# Lattice Coverings

Anqi Li - following [3]

### 1 Introduction

Let  $K \subset \mathbb{R}^n$  be a convex body (i.e. convex set with non-empty interior). A family of translates of K is called *covering* if their union is  $\mathbb{R}^n$ . This talk is about *lattice coverings* which is when these translation vectors are vectors of a lattice  $L \subset \mathbb{R}^n$ . Vaguely, the goal is to bound the smallest density of a lattice covering which can be imprecisely thought of as "the best choice of a lattice L to minimize the sum of volumes of the translates of K divided by the volume of  $\mathbb{R}^{n}$ ".

More precisely, for a convex body  $K \subset \mathbb{R}^n$  and a lattice  $L \subset \mathbb{R}^n$  define the covering density of K with respect to L to be

$$\Theta_K(L) := \frac{\inf\{\operatorname{Vol}(rK) : rK + L = \mathbb{R}^n\}}{|\det(L)|}.$$

In other words, we want the smallest possible r such that placing a dilate of K by a factor of r at each lattice point would cover all of space.

**Remark 1.1.** In the covering literature, there is also the notion of covering radius. This current notion of  $\Theta_K(L)$  in some sense capture more fine grained notions of the covering problem since volume scales rapidly with the dimension n of the problem.

**Definition 1.2.** The *lattice covering density* of a convex body  $K \subset \mathbb{R}^n$  is

$$\Theta_K = \inf_L \{ \Theta_K(L) : L \subset \mathbb{R}^n \text{ lattice} \}.$$

This quantifies the notion of finding a lattice L for which the overlaps of translates K does not take up too much space.

**Example 1.3.** A (silly) example is to consider K to be the n-dimensional unit cube. Then taking  $L = \mathbb{Z}^n$  we get  $\Theta_K(L) = \Theta_K = 1$ .

#### 1.1 Earlier results

One of the most important works in this direction is due to Rogers [4, 5].

**Theorem 1.4.** When K = B(0, 1) is the n-dimensional Euclidean ball, there exist (absolute) constants  $c_1, c_2$  such that

$$c_1 n \le \Theta_K \le c_2 n (\log n)^{1/2 \log_2(2\pi e)}$$
.

The symmetry of the Euclidean ball is very critical in the proof of this theorem. Gritzmann [2] proved a similar looking bound for a larger class of convex bodies.

**Theorem 1.5.** For every convex body K in  $\mathbb{R}^n$  with an affine image symmetric about at least  $\log \log n + 4$  coordinate hyperplanes, there exists an absolute constant  $c_4$  such that

$$\Theta_K \le c_4 n (\log n)^{1 + \log_2 e}.$$

Up until [3], the best upper bound for general, not necessarily symmetric, convex bodies K is the following bound due to Rogers.

**Theorem 1.6.** For  $K \subset \mathbb{R}^n$  there exists (absolute) constant  $c_5$  such that

$$\Theta_K \le n^{\log \log n + c_5}.$$

### 1.2 New results in [3]

The first theorem that we will discuss gives a polynomial upper bound for the lattice covering density of general convex bodies *K*.

**Theorem 1.7** ([3, Theorem 1.1]). For  $K \subset \mathbb{R}^n$  there exists (absolute) constant c such that

$$\Theta_K \leq cn^2$$
.

The next question we may ask is what about the covering density of K with respect to a random lattice L? To formalize this question we need to introduce a probability measure on the space of lattices. We can identify the space  $\mathcal{L}_n$  of all lattice of covolume 1 with  $SL_n(\mathbb{R})/SL_n(\mathbb{Z})$ . Let  $\mu_n$  be the unique Haar measure on  $\mathcal{L}_n$  that is  $SL_n(\mathbb{R})$ -invariant. We ask: what is the  $\mu_n$ -typical behavior of  $\Theta_K(L)$ ?

There is some subtlety in asking this question. It turns out that  $\mathbb{E}_{\mu_n}\Theta_K(L)=\infty$ . The following theorem by Strömbergsson [7] hints at the right kind of question that we should ask.

