BOUNDS ON THE DENSITY OF SMOOTH LATTICE COVERINGS

OR ORDENTLICH, ODED REGEV, AND BARAK WEISS

ABSTRACT. Let $\mathcal{K}$ be a convex body in $\mathbb{R}^n$, let L be a lattice with unit covolume, and let $\eta > 0$. We say that $\mathcal{K}$ and L form an *η-smooth cover* if each point $x \in \mathbb{R}^n$ is covered by $(1 \pm \eta)\mathrm{vol}(\mathcal{K})$ translates of $\mathcal{K}$ by L. We prove that for any positive σ and η, asymptotically as $n \to \infty$, for any $\mathcal{K}$ of volume $n^{3+\sigma}$, one can find a lattice L for which $\mathcal{K}, L$ form an η-smooth cover. Moreover, this property is satisfied with high probability for a lattice chosen randomly, according to the Haar-Siegel measure on the space of lattices. Similar results hold for random construction A lattices, albeit with a worse power law, provided that the ratio between the covering and packing radii of $\mathbb{Z}^n$ with respect to $\mathcal{K}$ is at most polynomial in n. Our proofs rely on a recent breakthrough of Dhar and Dvir on the discrete Kakeya problem.

1. INTRODUCTION

Let Conv_n denote the set of bounded convex subsets of $\mathbb{R}^n$ with nonempty interior. For a lattice $L \subset \mathbb{R}^n$, convex set $\mathcal{K} \in \mathrm{Conv}_n$, and a point $x \in \mathbb{R}^n$ we denote

$$N(L, \mathcal{K}, x) \stackrel{\mathrm{def}}{=} |L \cap (\mathcal{K} + x)| = |\{y \in L \ : \ x \in y - \mathcal{K}\}| \,. \tag{1}$$

The expectation of $N(L, \mathcal{K}, x)$ when x is drawn uniformly from a fundamental domain for L is $\mathrm{vol}(\mathcal{K})/\mathrm{covol}(L)$; thus if we draw x uniformly in a ball $B(0, T)$ with respect to some norm, the expectation of $N(L, \mathcal{K}, x)$ approaches $\mathrm{vol}(\mathcal{K})/\mathrm{covol}(L)$, in the limit as $T \to \infty$. Furthermore, we have that $\frac{N(L, \alpha\mathcal{K}, x)}{\mathrm{vol}(\alpha\mathcal{K})/\mathrm{covol}(L)}$ tends to 1 as the dilation factor α grows, where the convergence is uniform in x. It is therefore natural to ask, given $\mathcal{K} \in \mathrm{Conv}_n$ and a lattice $L \subset \mathbb{R}^n$, whether the fraction $\frac{N(L, \mathcal{K}, x)}{\mathrm{vol}(\mathcal{K})/\mathrm{covol}(L)}$ is nearly constant on $\mathbb{R}^n$. To that end we define the following quantity:

Date: June 10, 2024.

Definition 1.1. *The* covering smoothness *of a lattice $L \subset \mathbb{R}^n$ with respect to a convex body $\mathcal{K} \in \mathrm{Conv}_n$ is defined as*

$$\eta(\mathcal{K}, L) \stackrel{\mathrm{def}}{=} \sup_{x \in \mathbb{R}^n} \left| \frac{N(L, \mathcal{K}, x)}{\mathrm{vol}(\mathcal{K})/\mathrm{covol}(L)} - 1 \right|.$$

Note that $\eta(\mathcal{K}, L) < 1$ immediately implies that $L + \mathcal{K} = \mathbb{R}^n$. In this case the pair $(L, \mathcal{K})$ is said to be *a covering*. (The reverse statement is not true — there may be points x that are covered an exceptionally large number of times by translates of $\mathcal{K}$.) As in the abstract, if $\eta(\mathcal{K}, L) < \eta$ we say that the covering given by $\mathcal{K}$ and L is *η-smooth.*

Let μ_n denote the Haar-Siegel measure; that is, the unique probability measure on the space of lattices in $\mathbb{R}^n$ of unit covolume, which is invariant under volume preserving linear transformations. Our main result is that for every $\mathcal{K} \in \mathrm{Conv}_n$ whose volume is polynomial in n, and for most lattices in $\mathbb{R}^n$, the covering smoothness is small.

Theorem 1.2. *Let $n > 25$, and let $\mathcal{K} \in \mathrm{Conv}_n$. Let $\delta, \varepsilon \in (0, 1)$, and assume $\mathrm{vol}(\mathcal{K}) \geq c_1 \left(\frac{1}{\varepsilon\delta}\right)^{6.5} n^3$, where $c_1 = 2^{66}$. Then, for $L \sim \mu_n$ we have*

$$\Pr\left(\eta(\mathcal{K}, L) \geq \varepsilon\right) < \delta. \tag{2}$$

In particular, for any positive ε, σ,

$$\sup_{\mathcal{K} \in \mathrm{Conv}_n, \mathrm{vol}(\mathcal{K}) \geq n^{3+\sigma}} \Pr\left(\eta(\mathcal{K}, L) \geq \varepsilon\right) \longrightarrow_{n \to \infty} 0.$$

We did not attempt to optimize the multiplicative constant c_1 in this result, or similar constants c_i in the sequel.

Theorem 1.2 and the remaining statements below might find applications in computer science. Specifically, in lattice-based cryptography, smoothing a lattice is a key idea used to hide secret information from an adversary [MR07]. Typically, one considers smoothing by a Gaussian distribution. However, for some applications it might be advantageous to smooth using a convex body, since sampling from a convex body like a cube can be more efficient. It should be noted that in many cryptographic applications, closeness in L_1 is sufficient, and such L_1-smoothness results (in fact, even L_2-smoothness) are often much easier to prove (see, e.g., [DADRT23]); yet there are many cases where closeness in L_∞ (as in our results) leads to tighter results [BLRL$^+$18].

It is instructive to compare Theorem 1.2 with our previous work [ORW21] on lattice coverings. Recall that for a lattice $L \subset \mathbb{R}^n$ of covolume one, the *covering density* $\Theta(\mathcal{K}, L)$ is the minimal volume of

a dilate $\alpha\mathcal{K}$ such that $(L, \alpha\mathcal{K})$ is a covering. One of the results of [ORW21] is that

$$\sup_{\mathcal{K}\in \mathrm{Conv}_n} \inf_{L \text{ of covolume } 1} \Theta(\mathcal{K}, L) \tag{3}$$

grows at most quadratically in n (prior to [ORW21] the best known bound, due to Rogers [Rog58], was superpolynomial). In fact, it was shown that for any $\delta > 0$, any $\sigma > 0$, any large enough n and any $\mathcal{K} \in \mathrm{Conv}_n$, if $\mathrm{vol}(\mathcal{K}) \geq n^{2+\sigma}$ then the μ_n-probability that $(L, \mathcal{K})$ is a covering is at least $1 - \delta$. Fixing $\varepsilon \in (0, 1)$, we deduce easily from Theorem 1.2 the slightly weaker statement, in which $2 + \sigma$ is replaced with $3 + \sigma$. That is, when $\mathrm{vol}(\mathcal{K}) > n^{2+\sigma}$, we know from [ORW21] that a random L gives a covering, and from Theorem 1.2 we know that when $\mathrm{vol}(\mathcal{K}) > n^{3+\sigma}$ a random L gives an ε-smooth covering. On the other hand, [CFR59] shows that for $\mathcal{K}$ taken as the Euclidean ball and any lattice L of covolume 1, $\eta(\mathcal{K}, L) \geq 1$ (and moreover, $(L, \mathcal{K})$ is not a covering) unless $\mathrm{vol}(\mathcal{K}) = \Omega(n)$.

While we intuitively expect covering to become smoother as we scale up $\mathcal{K}$, it turns out that in general $\alpha \mapsto \eta(\alpha\mathcal{K}, L)$ is not monotonically non-increasing. To see this, take $L = \mathbb{Z}^n$ and $\mathcal{K} = [0, 1)^n$. Then $\eta(\mathcal{K}, \mathbb{Z}^n) = 0$ yet for small $\varepsilon > 0$, $\eta((1+\varepsilon)\mathcal{K}, \mathbb{Z}^n) = (2/(1+\varepsilon))^n - 1$. It is therefore natural to further define the following quantity for a lattice $L \subset \mathbb{R}^n$ and $\mathcal{K} \in \mathrm{Conv}_n$,

$$\Phi_{\mathcal{K},L}(\varepsilon) \stackrel{\text{def}}{=} \sup\left\{ \frac{\mathrm{vol}(\alpha\mathcal{K})}{\mathrm{covol}(L)} \ : \ \alpha > 0 \text{ satisfies } \eta(\alpha\mathcal{K}, L) > \varepsilon \right\}.$$

In particular, for a lattice $L \subset \mathbb{R}^n$ of unit covolume, we have that $\eta(\alpha\mathcal{K}, L) \leq \varepsilon$ for *all* dilates $\alpha\mathcal{K}$ of volume exceeding $\Phi_{\mathcal{K},L}(\varepsilon)$. We prove the following theorem.

