big(\sum_{e\in E} e_j z^e\Big)\Big(\sum_{a\in A} z^a\Big)+\Big(\sum_{e\in E} z^e\Big)\Big(\sum_{a\in A} a_j z^a\Big)\\ &\quad= k\frac{\partial}{\partial z_j}\Big(\frac{z_1^q-1}{z_1-1}\frac{z_2^q-1}{z_2-1}\cdots\frac{z_d^q-1}{z_d-1}\Big)\\ &= k\,\frac{z_1^q-1}{z_1-1}\,\frac{z_2^q-1}{z_2-1}\cdots\Big(z_j+2z_j^2+3z_j^3+\cdots+(q-1)z_j^{q-1}\Big)\cdots\frac{z_d^q-1}{z_d-1}.\end{aligned}$$

We now let all $z_j=1$, obtaining

$$(4.2)\qquad \Big(\sum_{e\in E} e_j\Big)|A|+\Big(\sum_{a\in A} a_j\Big)|E| = kq^{d-1}\,\frac{(q-1)q}{2} \mod q = 0 \mod q.$$

Putting together all d of these identities (one for each index j) into vector form, we obtain the desired result. □

PROOF OF COROLLARY 1.13. We may now continue to differentiate equation (4.1), applying to it the operator $z_j\frac{\partial}{\partial z_j}$ once again.

$$\begin{aligned}(4.3)\qquad &\Big(\sum_{e\in E} e_j^2 z^e\Big)\Big(\sum_{a\in A} z^a\Big)+2\Big(\sum_{e\in E} e_j z^e\Big)\Big(\sum_{a\in A} a_j z^a\Big)+\Big(\sum_{e\in E} z^e\Big)\Big(\sum_{a\in A} a_j^2 z^a\Big)\\ &= k\,\frac{z_1^q-1}{z_1-1}\,\frac{z_2^q-1}{z_2-1}\cdots\Big(z_j+2^2z_j^2+3^2z_j^3+\cdots+(q-1)^2z_j^{q-1}\Big)\cdots\frac{z_d^q-1}{z_d-1}.\end{aligned}$$

Again specializing to all $z_j = 1$, we obtain

$$\Big(\sum_{e\in E} e_j^2\Big)|A| + \Big(\sum_{a\in A} a_j^2\Big)|E| + 2\Big(\sum_{e\in E} e_j\Big)\Big(\sum_{a\in A} a_j\Big)$$
$$= k\,q^{d-1}\big(1 + 2^2 + 3^2 + \cdots + (q-1)^2\big) \mod q$$
$$= 0 \mod q. \quad \square$$

We note that we may continue to get arbitrarily many identities by differentiating arbitrarily many times with respect to each z_j.

References

[1] A. Alexandrov, *Convex Polyhedra* (translated from the 1950 Russian edition by N. S. Dairbekov, S. S. Kutateladze and A. B. Sossinsky, with comments and bibliography by V. A. Zalgaller and appendices by L. A. Shor and Yu. A. Volkov), Springer Monographs in Mathematics, Springer-Verlag (Berlin, 2005).

[2] M. Bennett, A. Iosevich and J. Pakianathan, Three point configurations in two-dimensional vector spaces over finite fields via the Elekes–Sharir paradigm, *Combinatorica*, **34** (2014) (to appear).

[3] P. Erdős and C. Rogers, Covering space with convex bodies, *Acta Arith.*, **7** (1961), 281–285.

[4] A. Fernandes, C. Maquera and J. Venato-Santos, Jacobian conjecture and semi-algebraic maps, *Math. Proc. Cambridge Philos. Soc.*, **157** (2014), 221–229.

[5] B. Gordon, Multiple tilings of Euclidean space by unit cubes, *Comput. Math. Appl.*, **39** (2000), 49–53.

[6] N. Gravin, M. N. Kolountzakis, S. Robins and D. Shiryaev, Structure results for multiple tilings in 3D, *Discrete Comput. Geom.*, **50** (2013), 1033–1050.

[7] N. Gravin, S. Robins and D. Shiryaev, Translational tilings by a polytope, with multiplicity, *Combinatorica*, **32** (2012), 629–649.

[8] D. Hart, A. Iosevich, D. Koh, S. Senger, and Ignacio Uriarte-Tuero, Distance graphs in vector spaces over finite fields, in: *Recent Advances in Harmonic Analysis and Applications*, Springer Proc. Math. Stat., vol. 25, Springer (New York, 2013), pp. 139–160.

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

[10] P. McMullen, Convex bodies which tile space by translation, *Mathematika*, **27** (1980), 113–121.

[11] R. Robinson, Multiple tilings of n-dimensional space by unit cubes, *Math. Z.*, **166** (1979), 225–264.