**Theorem 1.8.** Let  $\mu_n$  be defined as above. For any  $\delta > 0.77$ , as  $n \to \infty$ , we have that

$$\mu_n(\{L: \Theta_K(L) \ge (1+\delta)^n\}) \to 0.$$

In this direction, the following was proven in [3].

**Theorem 1.9** ([3, Theorem 1.2]). There are (absolute constants)  $c_1, c_2 > 0$  such that for any n and for all  $M \in [n^2, n^3]$ ,

$$\sup_{K: n-dim \ convex \ body} \mu_n\{L: \Theta_K(L) > M\} < c_1 e^{-c_2 M/n^2}.$$

Intuitively what this result says is that one way to construct an optimal lattice packing is to sample a random lattice.

### 2 Overview of tools

### 2.1 Rogers-Schmidt bounds

We need the following theorem due to Schmidt (essentially Theorem 4 of [6]). We use the following notation. For a lattice  $L \subset \mathbb{R}^n$ , define the torus  $\mathbb{T}_L = \mathbb{R}^n/L$ . Let  $m_L$  be the normalized Lebesgue measure on  $\mathbb{T}_L$ . Let  $\pi_L : \mathbb{R}^n \to \mathbb{T}_L$  be the projection map. Given a measurable set  $J \subset \mathbb{R}^n$ , we are interested in the proportion of the torus  $\mathbb{T}_L$  that is missed by the projection  $\pi_L(J)$  of J onto the torus. Write  $\mathcal{E}(J,L) = 1 - m_L(\pi_L(J))$ .

**Theorem 2.1.**  $J \subset \mathbb{R}^n$  be a measurable set. There exists constants  $c_1, c_2 > 0$  such that if  $V = \text{vol}(J) \le c_1 n$  then for all  $\kappa > 0$ ,

$$\mu_n(\{L:\mathcal{E}(J,L)>\kappa e^{-V}\})\leq \frac{1}{\kappa}+\frac{c_2}{\kappa}e^{V-c_1n}.$$

Heuristically, suppose  $L = \mathbb{Z}^n$  and think of every point on the torus  $\mathbb{T}_L$  as an independent event for if it is hit by the projection map  $\pi_L$ . Then the expected number of points hit is approximately  $e^{-\text{vol}(J)}$ . The theorem can then be thought of as deviation inequalities for random lattices. The key technical tool used to prove this kind of theorems in the geometry of numbers is a suitable generalization of Siegel's integral formula.

**Theorem 2.2** (Siegel's integral formula). For compactly supported, bounded and measurable  $f: \mathbb{R}^n \to \mathbb{R}$ , we have

$$\int_{\mathcal{L}_n} \sum_{x \in I \setminus \{0\}} f(x) d\mu_n(L) = \int_{\mathbb{R}^n} f(x) dx.$$

As a sidebar for how these kinds of integral formula are used, if we set f to be the characteristic function of a set  $S \subset \mathbb{R}^n$ , then the sum counts  $|S \cap \mathcal{L} \setminus \{0\}|$  and so we recover a version of Minkowski's theorem that a random lattice sampled according to  $\mu_n$  has on average  $\operatorname{vol}(S)$  nonzero vectors contained in it. It is conceivable that we would then need a higher moment version of this theorem for the lattice counting function  $\sum_{x \in \mathcal{L} \setminus \{0\}} f(x)$ .

**Theorem 2.3** (Rogers' integral formula). *For* k < n, *let*  $f : (\mathbb{R}^n)^k \to \mathbb{R}$  *be compactly supported, bounded and measurable* 

$$\int_{\mathcal{L}_n} \sum_{\substack{x_1, \dots, x_k \in L \\ independent}} f(x_1, \dots, x_k) d\mu_n(L) = \int_{\mathbb{R}^n} \dots \int_{\mathbb{R}^n} f(x_1, \dots, x_k) dx_1 \dots dx_k.$$

We do not go into further detail about how to prove these formulas, and refer the interested reader to [5]. Instead, we record the following useful corollary of Theorem 2.1 via Markov's inequality.