Theorem 1.3. *Let $n > 25$, and let $\mathcal{K} \in \mathrm{Conv}_n$. Let $\delta, \varepsilon \in (0, 1)$, and $c_2 = 2^{112}$. Then, for $L \sim \mu_n$ we have*

$$\Pr\left(\Phi_{\mathcal{K},L}(\varepsilon) \geq c_2 \left(\frac{1}{\varepsilon^2\delta}\right)^{6.5} n^3 \right) < \delta. \tag{4}$$

1.1. **Construction A lattices.** In many applications in electrical engineering and computer science, integer lattices known as *construction A lattices* are of interest [CS88, Loe97]. For a prime p let $\mathbb{F}_p$ denote the field with p elements. For $r \in \{1, \ldots, n\}$, let $\mathrm{Gr}_{n,r}(\mathbb{F}_p)$ denote the collection of subspaces of dimension r in $\mathbb{F}_p^n$, or equivalently, the rank-r additive subgroups of $\mathbb{F}_p^n$. We can identify $\mathbb{F}_p$ with the residues $\{0, \ldots, p-1\}$, and thus identify $\mathbb{F}_p^n$ with the quotient $\mathbb{Z}^n/p\mathbb{Z}^n$. We have a natural *reduction mod p* homomorphism $\pi_p : \mathbb{Z}^n \to \mathbb{F}_p^n$, which

sends each coordinate of $x \in \mathbb{Z}^n$ to its class modulo p. Any element $S \in \mathrm{Gr}_{n,r}(\mathbb{F}_p)$ gives rise to a sub-lattice $\pi_p^{-1}(S) \subset \mathbb{Z}^n$, which contains $p\mathbb{Z}^n$ as a subgroup of index p^r, and with $\pi_p^{-1}(S)/p\mathbb{Z}^n$ isomorphic as an abelian group to $S \cong \prod_1^r \mathbb{Z}/p\mathbb{Z}$. The ensemble of lattices obtained by drawing $S \sim \mathrm{Uniform}(\mathrm{Gr}_{n,r}(\mathbb{F}_p))$ and setting $L = \frac{1}{p} \cdot \pi_p^{-1}(S)$ is called the *random* (p,r) *construction A ensemble*[1] and such lattices are called (p,r) *construction A lattices*.

Theorem 1.2 holds for any $\mathcal{K} \in \mathrm{Conv}_n$, with uniform constants. However, if $\mathcal{K}$ is such that $N(\mathcal{K}, \mathbb{Z}^n, 0)$ is large (for example $\mathcal{K} = \prod_1^{n-1}[\varepsilon^{-1}, \varepsilon^{-1}] \times [-\varepsilon^{n-1}, \varepsilon^{n-1}]$ for ε small), it will not be smoothed by applying construction A, unless p and r are large (depending on $\mathcal{K}$). Thus our results for construction A lattices depend on $\mathcal{K}$. The dependence arises via the ratio between the *covering radius* and *packing radius* of $\mathcal{K}$ with respect to $\mathbb{Z}^n$. Namely, for a convex body $\mathcal{K} \in \mathrm{Conv}_n$ and a lattice $L \subset \mathbb{R}^n$ we denote by $\mathrm{r}_{\mathrm{cov},\mathcal{K}}(L)$ the infimum of α for which $(L, \alpha\mathcal{K})$ is a covering, and by $\mathrm{r}_{\mathrm{pack},\mathcal{K}}(L)$ the supremum of α for which $(L, \alpha\mathcal{K})$ is a *packing*, i.e., the translates $\{\ell + \alpha\mathcal{K} : \ell \in L\}$ are disjoint. We denote by

$$\rho_{\mathcal{K}}(L) \stackrel{\mathrm{def}}{=} \frac{\mathrm{r}_{\mathrm{cov},\mathcal{K}}(L)}{\mathrm{r}_{\mathrm{pack},\mathcal{K}}(L)} \tag{5}$$

the ratio between the covering and the packing radius. We show that for $\mathcal{K} \in \mathrm{Conv}_n$ for which both $\mathrm{vol}(\mathcal{K})$ and $\rho_{\mathcal{K}}(\mathbb{Z}^n)$ are polynomial in n, for a typical construction A lattice with adequately tuned p, r, scaled to have unit covolume, the covering smoothness is small.

Theorem 1.4. *Let $n > 25$, and let $\mathcal{K} \in \mathrm{Conv}_n$ and $b > 0$ satisfy*

$$0 \le b \le \frac{n}{2\log_2 n} \quad \text{and} \quad \rho_{\mathcal{K}}(\mathbb{Z}^n) < n^b. \tag{6}$$

Let $\delta, \varepsilon \in (0,1)$, and assume $\mathrm{vol}(\mathcal{K}) \ge c_3 \left(\frac{1}{\varepsilon\delta}\right)^6 n^{3(1+2b)}$, where $c_3 = e \cdot 2^{33}$. Let p be a prime number satisfying

$$\frac{1024}{(\varepsilon\delta)^2} n^{1+2b} \le p \le \frac{2048}{(\varepsilon\delta)^2} n^{1+2b}, \tag{7}$$

[1]Some authors define the (p,r) random construction A ensemble slightly differently, taking $S' = \mathrm{span}_{\mathbb{F}_p}(v_1, \ldots, v_r)$ and $v_1, \ldots, v_r \overset{i.i.d.}{\sim} \mathrm{Uniform}(\mathbb{F}_p^n)$ and $L = \frac{1}{p} \cdot \pi_p^{-1}(S')$. Since $\Pr(S' \notin \mathrm{Gr}_{n,r}(\mathbb{F}_p)) \le p^{r-n}$ and, moreover, S' is conditionally uniform on $\mathrm{Gr}_{n,r}(\mathbb{F}_p)$ under the event $S' \in \mathrm{Gr}_{n,r}(\mathbb{F}_p)$, we have that the total variation distance between the distributions corresponding to the two definitions is at most p^{r-n}.

and $r = 3 + \left\lceil \frac{n}{\log p} \left(b \log n + \log 3 \right) \right\rceil$. *Then, if* L *is drawn from the* (p, r) *random construction A ensemble (so that* $\mathrm{covol}(p^{r/n} L) = 1$*), we have*

$$\Pr\left(\eta(\mathcal{K}, p^{r/n} L) \geq \varepsilon \right) < \delta \, .$$

An important special case is the Euclidean ball, namely $\mathcal{K} = \mathcal{B}_n = \{x \in \mathbb{R}^n \ : \ \|x\|_2 \leq 1\}$. It is well known (and easy to see) that

$$\mathrm{r}_{\mathrm{pack}, \mathcal{B}_n}(\mathbb{Z}^n) = \frac{1}{2} \qquad \text{and} \quad \mathrm{r}_{\mathrm{cov}, \mathcal{B}_n}(\mathbb{Z}^n) = \frac{\sqrt{n}}{2},$$

which gives

$$\rho_{\mathcal{B}_n}(\mathbb{Z}^n) = n^{1/2}.$$

Thus, the following is an immediate consequence of Theorem 1.4.

Corollary 1.5. *Let* $n > 25$*, and let* $\delta, \varepsilon \in (0, 1)$*, and for* $\alpha > 0$*, assume*

$$\mathrm{vol}(\alpha \mathcal{B}_n) \geq c_3 \left(\frac{1}{\varepsilon \delta} \right)^6 n^6,$$

where $c_3 = e \cdot 2^{33}$*. Let* p *be a prime number satisfying*

$$\frac{1024}{(\varepsilon \delta)^2} n^2 \leq p \leq \frac{2048}{(\varepsilon \delta)^2} n^2,$$

and $r = 3 + \left\lceil \frac{n}{\log p} \left(\frac{1}{2} \log 9n \right) \right\rceil$. *Then if* L *is drawn from the* (p, r) *random construction A ensemble (so that* $\mathrm{covol}(p^{r/n} L) = 1$*), we have*

$$\Pr\left(\eta(\alpha \mathcal{B}_n, p^{r/n} L) \geq \varepsilon \right) < \delta \, .$$

Similarly to the case where L is drawn at random according to the distribution μ_n, we can also show that for L drawn from the (p, r) random construction A ensemble, for $\mathcal{K} \in \mathrm{Conv}_n$ with $\rho_{\mathcal{K}}(\mathbb{Z}^n)$ polynomial in n, we have that with high probability $\Phi_{\mathcal{K}, L}(\varepsilon)$ is also polynomial in n, provided that p and r are chosen adequately.

Theorem 1.6. *Let* $n > 25$*, and let* $\mathcal{K} \in \mathrm{Conv}_n$ *and* $b > 0$ *satisfy* (6)*. Let* $\delta, \varepsilon \in (0, 1)$*, and* $c_4 = e \cdot 2^{57}$*. Let* p *be a prime number satisfying*

$$\frac{2^{18}}{(\varepsilon^2 \delta)^2} n^{3+2b} \leq p \leq \frac{2^{19}}{(\varepsilon^2 \delta)^2} n^{3+2b}, \tag{8}$$

and $r = 3 + \left\lceil \frac{n}{\log p} \left(b \log n + \log 3 \right) \right\rceil$. *Then, if* L *is drawn from the* (p, r) *random construction A ensemble, we have*

$$\Pr\left(\Phi_{\mathcal{K},L}(\varepsilon) > c_4 \left(\frac{1}{\varepsilon^2 \delta} \right)^6 n^{9+6b} \right) \leq \delta. \tag{9}$$

1.2. **Non-lattice smooth coverings.** If one relaxes the requirement that L is a lattice, it is slightly more complicated to define smooth covers, but much easier to construct them.

Let $L \subset \mathbb{R}^n$ be a discrete set (not necessarily a lattice). We continue to use the notation $N(L, \mathcal{K}, x)$ defined in (1). Let $B(0, T)$ denote the ball of radius T around the origin with respect to the Euclidean norm, and define the *asymptotic upper density* of L by

$$D(L) \stackrel{\text{def}}{=} \limsup_{T \to \infty} \frac{|B(0,T) \cap L|}{\text{vol}(B(0,T))}. \tag{10}$$

If the limit in (10) exists we will say that L *has an asymptotic density*. Note that lattices have an asymptotic density given by $D(L) = \text{covol}(L)^{-1}$. Now for $\mathcal{K} \in \text{Conv}_n$, and L as above, we set

$$\eta(\mathcal{K}, L) \stackrel{\text{def}}{=} \sup_{x \in \mathbb{R}^n} \left| \frac{N(L, \mathcal{K}, x)}{\text{vol}(\mathcal{K})\, D(L)} - 1 \right|.$$

With this notation we have:

Theorem 1.7. *For any* $0 < \varepsilon < 1$, $n \geq 20$, *and any* $\mathcal{K} \in \text{Conv}_n$ *there is a discrete set* $L \subset \mathbb{R}^n$ *which has an asymptotic density, satisfying*

$$\text{vol}(\mathcal{K}) D(L) \leq \frac{14}{\varepsilon^2} \left(n \log n + n \log \frac{1280}{\varepsilon} + 2 \right) \quad \text{and} \quad \eta(\mathcal{K}, L) < \varepsilon. \tag{11}$$

We remark that the set L constructed in the proof of Theorem 1.7 is *periodic*, i.e., consists of finitely many translates of a lattice in $\mathbb{R}^n$. We also remark that Theorem 1.7 can be derived by modifying the proof of Erdős and Rogers [ER62], who proved a closely related statement. For completeness, we include a proof in Section 3.5 that follows the proof structure of our main theorem.

1.3. **Acknowledgements.** The authors are grateful to Bo'az Klartag for suggesting the question of seeking smooth lattice coverings, to Manik Dhar and Ze'ev Dvir for sharing an early draft of their result, and to Chris Peikert for useful comments. The first author is supported by ISF 1641/21, the second author is supported by a Simons

Investigator Award from the Simons Foundation, and the third author is supported by ISF 2019/19 and ISF-NSFC 3739/21.

2. Techniques and Notation

The main results of this paper follow from the somewhat technical Theorem 3.4. This result is derived in turn from a new result of Dhar and Dvir (Theorem 2.2), which is a crucial input to this paper. In this section we introduce notations, give a brief overview of our approach, and state Theorem 2.2.

For a lattice $L \subset \mathbb{R}^n$ let $\mathbb{T}_L \stackrel{\text{def}}{=} \mathbb{R}^n/L$ be the quotient torus, let m_L be the Haar probability measure on $\mathbb{T}_L$, and let $\pi_L : \mathbb{R}^n \to \mathbb{T}_L$ be the quotient map. Let $v_1, \ldots, v_n$ be the generators of L given by the columns of g so that the parallellepiped

$$\mathcal{P}_L = \left\{ \sum a_i v_i : \forall i,\ 0 \leq a_i < 1 \right\}$$

is a fundamental domain for $\mathbb{R}^n/L$. Define the discrete 'net'

$$\mathcal{P}_L^{(\text{disc})} \stackrel{\text{def}}{=} \left\{ \sum a_i v_i \in \mathcal{P}_L : a_i \in \left\{ 0, \frac{1}{p}, \ldots, 1 - \frac{1}{p} \right\} \right\} \tag{12}$$

and set

$$\frac{L}{p} \stackrel{\text{def}}{=} \frac{1}{p} \cdot L.$$

Then the elements of $\mathcal{P}_L^{(\text{disc})}$ are coset representatives for the inclusion $L \subset \frac{L}{p}$, and there is an isomorphism (as abelian groups) $\mathcal{P}_L^{(\text{disc})} \cong \mathbb{F}_p^n$.

Next, we introduce a well-studied technique for randomly choosing lattices. Given $L = g\mathbb{Z}^n$, where g is an invertible $n \times n$ matrix, and given $S \in \text{Gr}_{n,r}(\mathbb{F}_p)$, we define the super-lattice $L(S) \supset L$ as

$$L(S) \stackrel{\text{def}}{=} \frac{1}{p} \cdot g\pi_p^{-1}(S). \tag{13}$$

Notice that the scaled-up version $p^{r/n} \cdot L(S)$ of $L(S)$ is of the same covolume as L. The assignment

$$L \ \mapsto \ \left\{ p^{r/n} L(S) : S \in \text{Gr}_{n,r}(\mathbb{F}_p) \right\} \tag{14}$$

is a special case of the so-called *Hecke correspondence.* Note that the individual lattice $L(S)$ also depends on the initial choice of g for which $L = g\mathbb{Z}^n$, but the collection on the right-hand side of (14) does not. Also note that Construction A lattices are a special case of this construction (up to scaling), starting with $L = \mathbb{Z}^n$.

Given a convex body $\mathcal{K}$, our goal is to find a lattice for which the covering smoothness is small. We will choose this lattice to be $L(S)$ for a randomly chosen $S \in \text{Gr}_{n,r}(\mathbb{F}_p)$ for some r and p, and where

L is a lattice for which we have a reasonable bound on $\rho_{\mathcal{K}}(L)$. For instance, in the proof of Theorem 1.2, we will take L to be a randomly chosen lattice according to the Haar-Siegel measure μ_n, which has a small $\rho_{\mathcal{K}}$ (Proposition 3.6); importantly, by [ORW21, Proposition 2.1], $L(S)$ is also distributed according to μ_n (up to scaling), as needed for the conclusion of Theorem 1.2.

By rescaling $\mathcal{K}$ we may assume that L forms a packing with respect to $\mathcal{K}$ and a covering with respect to the dilate $\rho_{\mathcal{K}}(L)\mathcal{K}$. Recall that our goal is to show that the function

$$\mathbb{T}_{L(S)} \to \mathbb{N}, \qquad x \mapsto |(x + L(S)) \cap \mathcal{K}| \tag{15}$$

is uniformly close to a constant function. By a discretization procedure (see Proposition 3.1), it will be sufficient to show that the restriction of the function in (15) to $\mathcal{P}_L^{(\mathrm{disc})}$ is close to a constant function. This uses the fact that L is a covering with respect to $\rho_{\mathcal{K}}(L)\mathcal{K}$ and assumes that p is chosen sufficiently large with respect to $\rho_{\mathcal{K}}(L)$.

The final step in the proof is to reduce the problem to an analogous problem in $\mathbb{F}_p^n$. Denoting by $A \subset \mathbb{F}_p^n$ the set $\pi_L\left(\frac{L}{p} \cap \mathcal{K}\right)$ viewed as a subset of $\mathbb{F}_p^n$, we have that for any $x \in \mathcal{P}_L^{(\mathrm{disc})}$,

$$|(x + L(S)) \cap \mathcal{K}| = \left|\pi_L\Big((x + L(S)) \cap \mathcal{K}\Big)\right| = |(x + S) \cap A| \,, \tag{16}$$

where the first equality uses the assumption that L forms a packing with respect to $\mathcal{K}$ (and so π_L is injective on $\mathcal{K}$) and on the right-hand side we think of x as being in $\mathbb{F}_p^n$. Thus our problem reduces to showing that a randomly chosen S leads to a smooth covering of $\mathbb{F}_p^n$ by the S-translates of A. This is precisely the problem addressed by Dhar and Dvir.

To state their result we need the following discrete analogue of the covering smoothness:

Definition 2.1. *Let p be a prime number. The* smoothness of a set $S \subset \mathbb{F}_p^n$ with respect to a set $A \subset \mathbb{F}_p^n$ *is defined as*

$$\eta_{\mathbb{F}_p}(A, S) \stackrel{\mathrm{def}}{=} \sup_{x \in \mathbb{F}_p^n} \left| \frac{|(x + S) \cap A|}{|S| \cdot |A| \cdot p^{-n}} - 1 \right| .$$

With this notation we have:[2]

[2]The precise statement given in [DD22, Theorem III.3] deals only with the smallest possible choice of $r = 3+n-\lfloor \log_p |A| \rfloor = \lceil 3+n-\log_p |A| \rceil$. However, any larger choice of r also works, since, as noted in [DD22], if a subspace S is τ-shift-balanced, and S' is a subspace containing S, then S' is also τ-shift-balanced.

Theorem 2.2 (Dhar and Dvir, Theorem III.3 in [DD22])**.** *Let $n \geq 5$, let $\delta, \tau \in (0,1)$ and let p be a prime number satisfying $p > 64n/(\tau\delta)^2$. Let $A \subset \mathbb{F}_p^n$ and let $4 \leq r \leq n$ be an integer satisfying $r > 3 + n - \log_p |A|$. Then for $S \sim \text{Uniform}\left(\text{Gr}_{n,r}(\mathbb{F}_p)\right)$ we have*

$$\Pr(\eta_{\mathbb{F}_p}(A, S) > \tau) < \delta. \tag{17}$$

To summarize, by (16) and the discretization argument, if the conclusion of Theorem 2.2 holds with $A = \pi_L\left(\frac{L}{p} \cap \mathcal{K}\right)$, then we obtain the desired result, namely, that with high probability, $L(S)$ is a smooth covering for $\mathcal{K}$ of density

$$\frac{\text{vol}(\mathcal{K})}{\text{covol}(L(S))} = p^r \frac{\text{vol}(\mathcal{K})}{\text{covol}(L)} \ .$$

Noting that $|A| \approx p^n \frac{\text{vol}(\mathcal{K})}{\text{covol}(L)}$ (Lemma 3.3) and taking $r = 3+n-\log_p |A|$ (ignoring here the technicality of r having to be an integer) we get a density of about p^3. Finally, we need to choose p to satisfy the conditions of Theorem 2.2 and be large enough compared to $\rho_{\mathcal{K}}(L)$ for the discretization argument to work.

We end this section by noting that improvements to Theorem 2.2 will yield improvements in our results. We make this precise in Remark 3.7.