**Corollary 2.4.** Suppose *J* is a measurable set such that vol(J) = 2, then for any M > 0,

$$\mu_n(\{L: \mathcal{E}(J, L) \ge M\}) \le M^{-1}e^{-2} + O(e^{-n}).$$

### 2.2 Rank 2 Kakeya

**Definition 2.5.** We say that  $K \subset \mathbb{F}_p^n$  is an  $\varepsilon$ -*Kakeya set of rank r* if

$${S \in Gr_{n,r}(\mathbb{F}_n) \text{ such that } \exists x \text{ with } x + S \subset K} \ge \varepsilon |Gr_{n,r}(\mathbb{F}_n)|.$$

When  $\varepsilon = 1$  and r = 1 we recover the familiar notion of a discrete Kakeya set that contains a translated line in every direction. It turns out that the rank that we care about is r = 2. We will need the following result.

**Theorem 2.6.** *If*  $K \subset \mathbb{F}_p^n$  *is a*  $\varepsilon$ *-Kakeya set of rank* 2 *then* 

$$|K| \ge \varepsilon e^{-2n/p} p^n$$
.

At this stage, it is unclear why we care about this notion of  $\varepsilon$ -Kakeya set of rank 2. We will see its relevance in the next section. We defer the proof of this theorem to the last section. The proof is based on the method of multiplicities, which was the method used to obtain the bound of  $q^n/(2-1/q)^n$  in the (rank 1) Kakeya problem. In some sense, the proof of this theorem is fairly standard, and the new idea of the paper is in how this theorem is applied to the problem of lattice coverings.

### 3 Proof sketches of Theorem 1.7 and Theorem 1.9

WLOG by dilating we assume that Vol(K) = 2.

#### 3.1 Theorem 1.7

#### 3.1.1 Step I

First, we *cover most of space* using Corollary 2.4 which gives us a lattice  $L_1 \in \mathcal{L}_n$  with "small" holes, that is, such that  $m_{L_1}(\pi_{L_1}(K)) = 1 - e^{-2}/2 > 1/2$  where  $m_{L_1}$  is the normalized Lebesgue measure.

#### 3.1.2 Step II

By passing to a fundamental region of  $L_1$ , we can *discretize the set-up* by considering a finer grid than  $L_1$ . In what follows think of p as a prime on the order of n (chosen by Bertrand's postulate, say). Consider  $L_2 = \frac{1}{p} \cdot L_1$  obtained by dilating  $L_1$  by a factor of p in all directions:  $\pi_{L_1}(L_2) \subset \mathbb{T}_{L_1}$  is a dense  $p \times p \times \cdots \times p$  grid. We make the identification  $\pi_{L_1}(L_2) \simeq \mathbb{F}_p^n$ .

#### **3.1.3** Step III

We now work strictly in the fundamental region of  $L_1$ . We want to find an intermediate lattice  $L_1 \subset L \subset L_2$  such that putting copies of K at L covers the lattice  $L_2$ . Precisely, we want  $\pi_{L_1}(L+K) \supset \pi_{L_1}(L_2)$ .

Recall we identified  $\pi_{L_1}(L_2)$  with  $\mathbb{F}_p^n$ , and so  $L = \pi_{L_1}^{-1}(S)$  for a subspace  $S \subset \mathbb{F}_p^n$ . Then the covolume of L is given by

$$[L:L_1]^{-1}=p^{-\dim S}.$$

Now, we make the observation that if a convex body covers half the space then dilating it by a factor of 2 covers all of space.

**Observation 3.1.** Let K be an n-dimensional convex body and  $L \subset \mathbb{R}^n$  be a lattice. Suppose that

$$m_L(\pi_L(K)) > \frac{1}{2}.$$

Then  $L + 2K = \mathbb{R}^n$ .

*Proof.* Since  $m_L(\pi_L(K))$ ,  $M_L(\pi_L(-K)) > \frac{1}{2}$ , for any  $x \in \mathbb{T}_L$  it follows that there exists  $z_1, z_2 \in \pi_L(K)$  such that  $z_1 - x = z_2$ . Lifting  $z_1, z_2 \in \pi_L(K)$  into  $y_1, y_2 \in K$  we have that  $x = \pi_L(y_1 + y_2)$ . Since this holds for any  $x \in \mathbb{T}_L$  we obtain the desired conclusion.

Applying to  $\frac{1}{p} \cdot K$  and combining with Step I, we see that  $L_2 + \frac{2}{p} \cdot K = \mathbb{R}^n$ . Since  $L_2 \subset L + K$ , it follows that  $\mathbb{R}^n = L + (1 + \rho)K$ . For this lattice L, we have that

$$\Theta_K(L) \le \frac{\operatorname{vol}((1+2/p) \cdot K)}{\operatorname{covol}(L)} \approx p^{\dim S}.$$

So we really want to find an L with the property that  $\pi_{L_1}(L+K) \supset \pi_{L_1}(L_2)$  but also minimizing the dimension of the corresponding subset S. We will find S such that dim S=2 via the rank 2 Kakeya bound. Note that this recovers the quadratic bound in Theorem 1.7.

Let  $\mathbb{F}_p^n \cap \pi_{L_1}(K) = \widetilde{K}$ . We can rewrite our desired property as wanting to find S such that  $(x+S) \cap \widetilde{K} \neq \emptyset$  for all  $x \in \mathbb{F}_p^n$ . Let  $\widetilde{K}^c = \mathbb{F}_p^n - \widetilde{K}$ . Then the aforementioned can be written as  $\widetilde{K}^c$  not containing a copy of a translate of S, that is  $\widetilde{K}^c$  is not a 1-Kakeya set of rank 2! Theorem 2.6 gives a lower bound on the size of a Kakeya set, so if  $\widetilde{K}$  is large enough then its complement cannot be a discrete Kakeya set.

By Step 1, we have that  $|\widetilde{K}| \ge (1 - e^{-2}/2) \cdot p^n$  so that  $|\widetilde{K}^c| < e^{-2}p^n$  and applying Theorem 2.6 shows that  $\widetilde{K}^c$  is not a Kakeya set. So there exists  $S \in Gr_{n,2}(\mathbb{F}_p)$  with the desired properties, and we are done.

**Remark 3.2.** There is a subtle point here, which is that it only makes sense to apply Observation 3.1.3 to very small bodies because we are increasing the volume significantly by a factor of  $2^n$ ; when we discretized the problem we shrank K to work with  $\frac{1}{p} \cdot K$  and hence obtained a small enough body to apply Observation 3.1.3.

#### 3.2 Theorem 1.9

In this section, we note the modifications that we need to make to the proof of Theorem 1.7 to obtain this probabilistic version of the theorem.

Recall that we had a 3 step process: first we picked some lattice  $L_1$  such that using  $L_1$  we could cover a large fraction of space after translating K. Next, we thickened  $L_1$  to obtain  $L_2 = \frac{1}{p} \cdot L_1$  and made the identification  $L_2/L_1 \simeq \mathbb{F}_p^n$ . Then, we chose some subspace  $S \in \operatorname{Gr}_{n,2}(\mathbb{F}_p)$  and the final output was the "thickening"  $L = L_1 + S$ . For Theorem 1.9 we are sampling according to  $\mu_n$  so we need to show that our current sampling procedure still gives a lattice chosen according to  $\mu_n$ .

**Lemma 3.3** (White lie version of [3, Proposition 2.1]). The output of the following algorithm produces a random lattice (after rescaling appropriately) chosen according to  $\mu_n$ . Let p be any fixed prime in the interval [n, 2n).

Sampling procedure

- (1) Sample L' according to  $\mu_n$ .
- (2) Sample  $S \in Gr_{n,2}(\mathbb{F}_p)$  uniformly at random.
- (3) Output  $L = \frac{1}{p} \cdot L' + S$ .