3. Proofs of Main Results for Lattices

3.1. **Discretization.** For subsets $A, B \subset \mathbb{R}^n$ and $c \in \mathbb{R}$ we denote as usual

$$A + B \stackrel{\text{def}}{=} \{a + b : a \in A, b \in B\}, \quad cA \stackrel{\text{def}}{=} \{ca : a \in A\}.$$

Proposition 3.1. *Let $L' \subset \mathbb{R}^n$ be a discrete subset of $\mathbb{R}^n$ such that $L' = -L'$, let $\mathcal{K} \in \text{Conv}_n$, and assume $0 < \rho < 1$ is such that $L' + \rho\mathcal{K} = \mathbb{R}^n$. Then for any $x \in \mathbb{R}^n$ there are $y_1, y_2 \in L'$ such that*

$$(1-\rho)\mathcal{K} + y_1 \subset \mathcal{K} + x \subset (1+\rho)\mathcal{K} + y_2. \tag{18}$$

Proof. The convexity of $\mathcal{K}$ implies that for any positive α and β we have

$$\alpha\mathcal{K} + \beta\mathcal{K} = (\alpha+\beta)\left\{\frac{\alpha}{\alpha+\beta}k_1 + \frac{\beta}{\alpha+\beta}k_2 : k_1, k_2 \in \mathcal{K}\right\} = (\alpha+\beta)\mathcal{K}. \tag{19}$$

For the containment on the right-hand side of (18), since $L' + \rho\mathcal{K} = \mathbb{R}^n$, for any $x \in \mathbb{R}^n$ there is $y_2 \in L'$ such that $x \in y_2 + \rho\mathcal{K}$. Thus if $y \in \mathcal{K} + x$ then $y \in \mathcal{K} + \rho\mathcal{K} + y_2 = (1+\rho)\mathcal{K} + y_2$.

For the other containment, since $\mathbb{R}^n = -\mathbb{R}^n = -(L'+\rho\mathcal{K}) = L'-\rho\mathcal{K}$, there is $y_1 \in L'$ such that $x \in y_1 - \rho\mathcal{K}$, and thus $y_1 \in x + \rho\mathcal{K}$. Now if $y \in (1-\rho)\mathcal{K} + y_1$ then $y \in (1-\rho)\mathcal{K} + \rho\mathcal{K} + x = \mathcal{K} + x$. □

As an immediate corollary we see that if L', $\mathcal{K}$ and ρ satisfy the conditions of Proposition 3.1 and $L \subset \mathbb{R}^k$ is a discrete subset, then:

(1) $\forall x \in \mathbb{R}^n\ \exists x' \in L'$ such that $N(L,\mathcal{K},x) \le N(L,(1+\rho)\mathcal{K},x')$;
(2) $\forall x \in \mathbb{R}^n\ \exists x' \in L'$ such that $N(L,\mathcal{K},x) \ge N(L,(1-\rho)\mathcal{K},x')$.

Consequently, we have:

Lemma 3.2. *Let $L', \mathcal{K}$ and ρ satisfy the conditions of Proposition 3.1 and let $L \subset \mathbb{R}^n$ be a discrete subset. Then:*

(1) $\max_{x\in\mathbb{R}^n} N(L,\mathcal{K},x) \le \max_{x'\in L'} N(L,(1+\rho)\mathcal{K},x')$;
(2) $\min_{x\in\mathbb{R}^n} N(L,\mathcal{K},x) \ge \min_{x'\in L'} N(L,(1-\rho)\mathcal{K},x')$.

The following standard lemma will be useful. We give the proof for lack of a suitable reference.

Lemma 3.3. *Let $L \subset \mathbb{R}^n$ be a lattice and $\mathcal{D} \in \mathrm{Conv}_n$, and assume that $L + \beta\mathcal{D} = \mathbb{R}^n$ for some $\beta \in (0,1)$. Then*

$$(1-\beta)^n \frac{\mathrm{vol}(\mathcal{D})}{\mathrm{covol}(L)} \le |L \cap \mathcal{D}| \le (1+\beta)^n \frac{\mathrm{vol}(\mathcal{D})}{\mathrm{covol}(L)}. \tag{20}$$

Proof. Let $N_{\mathcal{D}} \stackrel{\mathrm{def}}{=} L \cap \mathcal{D}$, and let $\mathcal{V}$ be a fundamental domain for L contained in $\beta\mathcal{D}$; that is, a measurable set such that for each $x \in \mathbb{R}^n$ there is exactly one $\ell \in L$ for which $x \in \ell + \mathcal{V}$. Such a fundamental domain exists since $L + \beta\mathcal{D} = \mathbb{R}^n$. Define the sets

$$\mathcal{S}_+ \stackrel{\mathrm{def}}{=} N_{\mathcal{D}} + \mathcal{V}$$
$$\mathcal{S}_- \stackrel{\mathrm{def}}{=} N_{\mathcal{D}} + (-\mathcal{V}).$$

We have that $\mathrm{vol}(\mathcal{S}_+) = \mathrm{vol}(\mathcal{S}_-) = |N_{\mathcal{D}}|\mathrm{covol}(L)$. Thus, to establish (20), it suffices to show that

$$\mathcal{S}_+ \subseteq (1+\beta)\mathcal{D}$$
$$\mathcal{S}_- \supseteq (1-\beta)\mathcal{D}.$$

The inclusion $\mathcal{S}_+ \subseteq (1+\beta)\mathcal{D}$ follows from $N_{\mathcal{D}} \subset \mathcal{D}$, $\mathcal{V} \subseteq \beta\mathcal{D}$ and the convexity of $\mathcal{D}$, using (19). To see that $(1-\beta)\mathcal{D} \subseteq \mathcal{S}_-$, since $-\mathcal{V}$ is also a fundamental domain for L, for any $x \in (1-\beta)\mathcal{D}$ there is $y \in L$ such that $x \in y - \mathcal{V}$. Thus, $y \in x + \mathcal{V} \subset (1-\beta)\mathcal{D} + \beta\mathcal{D} = \mathcal{D}$, and consequently $y \in N_{\mathcal{D}}$. □

3.2. **From packing to smooth covering.** Our analysis of $\eta(\mathcal{K}, L(S))$ (the covering smoothness of a lattice, Definition 1.1) relies on the analysis of $\eta_{\mathbb{F}_p}(A, S)$ (the analogous discrete smoothness, Definition 2.1), where A is a discrete analogue of the projection of $\mathcal{K}$ modulo L, and S is a randomly chosen subspace of $\mathbb{F}_p^n \cong \mathcal{P}_L^{(\mathrm{disc})}$ of dimension r, where r will be carefully chosen.

We now derive our main technical statement from Theorem 2.2.

Theorem 3.4. *Let $n \geq 5$, let $\delta, \tau \in (0,1)$ and let p be a prime number satisfying $p > 64n/(\tau\delta)^2$. Let $L \subset \mathbb{R}^n$ be a lattice and let $\mathcal{K} \in \mathrm{Conv}_n$, and assume that there is some real number $1 < c < \frac{p}{2n}$ such that $\left(L, \left(1+\frac{c}{p}\right)\mathcal{K}\right)$ is a packing and $(L, c\mathcal{K})$ is a covering. Let $4 \leq r \leq n$ be an integer satisfying*

$$r > 3 + \log_p \frac{\mathrm{covol}(L)}{\mathrm{vol}(\mathcal{K})} + 3c\,\frac{n}{p\log p}\,, \tag{21}$$

and let $S \sim \mathrm{Uniform}\left(\mathrm{Gr}_{n,r}(\mathbb{F}_p)\right)$. Then

$$\Pr\left(\eta(\mathcal{K}, L(S)) \geq \tau + 8c\,\frac{n}{p}\right) < 2\delta. \tag{22}$$

Proof. Set $\rho \stackrel{\mathrm{def}}{=} \frac{c}{p}$, so that $\rho \in \left(0, \frac{1}{2n}\right)$ and $(\frac{L}{p}, \rho\mathcal{K})$ is a covering. Set $\mathcal{D} \stackrel{\mathrm{def}}{=} (1+\rho)\mathcal{K}$ and $\beta \stackrel{\mathrm{def}}{=} \frac{\rho}{1+\rho}$, so that $\beta\mathcal{D} = \rho\mathcal{K}$ and we can apply the right-hand side of (20) to obtain

$$\left|\frac{L}{p} \cap (1+\rho)\mathcal{K}\right| \leq (1+\beta)^n \cdot \frac{\mathrm{vol}(\mathcal{D})}{\mathrm{covol}(\frac{L}{p})} = (1+2\rho)^n \frac{\mathrm{vol}(\mathcal{K})}{\mathrm{covol}(L)} p^n. \tag{23}$$

Similarly, by setting $\mathcal{D} \stackrel{\mathrm{def}}{=} (1-\rho)\mathcal{K}$ and $\beta \stackrel{\mathrm{def}}{=} \frac{\rho}{1-\rho}$, we have

$$(1-2\rho)^n \frac{\mathrm{vol}(\mathcal{K})}{\mathrm{covol}(L)} p^n \leq \left|\frac{L}{p} \cap (1-\rho)\mathcal{K}\right|. \tag{24}$$

Write $L = g\mathbb{Z}^n$ and for any $S \in \mathrm{Gr}_{n,r}(\mathbb{F}_p)$, define $L(S)$ by (13) and define $\mathcal{P}_L^{(\mathrm{disc})}$ by (12), where the v_i are the columns of g. Denote by A_0 (respectively, A_1) the set of all points in $\mathcal{P}_L^{(\mathrm{disc})}$ covered by $L + (1-\rho)\mathcal{K}$ (respectively, $L + (1+\rho)\mathcal{K}$), viewed as elements of $\mathbb{F}_p^n$. Since L forms a packing with respect to $(1+\rho)\mathcal{K}$ (and also with respect to $(1-\rho)\mathcal{K}$), the restriction of the projection $\pi_L : \mathbb{R}^n \to \mathbb{T}_L$ to $(1+\rho)\mathcal{K}$ (and thus to $(1-\rho)\mathcal{K}$) is injective. Thus, by (23) and (24) we have

$$(1-2\rho)^n \frac{\mathrm{vol}(\mathcal{K})}{\mathrm{covol}(L)} p^n \leq |A_i| \leq (1+2\rho)^n \frac{\mathrm{vol}(\mathcal{K})}{\mathrm{covol}(L)} p^n, \quad i = 0, 1, \tag{25}$$

and each point in A_0 (or A_1) is covered exactly once.