Note that Corollary 2.4 tells us that most choices of L' in step (1) of the sampling procedure above would produce a lattice such that L' + K covers a large proportion of  $\mathbb{R}^n$ . However, in the proof of Theorem 1.7 we only used the fact that we could find *one* possible subspace S such that  $\widetilde{K} + S = \mathbb{F}_p^n$ , while need that

$$\frac{|\{S \in \operatorname{Gr}_{n,2}(\mathbb{F}_p^n) : \forall x \in \mathbb{F}_p^n, (x+S) \cap \widetilde{K} \neq \emptyset\}|}{|\operatorname{Gr}_{n,2}(\mathbb{F}_p^n)|}$$

so that when we sample S uniformly in step (2) we output a lattice L at the end of the algorithm with high probability.

Equivalently, we want the complement  $\widetilde{K}^c$  to miss many possible planes. Now if  $\widetilde{K}^c$  is not an  $\varepsilon$ -Kakeya set of rank 2 we would be done, and this is exactly the kind of conclusion we can obtain via Theorem 2.6.

## 4 Proof of rank 2 Kakeya

In this section, we prove the following lower bound on  $\varepsilon$ -Kakeya set of rank 2 that we need.

**Theorem 4.1.** If  $K \subset \mathbb{F}_p^n$  is a  $\varepsilon$ -Kakeya set of rank 2 then

$$|K| \ge \varepsilon e^{-2n/p} p^n$$
.

We begin by proving the following, which uses the same kind of polynomial method as in [1].

**Theorem 4.2.** Let  $\varepsilon \in (0,1]$ . If  $K \subset \mathbb{F}_p^n$  is an  $\varepsilon$ -Kakeya set of rank 2 then

$$|K| \ge \left(1 + \frac{(p-1)}{p^2 \varepsilon}\right)^{-n} p^n.$$

Note that the bound deteriorates for small  $\varepsilon$ . We will boost the bound to get the desired linear dependence on  $\epsilon$  in Theorem 2.6 via a probabilistic sampling argument.

### 4.1 Probabilistic boosting

**Lemma 4.3.** Let  $0 < \varepsilon < \delta < 1$ . Assume  $K \subset \mathbb{F}_p^n$  is an  $\varepsilon$ -Kakeya set of rank 2, then there exists a  $\delta$ -Kakeya set  $A \subset \mathbb{F}_p^n$  of rank 2 of size

$$|A| \le \left\lfloor \frac{\log(1-\delta)}{\log(1-\varepsilon)} \right\rfloor |K|.$$

*Proof.* For the given K, consider the associated subset W of Gr(n,2) of planes such that K contains some translate of it. Let  $N = \frac{\log(1-\delta)}{\log(1-\varepsilon)}$  and choose  $g_1, \ldots, g_N$  from  $GL_n(\mathbb{F}_p)$  independently and uniformly at random. It suffices to prove that

$$\left|\bigcup_{i} g_{i}W\right| \geq \delta |G_{n,2}(\mathbb{F}_{p})|.$$

Now, for some  $U \in W$  we have that the probability  $U \notin g_i W$  is given by  $1 - |B|/|G_{n,2}(\mathbb{F}_p)| \le 1 - \varepsilon$  and so

$$\mathbb{P}\left[U \notin \bigcup_{i=1}^{N} g_i W\right] \leq (1-\varepsilon)^N \leq 1-\delta.$$

The desired conclusion follows from linearity of expectation.

In particular, an immediate consequence of this lemma is that if K is an  $\varepsilon$ -Kakeya set of rank 2 then for any  $0 < \varepsilon < \delta < 1$ , we have that

$$|K| \ge \left( \left\lceil \frac{\log(1-\delta)}{\log(1-\varepsilon)} \right\rceil \right)^{-1} \cdot \left( 1 + (p-1)/(p^2 \varepsilon) \right)^{-n} \cdot p^n.$$

Taking  $\delta = 1/2$  so that  $\left\lceil \frac{\log(1-\delta)}{\log(1-\varepsilon)} \right\rceil \le 1/\varepsilon$ , we recover the bound

$$|K| \ge \varepsilon (1 + 2(q - 1)q^{-2})^{-n} q^n \ge \varepsilon p^n e^{-2n/p}.$$

### 4.2 Polynomial method

The scheme of the proof is as follows:

- Find a low degree non-zero polynomial that vanishes "with high multiplicity" on the  $\varepsilon$ -Kakeya set of rank 2, where the degree of the polynomial grows in the size of the Kakeya set.
- Show that the homogenous polynomial vanishes with high probability on a large subset of  $\mathbb{F}_p^n$ .
- Using a multiplicity version of the Schwartz-Zippel lemma that the homogeneous part of the polynomial was be identically zero if the Kakeya set is too small.

Now we introduce the Hasse derivative which can be thought of as a formal derivative in the finite field setting that has properties which parallels the usual notion of derivative in polynomial rings over general fields. This notion of the Hasse derivative will allow us to introduce a notion of multiplicity that is similar to the usual notion of a polynomial vanishing to a given order.

Some notation: for a multi-index  $\alpha \in \mathbb{N}_0^n$  write  $|\alpha| = \alpha_1 + \alpha_2 + \cdots + \alpha_n$ . Let  $X^{\alpha}$  denote  $x_1^{\alpha_1} \dots x_n^{\alpha_n}$ . For a polynomial P, let  $P_H$  denote the homogeneous part of P with the highest total degree.

**Definition 4.4.** For  $P \in \mathbb{F}_p[X]$ , the  $\alpha$ -Hasse derivative of P, denoted  $P^{(\alpha)}$ , is the polynomial which is the coefficient  $Y^{\alpha}$  in the expansion of P(X + Y), i.e.

$$P(X+Y) = \sum_{\alpha} P^{(\alpha)}(X)Y^{\alpha}.$$

**Definition 4.5.** The *multiplicity* of *P* at a point *X*, denoted mult(P, X), is the largest integer *i* such that  $P^{(\alpha)}(X) = 0$  for all  $\alpha$  with  $|\alpha| < i$ .

The following lemma summarizes the properties of the Hasse derivative that we need.

**Lemma 4.6.** • If  $X \in \mathbb{F}_p^n$  is such that  $\operatorname{mult}(P, X) = m$ , then  $\operatorname{mult}(P^{(\alpha)}, X) \ge m - |\alpha|$ .

• (Behavior of multiplicity under composition) For any  $X \in \mathbb{F}_n^n$  and polynomial P, Q, we have that

$$\operatorname{mult}(P \circ Q, X) \ge \operatorname{mult}(P, Q(X)).$$

We will also need the following multiplicity-version of the Schwartz-Zippel lemma.

**Lemma 4.7.** Let  $P \in \mathbb{F}_p[X]$  be a non-zero polynomial of degree at most d. Then for any finite  $S \subset \mathbb{F}_p$ , we have

$$\sum_{X \in \mathbb{F}_n^n} \operatorname{mult}(P, X) \le d|S|^{n-1}.$$

The following lemma expresses the polynomial technique.

**Lemma 4.8.** Given a set  $K \subset \mathbb{F}_p^n$  and non-negative integers m, d such that  $\binom{m+n-1}{n}|S| \leq \binom{n+d}{d}$ , then there exists a non-zero polynomial  $P \in \mathbb{F}_p[X]$  of total degree at most d such that  $\operatorname{mult}(P,X) \geq m$  for all  $X \in K$ .

With these tools in hand, we can now implement the scheme of the proof as mentioned at the beginning of this section.

*Proof.* For parameters, let  $d = cq^3 - 1$  and  $m = (q^2 + (q-1)/ε)c$  for sufficiently large c. We will show that  $|K| \ge \binom{n+d}{d} / \binom{m+n-1}{n}$ . For our choices of d and m, we have that  $\binom{n+d}{d} / \binom{m+n-1}{n} \to (1+(p-1)p^{-2}ε^{-1})^{-n}p^n$  as  $c \to ∞$ . Let  $\ell = (qm-d)/(q-1)$ . Not also for this choice of parameters we have that  $k < εp^2\ell$ . We will construct a polynomial P of degree k such that  $P_H$  vanishes to degree  $\ell$  on a large subset of  $\mathbb{F}_p^2$  which vaguely corresponds to the planes lying in the δ-Kakeya set.