For any $x \in \mathcal{P}_L^{(\mathrm{disc})}$ we have that

$$N(L(S), (1-\rho)\mathcal{K}, x) = |(x+S) \cap A_0|,$$
$$N(L(S), (1+\rho)\mathcal{K}, x) = |(x+S) \cap A_1|,$$

where, with some abuse of notation, on the left-hand side we treat x as a vector in $\mathbb{R}^n$ and on the right-hand side as an element of $\mathbb{F}_p^n \cong \mathcal{P}_L^{(\mathrm{disc})}$. Let

$$E_0 \stackrel{\mathrm{def}}{=} \left\{ S \in \mathrm{Gr}_{n,r}(\mathbb{F}_p) \ : \ \eta_{\mathbb{F}_p}(A_0, S) > \tau \right\} \tag{26}$$

$$E_1 \stackrel{\mathrm{def}}{=} \left\{ S \in \mathrm{Gr}_{n,r}(\mathbb{F}_p) \ : \ \eta_{\mathbb{F}_p}(A_1, S) > \tau \right\}, \tag{27}$$

and $E = E_0 \cup E_1$. For all $S \in E^c$ and $x \in \mathcal{P}_L^{(\mathrm{disc})}$ we have

$$\begin{aligned} N\left(L(S), (1-\rho)\mathcal{K}, x\right) &\geq (1-\tau)|S| \cdot |A_0| \cdot p^{-n} \\ &\geq (1-\tau)\frac{|S| \cdot (1-2\rho)^n \mathrm{vol}(\mathcal{K})}{\mathrm{covol}(L)} \\ &= (1-\tau)(1-2\rho)^n \frac{\mathrm{vol}(\mathcal{K})}{\mathrm{covol}(L(S))}, \end{aligned}$$

and

$$\begin{aligned} N(L(S), (1+\rho)\mathcal{K}, x) &\leq (1+\tau)|S| \cdot |A_1| \cdot p^{-n} \\ &\leq (1+\tau)\frac{|S| \cdot (1+2\rho)^n \mathrm{vol}(\mathcal{K})}{\mathrm{covol}(L)} \\ &= (1+\tau)(1+2\rho)^n \frac{\mathrm{vol}(\mathcal{K})}{\mathrm{covol}(L(S))}. \end{aligned}$$

Let $L' = \frac{1}{p}L = L + \mathcal{P}_L^{(\mathrm{disc})}$. By assumption, $(L', \rho\mathcal{K})$ is a covering. Thus, by part (2) of Lemma 3.2 we have that for all $S \in E^c$,

$$\begin{aligned} \min_{x \in \mathbb{R}^n} N(L(S), \mathcal{K}, x) &\geq \min_{x' \in L'} N\left(L(S), (1-\rho)\,\mathcal{K}, x'\right) \\ &= \min_{x' \in \mathcal{P}_L^{(\mathrm{disc})}} N(L(S), (1-\rho)\,\mathcal{K}, x') \\ &\geq (1-\tau)(1-2\rho)^n \frac{\mathrm{vol}(\mathcal{K})}{\mathrm{covol}(L(S))}, \end{aligned} \tag{28}$$

and

$$\begin{aligned} \max_{x \in \mathbb{R}^n} N(L(S), \mathcal{K}, x) &\leq \max_{x' \in L'} N\left(L(S), (1+\rho)\,\mathcal{K}, x'\right) \\ &= \max_{x' \in \mathcal{P}_L^{(\mathrm{disc})}} N\left(L(S), (1+\rho)\,\mathcal{K}, x'\right) \\ &\leq (1+\tau)(1+2\rho)^n \frac{\mathrm{vol}(\mathcal{K})}{\mathrm{covol}(L(S))}. \end{aligned} \tag{29}$$

Combining (28) and (29), we see that for any $S \in E^c$ we have

$$\begin{aligned}\eta(\mathcal{K}, L(S)) &= \sup_{x\in\mathbb{R}^n} \left| \frac{N(L(S), \mathcal{K}, x)}{\mathrm{vol}(\mathcal{K})/\mathrm{covol}(L(S))} - 1 \right| \\ &\le \max\left\{1-(1-\tau)(1-2\rho)^n, (1+\tau)(1+2\rho)^n - 1\right\} \\ &\le \max\left\{\tau + (1-\tau)2\rho n, \tau + (1+\tau)4\rho n\right\} \qquad (30) \\ &< \tau + 8\rho n,\end{aligned}$$

where in (30) we have used the basic bounds (for $0 < 2\rho < 1/n$)

$$\begin{aligned}1-(1-2\rho)^n &< 2n\rho, \qquad (31)\\ (1+2\rho)^n - 1 &< 4n\rho.\end{aligned}$$

Thus, we have shown that

$$\eta(\mathcal{K}, L(S)) < \tau + 8\rho n, \quad \forall S \in E^c. \qquad (32)$$

Using our assumption on r in (21) and the lower bound in (25), we have that for $i = 0, 1$,

$$\begin{aligned}r &> 3 + \log_p \frac{\mathrm{covol}(L)}{\mathrm{vol}(\mathcal{K})} + \frac{3\rho n}{\log p} \\ &\ge 3 + \log_p \left(\frac{p^n}{|A_i|}(1-2\rho)^n \right) + \frac{3\rho n}{\log p} \\ &= 3 + n - \log_p |A_i| + n\log_p(1-2\rho) + \frac{3\rho n}{\log p} \\ &\ge 3 + n - \log_p |A_i| \,.\end{aligned}$$

Here, we have used the inequality

$$-\log_p(1-2\rho) = \log_p\left(1 + \frac{2\rho}{1-2\rho}\right) \le \frac{1}{(1-2\rho)\log p} \cdot 2\rho < \frac{3\rho}{\log p},$$

where the last inequality follows from $\rho < 1/2n$ and $n \ge 5$. Thus, we may invoke Theorem 2.2 to obtain

$$\Pr(S \in E_i) < \delta, \quad i = 0, 1,$$

and therefore, by the union bound,

$$\Pr(S \in E) < 2\delta,$$

establishing our claim. □

In the sequel we will use the following convenient consequence of Theorem 3.4.

Corollary 3.5. *Let $n > 25$, $L \subset \mathbb{R}^n$ be a lattice with* $\mathrm{covol}(L) = 1$, *and $\delta, \tau \in (0,1)$. Also let $\mathcal{K} \in \mathrm{Conv}_n$ satisfy $\rho_{\mathcal{K}}(L) \leq \bar{\rho}$ for some $1 \leq \bar{\rho} < \left(\frac{2}{\delta}\right)^{\frac{n}{2}}$ and* $\mathrm{vol}(\mathcal{K}) > c_5 \bar{\rho}^6 \left(\frac{1}{\tau\delta}\right)^6 n^3$, *where $c_5 = e \cdot (128)^3$. Then, for any prime number p satisfying*

$$\max\left\{\frac{64\bar{\rho}^2 n}{(\tau\delta)^2}, \left((2.5)^{-n} \cdot \mathrm{vol}(\mathcal{K})\right)^{1/3}\right\} < p < (e^{-1} \cdot \mathrm{vol}(\mathcal{K}))^{1/3}, \tag{33}$$

denoting $r = 3 + \left\lceil \frac{n \log 3\bar{\rho}}{\log p} \right\rceil$, we have that for $S \sim \mathrm{Uniform}\left(\mathrm{Gr}_{n,r}(\mathbb{F}_p)\right)$ (so that $\mathrm{covol}(p^{r/n} L(S)) = 1$*),*

$$\Pr\left(\eta(\mathcal{K}, p^{r/n} L(S)) \geq 2\tau\right) < 2\delta. \tag{34}$$

We remark that the statement is not vacuous, i.e., there exists a prime number p satisfying (33). To see this, note that

$$\begin{aligned}
&\frac{(e^{-1} \cdot \mathrm{vol}(\mathcal{K}))^{1/3}}{\max\left\{\frac{64\bar{\rho}^2 n}{(\tau\delta)^2}, ((2.5)^{-n} \cdot \mathrm{vol}(\mathcal{K}))^{1/3}\right\}} \\
&= \min\left\{\frac{(e^{-1} \cdot \mathrm{vol}(\mathcal{K}))^{1/3}}{\frac{64\bar{\rho}^2 n}{(\tau\delta)^2}}, \frac{(e^{-1} \cdot \mathrm{vol}(\mathcal{K}))^{1/3}}{((2.5)^{-n} \cdot \mathrm{vol}(\mathcal{K}))^{1/3}}\right\} \geq 2,
\end{aligned}$$

and therefore, by Bertrand's postulate, there must exist a prime number satisfying (33). Recalling that $p > \frac{64\bar{\rho}^2 n}{(\tau\delta)^2} > (3\bar{\rho})^2$, it also holds that $r < n$ since

$$\frac{n \log 3\bar{\rho}}{\log p} \leq \frac{n \log 3\bar{\rho}}{2 \log 3\bar{\rho}} = \frac{n}{2}.$$

Proof of Corollary 3.5. We show that with the parameters above, the conditions of Theorem 3.4 hold for the lattice $p^{r/n} L$ with $c = 3p^{\frac{1}{n}} \bar{\rho}^2$. To that end, first note that $p > \frac{64\bar{\rho}^2 n}{(\tau\delta)^2} \geq \frac{64n}{(\tau\delta)^2}$ by definition. Furthermore,

we have that

$$\begin{aligned}\frac{8cn}{p} &= 24\bar{\rho}^2 p^{-(1-\frac{1}{n})} n \\ &\leq 24\bar{\rho}^2 \left(\frac{64\bar{\rho}^2 n}{(\tau\delta)^2}\right)^{-(1-\frac{1}{n})} n \\ &= \frac{24\bar{\rho}^{\frac{2}{n}} n^{1/n}}{64^{1-1/n}} (\tau\delta)^{2(1-\frac{1}{n})} \\ &< \frac{\bar{\rho}^{\frac{2}{n}}}{2} (\tau\delta)^{2(1-\frac{1}{n})} \\ &< \frac{\left(\bar{\rho}\delta^{\frac{n}{2}}\right)^{\frac{2}{n}}}{2}\tau \\ &< \tau, \end{aligned} \tag{35}$$

and in particular, this implies that $c < \frac{p}{2n}$. Next we lower bound the packing radius as

$$\begin{aligned}\mathrm{r}_{\mathrm{pack},\mathcal{K}}(p^{\frac{r}{n}}L) &= p^{\frac{r}{n}}\,\mathrm{r}_{\mathrm{pack},\mathcal{K}}(L) \geq p^{\frac{3}{n}} 3\bar{\rho}\mathrm{r}_{\mathrm{pack},\mathcal{K}}(L) \geq 3p^{\frac{3}{n}}\mathrm{r}_{\mathrm{cov},\mathcal{K}}(L) \\ &\geq 3p^{\frac{3}{n}}\left(\frac{1}{\mathrm{vol}(\mathcal{K})}\right)^{\frac{1}{n}} = 3\left(\frac{p^3}{\mathrm{vol}(\mathcal{K})}\right)^{\frac{1}{n}} > \frac{3}{2.5} \overset{(35)}{>} 1 + \frac{c}{p}, \end{aligned} \tag{36}$$

and upper bound the covering radius as

$$\begin{aligned}\mathrm{r}_{\mathrm{cov},\mathcal{K}}(p^{\frac{r}{n}}L) &= p^{\frac{r}{n}}\,\mathrm{r}_{\mathrm{cov},\mathcal{K}}(L) \leq 3p^{\frac{4}{n}}\mathrm{r}_{\mathrm{cov},\mathcal{K}}(L)\bar{\rho} \leq 3p^{\frac{4}{n}}\bar{\rho}^2\mathrm{r}_{\mathrm{pack},\mathcal{K}}(L) \\ &\leq 3p^{\frac{4}{n}}\bar{\rho}^2\left(\frac{1}{\mathrm{vol}(\mathcal{K})}\right)^{\frac{1}{n}} = 3p^{\frac{1}{n}}\bar{\rho}^2\left(\frac{p^3}{\mathrm{vol}(\mathcal{K})}\right)^{\frac{1}{n}} \leq 3p^{\frac{1}{n}}\bar{\rho}^2 e^{-\frac{1}{n}} < c. \end{aligned} \tag{37}$$

Finally, we have that

$$\begin{aligned} r &= \log_p \mathrm{covol}(p^{r/n}L) \\ &= \log_p \frac{\mathrm{covol}(p^{r/n}L)}{\mathrm{vol}(\mathcal{K})} + \log_p \mathrm{vol}(\mathcal{K}) \\ &\overset{(33)}{\geq} \log_p \frac{\mathrm{covol}(p^{r/n}L)}{\mathrm{vol}(\mathcal{K})} + 3 + \log_p(e) \\ &> 3 + \log_p \frac{\mathrm{covol}(p^{r/n}L)}{\mathrm{vol}(\mathcal{K})} + 3c\,\frac{n}{p\log p}, \end{aligned}$$

where we have used the fact that $\frac{3cn}{p} < 1$, due to (35), in the last inequality. Therefore, the conditions of Theorem 3.4 apply to the

lattice $p^{r/n}L$ and the convex body $\mathcal{K}$, with $c = 3p^{\frac{1}{n}}\bar{\rho}^2$. Thus, for $S \sim \text{Uniform}\left(\text{Gr}_{n,r}(\mathbb{F}_p)\right)$, we have that

$$\Pr\left(\eta(\mathcal{K}, p^{r/n}L(S)) \geq \tau + 8\frac{cn}{p}\right) < 2\delta.$$

The statement in (34) follows since $8\frac{cn}{p} < \tau$ by (35). □

To prove Theorem 1.2, we will also need the following auxiliary statement, proved in §3.3. Recall that μ_n denotes the Haar-Siegel probability measure.

Proposition 3.6. *For $L \sim \mu_n$, any convex body $\mathcal{K} \in \text{Conv}_n$, and any $\alpha > 0$,*

$$\Pr(\rho_{\mathcal{K}}(L) \geq 2 \cdot \alpha^2) < 3 \cdot \left(\frac{2}{\alpha}\right)^n.$$

Proof of Theorem 1.2 (assuming Proposition 3.6). Let $L' \sim \mu_n$. Recall from [ORW21, Prop. 2.1] that for any fixed prime p and any $1 \leq r \leq n$, if we sample S according to the uniform distribution on $\text{Gr}_{n,r}(\mathbb{F}_p)$, statistically independent of L', the lattice $L = p^{r/n}L'(S)$ will also be distributed according to μ_n. Thus, for $L \sim \mu_n$ and any $\tau \in (0,1)$,

$$\Pr(\eta(\mathcal{K}, L) \geq 2\tau) = \Pr(\eta(\mathcal{K}, p^{r/n}L'(S)) \geq 2\tau).$$

We proceed to upper bound the right hand side of the above expression, using Corollary 3.5. Let $\bar{\rho} = 8 \cdot \left(\frac{50}{\delta}\right)^{\frac{2}{n}}$ (note that $\bar{\rho} < \left(\frac{2}{\delta}\right)^{\frac{n}{2}}$ for $n > 25$), and let E be the set of all lattices L' with unit covolume for which $\rho_{\mathcal{K}}(L') < \bar{\rho}$. Applying Proposition 3.6 with $\alpha = 2\left(\frac{50}{\delta}\right)^{\frac{1}{n}}$, we have that $\Pr(L' \in E^c) < 0.06\delta$. Now, applying Corollary 3.5 with $\delta' = 0.47\delta$, $\tau = \varepsilon/2$, we see that for any $\mathcal{K} \in \text{Conv}_n$ with

$$\begin{aligned}\text{vol}(\mathcal{K}) &> \left(\frac{2}{0.47}\right)^6 c_5 \bar{\rho}^6 \left(\frac{1}{\varepsilon\delta}\right)^6 n^3 \\ &= \left(\frac{2}{0.47}\right)^6 \cdot 8^6 \cdot 50^{\frac{12}{n}} \cdot c_5 \cdot \left(\frac{1}{\delta}\right)^{\frac{12}{n}} \left(\frac{1}{\varepsilon\delta}\right)^6 n^3, \qquad (38)\end{aligned}$$

there is a prime number p and an integer $3 < r < n$ for which

$$\Pr\left(\eta(\mathcal{K}, p^{r/n}L'(S)) \geq \varepsilon \mid L' \in E\right) < 0.94\delta.$$

In particular, this holds for any $\mathcal{K} \in \text{Conv}_n$ with $\text{vol}(\mathcal{K}) > c_1\left(\frac{1}{\varepsilon\delta}\right)^{6.5} n^3$, since $c_1\left(\frac{1}{\varepsilon\delta}\right)^{6.5} n^3$ is greater than the right hand side of (38). Our claim

now follows since

$$\begin{aligned}\Pr\left(\eta(\mathcal{K},L)\geq\varepsilon\right)&=\Pr\left(\eta(\mathcal{K},p^{r/n}L'(S))\geq\varepsilon\right)\\&\leq\Pr(L'\in E^c)+\Pr\left(\eta(\mathcal{K},p^{r/n}L'(S))\geq\varepsilon\mid L'\in E\right)\\&<0.06\delta+0.94\delta.\end{aligned}$$

□

Remark 3.7. *Improved bounds in Theorem 2.2 will result in tighter upper bounds on the minimal required volume for smooth covering. Specifically, assume the following holds: for n large enough, $\delta,\tau\in(0,1)$ any prime $p>p^*$ and any $A\subset\mathbb{F}_p^n$ and $r>m_*+(n-\log_p|A|)$, the conclusion of Theorem 2.2 holds. Then, roughly speaking, the proof we give for Theorem 1.2, with simple modifications, shows that there is a constant $c>0$, such that* (2) *holds for any convex body $\mathcal{K}$ for which $\mathrm{vol}(\mathcal{K})\geq c\cdot(p_*)^{m_*}$, as long as $p_*=\Omega(n)$.*

On the other hand, it follows from [CFR59] *that there exists $\mathcal{K}\in\mathrm{Conv}_n$ with volume $\Omega(n)$ such that $\eta(\mathcal{K},L)\geq1$ for all unit covolume lattices. This gives an obvious bound on the extent to which Theorem 1.2 can be improved. Namely, if one can prove that* (17) *holds for fixed $0<\delta,\tau<1$, $p_*\asymp n$ and m_* arbitrarily close to 1, this will show that the lower bound in* [CFR59] *is essentially tight, and is attained for a "typical" lattice (and even for $\eta<1$, i.e., with smooth covering).*

For the proof of Theorem 1.4 we will also need the following statement, proved in §3.4.