- 1. Fix  $\alpha \in \mathbb{N}_0^n$  such that  $|\alpha| = w < \ell$ . By Lemma 4.8, we can find a polynomial P that vanishes to multiplicity at least m at each point of P. Write  $Q = P^{(\alpha)}$ .
- 2. We can think of set of planes which contain a translation lying in K as a subset of  $\mathbb{F}_p^2$ ; let  $U \subset \mathbb{F}_p^2$  be the set of pairs (x, y) such that there exists  $a \in \mathbb{F}_p^n$  such that  $a + xt_1 + yt_2 \in K$  for all  $t_1, t_2 \in \mathbb{F}_p$ . Note that  $|U| \ge \delta p^2$ . Step 1 means for  $(x, y) \in U$  there exists a such that

$$\operatorname{mult}(P, a + t_1 x + t_2 y) \ge m$$

for all  $t_1, t_2 \in \mathbb{F}_p$  which by the behavior of multiplicity under composition implies that if we think of  $Q(a + T_1x + T_2y) \in \mathbb{F}_p[T_1, T_2]$  then

$$\text{mult}(Q(a + T_1x + T_2y), (t_1, t_2)) \ge \text{mult}(Q, a + t_1x + t_2y) \ge m - w.$$

But deg  $Q(a + T_1x + T_2y) \le \deg Q \le k - w \le q(m - w)$  by definition of  $w < \ell$ . So an application of the Schwartz-Zippel lemma we stated above implies that  $Q(a + T_1x + T_2y)$  is the zero polynomial and so  $Q_H(T_1x + T_2y) \equiv 0$  as well. This means that for all  $(x, y) \in D$  we have that  $P_H^{(\alpha)}(T_1x + T_2y) \equiv 0$ .

3. Now, consider  $P_H^{(\alpha)}$  as a polynomial in n variables over  $\mathbb{F}_p(T_1,T_2)$ . Then we have shown that it vanishes at  $\widetilde{U}=\{xT_1+yT_2:(x,y)\in U\}$ . But now allowing  $\alpha$  to vary it follows that we have shown this for all  $|\alpha|<\ell$ , so that P vanishes to multiplicity at least  $\ell$  at all points of  $\widetilde{U}$ . Since  $|\widetilde{U}|\geq \delta p^{2n}$ , it follows by applying Schwartz-Zippel again that P has to be the zero polynomial since  $\deg P\leq k<\delta p^2\ell$ , which is a contradiction.

### References

[1] Zeev Dvir, Swastik Kopparty, Shubhangi Saraf, and Madhu Sudan, *Extensions to the method of multi- plicities, with applications to Kakeya sets and mergers*, 2009 50th Annual IEEE Symposium on Foundations of Computer Science—FOCS 2009, IEEE Computer Soc., Los Alamitos, CA, 2009, pp. 181–190. MR 2648400

- [2] Peter Gritzmann, Lattice covering of space with symmetric convex bodies, Mathematika **32** (1985), no. 2, 311–315 (1986). MR 834499
- [3] Or Ordentlich, Oded Regev, and Barak Weiss, *New bounds on the density of lattice coverings*, J. Amer. Math. Soc. **35** (2022), no. 1, 295–308. MR 4322394
- [4] C. A. Rogers, Lattice coverings of space, Mathematika 6 (1959), 33–39. MR 124820
- [5] \_\_\_\_\_, Packing and covering, Cambridge Tracts in Mathematics and Mathematical Physics, No. 54, Cambridge University Press, New York, 1964. MR 0172183
- [6] Wolfgang M. Schmidt, *The measure of the set of admissible lattices*, Proc. Amer. Math. Soc. **9** (1958), 390–403. MR 96638
- [7] Andreas Strömbergsson, *On the limit distribution of Frobenius numbers*, Acta Arith. **152** (2012), no. 1, 81–107. MR 2869212