Lemma 3.8. *For any lattice $L\subset\mathbb{R}^n$, convex set $\mathcal{K}\in\mathrm{Conv}_n$, and positive integer m, we have*

$$\eta(m\mathcal{K},L)\leq\eta(\mathcal{K},L).$$

Proof of Theorem 1.4 (assuming Lemma 3.8). Let

$$M=c_5\cdot4^6\cdot\left(\frac{1}{\varepsilon\delta}\right)^6n^{3(1+2b)}=c_3\left(\frac{1}{\varepsilon\delta}\right)^6n^{3(1+2b)},$$

so that by assumption we have $\mathrm{vol}(\mathcal{K})\geq M$. By Lemma 3.8, replacing $\mathcal{K}$ if necessary with $\frac{1}{a}\mathcal{K}$ for some integer $a\geq2$, we may further assume $\mathrm{vol}(\mathcal{K})\in[M,2^nM)$. We apply Corollary 3.5 with $L=\mathbb{Z}^n$, $\bar{\rho}=n^b$, $\delta'=\delta/2$ and $\tau=\epsilon/2$. It is straightforward to verify that p satisfies (33) for $\mathrm{vol}(\mathcal{K})\in[M,2^nM)$, and the conditions on $\mathrm{vol}(\mathcal{K})$ and r also trivially hold. Thus, recalling that $p^{r/n}L(S)=p^{r/n}\mathbb{Z}^n(S)$ is distributed as a lattice drawn from the (p,r) random construction A ensemble, we obtain the required statement. □

3.3. **High probability bounds on $\rho_{\mathcal{K}}(L)$.** In this subsection we will give a simple proof of Proposition 3.6. The first results showing the existence of a global constant $c > 0$, independent of the dimension n, such that for any $\mathcal{K} \in \mathrm{Conv}_n$ there is a lattice L such that $\rho_{\mathcal{K}}(L) < c$, are due to Butler [But72] and Bourgain [Bou87]. The probability (with respect to the Siegel-Haar measure) that a randomly chosen lattice satisfies $\rho_{\mathcal{K}}(L) < c$ was not discussed in these papers. Using [ORW21, Cor. 1.6] together with the bound $\mathrm{vol}(\mathcal{K} - \mathcal{K}) \leq \mathrm{vol}(4\mathcal{K})$ proved in [RS57], one sees that $\Pr\left(\rho_{\mathcal{K}}(L) > 4 + o(1)\right)$ vanishes exponentially fast with n. However, we can give a much simpler proof, albeit with a worse constant. Note that the value of the constant has small effect on the bounds we obtain for the covering smoothness.

Proof of Proposition 3.6. We will derive a high-probability lower bound on $\mathrm{r}_{\mathrm{pack},\mathcal{K}}(L)$ and a high-probability upper bound on $\mathrm{r}_{\mathrm{cov},\mathcal{K}}(L)$. Assume without loss of generality that $\mathrm{vol}(\mathcal{K}) = 1$. Denote

$$N^*(L, \mathcal{K}, x) \stackrel{\mathrm{def}}{=} |((L \setminus \{0\}) - x) \cap \mathcal{K}| = |\{y \in L \setminus \{0\} \ : \ x \in y - \mathcal{K}\}|.$$

For lower bounding $\mathrm{r}_{\mathrm{pack},\mathcal{K}}(L)$, let $\mathcal{K}_0 = \frac{1}{2\alpha}\mathcal{K}$ and let $N^*(L, \mathcal{K}_0 - \mathcal{K}_0, 0)$ be the number of non-zero points of the lattice L in $\mathcal{K}_0 - \mathcal{K}_0$. By Siegel's theorem [Sie45], we have

$$\mathbb{E}[N^*(L, \mathcal{K}_0 - \mathcal{K}_0, 0)] = \mathrm{vol}(\mathcal{K}_0 - \mathcal{K}_0).$$

Thus, by Markov's inequality,

$$\begin{aligned} \Pr(N^*(L, \mathcal{K}_0 - \mathcal{K}_0, 0) \neq 0) &= \Pr(N^*(L, \mathcal{K}_0 - \mathcal{K}_0, 0) \geq 1) \\ &\leq \mathbb{E}[N^*(L, \mathcal{K}_0 - \mathcal{K}_0, 0)] \\ &= \mathrm{vol}(\mathcal{K}_0 - \mathcal{K}_0) \\ &\leq \mathrm{vol}(4\mathcal{K}_0) = \left(\frac{4}{2\alpha}\right)^n, \end{aligned} \tag{39}$$

where the last inequality in (39) follows from [RS57, Theorem 1]. Now, since $N^*(L, \mathcal{K}_0 - \mathcal{K}_0, 0) = 0$ implies that L forms a packing with respect to $\mathcal{K}_0$, we see that

$$\Pr\left(\mathrm{r}_{\mathrm{pack},\mathcal{K}}(L) \leq \frac{1}{2\alpha}\right) \leq \left(\frac{2}{\alpha}\right)^n. \tag{40}$$

Recall that m_L denotes the Haar measure on $\mathbb{T}_L = \mathbb{R}^n/L$. For the upper bound on the covering radius recall the basic fact (see, e.g., [ORW21, Lemma 2.5]) that

$$m_L\left(\pi_L\left(\frac{\alpha}{2}\mathcal{K}\right)\right) > \frac{1}{2} \implies \mathrm{r}_{\mathrm{cov},\mathcal{K}}(L) \leq \alpha.$$

It therefore only remains to upper bound $\Pr\left(m_L(\pi_L(\mathcal{K}_1)) \leq 1/2\right)$, where $\mathcal{K}_1 = \frac{\alpha}{2}\mathcal{K}$. We do this by showing that $\mathbb{E}[m_L(\pi_L(\mathcal{K}_1))]$ is close to 1. We begin by noting that

$$\begin{aligned} m_L(\pi_L(\mathcal{K}_1)) &= \int_{x\in\mathcal{K}_1} \frac{1}{|(x+L)\cap\mathcal{K}_1|}dx \\ &= \int_{x\in\mathcal{K}_1} \frac{1}{1+N^*(L,\mathcal{K}_1,-x)}dx. \end{aligned}$$

Since the function $t \mapsto \frac{1}{1+t}$ is convex in the regime $t > 0$, we can apply Jensen's inequality and obtain

$$\begin{aligned} \mathbb{E}[m_L(\pi_L(\mathcal{K}_1))] &= \mathbb{E}\left[\int_{x\in\mathcal{K}_1} \frac{1}{1+N^*(L,\mathcal{K}_1,-x)}dx\right] \\ &= \int_{x\in\mathcal{K}_1} \mathbb{E}\left[\frac{1}{1+N^*(L,\mathcal{K}_1,-x)}\right]dx \qquad (41) \\ &\geq \int_{x\in\mathcal{K}_1} \frac{1}{1+\mathbb{E}\left[N^*(L,\mathcal{K}_1,-x)\right]}dx \qquad (42) \\ &= \int_{x\in\mathcal{K}_1} \frac{1}{1+\mathrm{vol}(\mathcal{K}_1)}dx \qquad (43) \\ &= \frac{\mathrm{vol}(\mathcal{K}_1)}{1+\mathrm{vol}(\mathcal{K}_1)}, \qquad (44) \end{aligned}$$

where (41) follows from Fubini's Theorem, (42) from Jensen's inequality and (43) from Siegel's summation formula. Let

$$P_e = \Pr\left(m_L(\pi_L(\mathcal{K}_1)) \leq \frac{1}{2}\right).$$

Since $m_L(\pi_L(\mathcal{K}_1)) \leq 1$ we have that

$$\mathbb{E}[m_L(\pi_L(\mathcal{K}_1))] \leq \frac{P_e}{2} + (1-P_e) = 1 - \frac{P_e}{2}.$$

Combining this with (44), we obtain

$$P_e \leq 2\left(1 - \frac{\mathrm{vol}(\mathcal{K}_1)}{1+\mathrm{vol}(\mathcal{K}_1)}\right) < \frac{2}{\mathrm{vol}(\mathcal{K}_1)}.$$

Thus,

$$\Pr(\mathrm{r}_{\mathrm{cov},\mathcal{K}}(L) \geq \alpha) < 2\cdot\left(\frac{2}{\alpha}\right)^n. \qquad (45)$$

Combining (40) and (45) we obtain the claimed result. □

3.4. **On the monotonicity of $\alpha \mapsto \eta(\alpha\mathcal{K}, L)$.** As mentioned above, the mapping $\alpha \mapsto \eta(\alpha\mathcal{K}, L)$ is not monotonically non-increasing in general. Nevertheless, Lemma 3.8, stated above, shows that for dilates by positive integers, the covering smoothness can only decrease. We can exploit this fact to establish Theorems 1.3 and 1.6, which show that for any $\mathcal{K} \in \mathrm{Conv}_n$ with sufficiently large (polynomial) volume, a typical lattice has small $\eta(\alpha\mathcal{K}, L)$ for all $\alpha \geq 1$. We first provide the proof of Lemma 3.8, and then leverage this result and prove Theorems 1.3 and 1.6.

Proof of Lemma 3.8. We can write

$$N(L, m\mathcal{K}, x) = N\left(\frac{L}{m}, \mathcal{K}, \frac{x}{m}\right) = \sum_a N\left(L, \mathcal{K}, \frac{x}{m} - a\right) ,$$

where the sums runs over all coset representatives a for the inclusion $L \subset \frac{L}{m}$. We therefore have

$$\begin{aligned}
\eta(m\mathcal{K}, L) &= \sup_{x\in\mathbb{R}^n} \left| \frac{N(L, m\mathcal{K}, x)}{\mathrm{vol}(m\mathcal{K})/\mathrm{covol}(L)} - 1 \right| \\
&= \sup_{x\in\mathbb{R}^n} \left| m^{-n} \sum_a \left(\frac{N(L, \mathcal{K}, x/m - a)}{\mathrm{vol}(\mathcal{K})/\mathrm{covol}(L)} - 1 \right) \right| \\
&\leq m^{-n} \sup_{x\in\mathbb{R}^n} \sum_a \left| \frac{N(L, \mathcal{K}, x/m - a)}{\mathrm{vol}(\mathcal{K})/\mathrm{covol}(L)} - 1 \right| \\
&\leq m^{-n} \sum_a \sup_{x\in\mathbb{R}^n} \left| \frac{N(L, \mathcal{K}, x/m - a)}{\mathrm{vol}(\mathcal{K})/\mathrm{covol}(L)} - 1 \right| = \eta(\mathcal{K}, L) .
\end{aligned}$$

□

Using this weak monotonicity property, we now show that if a lattice L smoothly covers $\mathbb{R}^n$ with respect to $\alpha_i\mathcal{K}$ for all α_i in a dense enough net in $[1, 2)$, it must smoothly cover $\mathbb{R}^n$ with respect to $\alpha\mathcal{K}$ for all $\alpha \geq 1$.

Lemma 3.9. *Let $n \in \mathbb{N}$ and $0 < \varepsilon < 1$. Let $\beta = \frac{\varepsilon}{8n}$ and $I = \left\lceil \frac{\log 2}{\log(1+\beta)} \right\rceil$. Define $\alpha_i = (1+\beta)^i$ for all $i = 0, 1, \ldots, I$, such that $\alpha_0 = 1$, and $\alpha_I \geq 2$. For a lattice $L \subset \mathbb{R}^n$ and $\mathcal{K} \in \mathrm{Conv}_n$ assume that $\eta(\alpha_i\mathcal{K}, L) \leq \varepsilon/2$ for all $i = 0, 1, \ldots, I$. Then $\eta(\alpha\mathcal{K}, L) < \varepsilon$ for all $\alpha \geq 1$.*

Proof. Note that for any $\alpha \in [1,2)$ there is $i \in \{1,\dots,I\}$ such that $\alpha_{i-1} \le \alpha \le \alpha_i$. We therefore have that for any $x \in \mathbb{R}^n$,

$$\begin{aligned}\frac{N(L,\alpha\mathcal{K},x)}{\mathrm{vol}(\alpha\mathcal{K})/\mathrm{covol}(L)} &\le \frac{\mathrm{vol}(\alpha_i\mathcal{K})}{\mathrm{vol}(\alpha\mathcal{K})}\frac{N(L,\alpha_i\mathcal{K},x)}{\mathrm{vol}(\alpha_i\mathcal{K})/\mathrm{covol}(L)}\\ &\le (1+\beta)^n\left(1+\frac{\varepsilon}{2}\right) < (1+\varepsilon),\end{aligned}$$

where in the last inequality we used the fact that $(1+\beta)^n \le e^{\beta n} \le 1+2\beta n = 1+\frac{\varepsilon}{4}$, which follows since $e^t < 1+2t$ for $t < 1/2$. Similarly,

$$\begin{aligned}\frac{N(L,\alpha\mathcal{K},x)}{\mathrm{vol}(\alpha\mathcal{K})/\mathrm{covol}(L)} &\ge \frac{\mathrm{vol}(\alpha_{i-1}\mathcal{K})}{\mathrm{vol}(\alpha\mathcal{K})}\frac{N(L,\alpha_{i-1}\mathcal{K},x)}{\mathrm{vol}(\alpha_{i-1}\mathcal{K})/\mathrm{covol}(L)}\\ &\ge (1+\beta)^{-n}\left(1-\frac{\varepsilon}{2}\right) > (1-\varepsilon),\end{aligned}$$

where, as above, in the last inequality we used the fact that $(1+\beta)^{-n} \ge \frac{1}{1+2\beta n} \ge 1-2\beta n = 1-\frac{\varepsilon}{4}$. Thus, $\eta(\alpha\mathcal{K},L) < \varepsilon$ for all $\alpha \in [1,2)$. Finally, for any $\alpha \ge 1$ there is a positive integer m such $\alpha' = \alpha/m \in [1,2)$, and thus, by Lemma 3.8, $\eta(\alpha\mathcal{K},L) < \varepsilon$. □

Proof of Theorem 1.3. Assume $\mathrm{vol}(\mathcal{K}) = c_2\left(\frac{1}{\varepsilon^2\delta}\right)^{6.5} n^3$. Let

$$\beta = \frac{\varepsilon}{8n} \text{ and } I = \left\lceil \frac{\log 2}{\log(1+\beta)} \right\rceil \le \frac{8n}{\varepsilon} - 1.$$

Define $\alpha_i = (1+\beta)^i$ for all $i = 0,1,\dots,I$ and note that

$$\alpha_i^n \ge e^{\frac{\varepsilon}{9}i}. \tag{46}$$

Indeed,

$$(1+\beta)^n = \left(1+\frac{\varepsilon}{8n}\right)^n = e^{n\log(1+\frac{\varepsilon}{8n})} \ge e^{n\frac{\varepsilon/8n}{1+\varepsilon/8n}} = e^{\frac{\varepsilon/8}{1+\varepsilon/8n}} > e^{\frac{\varepsilon/8}{9/8}} = e^{\frac{\varepsilon}{9}}.$$

For all $i = 0,1,\dots,I$ we apply Theorem 1.2 with $\varepsilon' = \varepsilon/2$ and $\delta_i = \frac{\delta\varepsilon}{64}\cdot e^{-\frac{\varepsilon}{60}i}$ and $\mathcal{K}_i = \alpha_i\mathcal{K}$. Noting that

$$c_1\left(\frac{1}{\varepsilon'\delta_i}\right)^{6.5} n^3 < (128)^{6.5}c_1\left(\frac{1}{\varepsilon^2\delta}\right)^{6.5} e^{\frac{\varepsilon}{9}i}n^3 \overset{(46)}{<} \alpha_i^n c_2\left(\frac{1}{\varepsilon^2\delta}\right)^6 n^3 \le \mathrm{vol}(\mathcal{K}_i),$$

the theorem implies that

$$\Pr\left(\eta(\alpha_i\mathcal{K},L) \ge \frac{\varepsilon}{2}\right) < \delta_i, \quad \forall i = 0,1,\dots,I. \tag{47}$$

Let E be the set of all unit covolume lattices such that $\eta(\alpha_i\mathcal{K}, L) < \varepsilon/2$ for all $i = 0, 1, \ldots, I$. By the union bound and (47), we have that

$$\begin{aligned}\Pr(L \notin E) &\le \sum_{i=0}^{I} \delta_i = \frac{\delta\varepsilon}{64} \sum_{i=0}^{I} e^{-\frac{\varepsilon}{60}i} < \frac{\delta\varepsilon}{64} \sum_{i=0}^{\infty} e^{-\frac{\varepsilon}{60}i} = \frac{\delta\varepsilon}{64} \frac{1}{1 - e^{-\frac{\varepsilon}{60}}} \\ &\le \frac{\delta\varepsilon}{64}\left(1 + \frac{60}{\varepsilon}\right) < \delta,\end{aligned}$$

where we have used the fact that $e^{-x} \le \frac{1}{1+x}$ for $x \ge 0$. Our claim now follows by applying Lemma 3.9. □

Proof of Theorem 1.6. Assume $\mathrm{vol}(\mathcal{K}) = c_4 \left(\frac{1}{\varepsilon^2\delta}\right)^6 n^{9+6b}$. Let $\beta = \frac{\varepsilon}{8n}$ and $I = \left\lceil \frac{\log 2}{\log(1+\beta)} \right\rceil \le \frac{8n}{\varepsilon} - 1$. Define $\alpha_i = (1+\beta)^i$ for all $i = 0, 1, \ldots, I$. For all $i = 0, 1, \ldots, I$ we apply Theorem 1.4 with $\varepsilon' = \varepsilon/2$ and $\delta' = \delta/(I+1)$ and $\mathcal{K}' = \alpha_i\mathcal{K}$. Noting that $\varepsilon'\delta' \ge \frac{\varepsilon^2\delta}{16n}$ and that

$$c_3 \left(\frac{1}{\varepsilon'\delta'}\right)^6 n^{3(1+2b)} \le c_4 \left(\frac{1}{\varepsilon^2\delta}\right)^6 n^{9+6b} \le \mathrm{vol}(\mathcal{K}'),$$

the theorem implies that

$$\Pr(\eta(\alpha_i\mathcal{K}, p^{r/n}L) \ge \varepsilon/2) < \frac{\delta}{I+1}, \quad \forall i = 0, 1, \ldots, I. \tag{48}$$

Let E be the set of all (p, r) construction A lattices such that

$$\eta(\alpha_i\mathcal{K}, p^{r/n}L) < \frac{\varepsilon}{2}, \quad \text{for } i = 0, 1, \ldots, I.$$

By the union bound and (48), we have that $\Pr(L \notin E) < \delta$. Our claim now follows by applying Lemma 3.9. □

3.5. **Non-lattice smooth coverings.** In this subsection we will prove Theorem 1.7. The proof follows the same outline and notation as the proof of Theorem 3.4. In the previous sections we started with a lattice L with a reasonable $\rho_{\mathcal{K}}(L)$ and constructed from it a denser lattice $L(S)$ by choosing $S \subset \mathbb{F}_p^n$ to be a subspace. The work of Dhar and Dvir [DD22] was then used to show that for any subset $A \in \mathbb{F}_p^n$, and a randomly uniform subspace $S \in \mathbb{F}_p^n$, if p is sufficiently large and $\frac{|S|\cdot|A|}{p^n} > p^3$, then $\eta_{\mathbb{F}_p}(A, S)$ is small with high probability. This was then leveraged for showing that under suitable conditions a randomly chosen subspace S will yield a lattice $L(S)$ such that $L(S)+\mathcal{K}$ smoothly covers $\mathbb{R}^n$. Note that if $S \subset \mathbb{F}_p^n$ is not a subspace, the discrete set $L(S)$, as given in (13) is not a lattice, but is nevertheless well defined, and has asymptotic density $\frac{|S|}{\mathrm{covol}(L)}$. Furthermore, recall that the definition of $\eta_{\mathbb{F}_p}(A, S)$ does not require S to be a subspace. For a random set

S (rather than a random subspace, as in [DD22]), controlling the tail of $\eta_{\mathbb{F}_p}(A,S)$ is a significantly simpler task. The following result easily follows from large deviation theory.

Lemma 3.10. *Let n,m be positive integers, p be a prime number and let $\delta,\tau \in (0,1)$. Let S be a set of m points identically distributed independently uniformly over $\mathbb{F}_p^n$. Then, for any set $A \subset \mathbb{F}_p^n$, we have that if $\frac{m|A|}{p^n} > \frac{3}{\tau^2}\left(n\log p - \log\frac{\delta}{2}\right)$, then*

$$\Pr(\eta_{\mathbb{F}_p}(A,S) \geq \tau \text{ or } |S| \neq m) \leq \delta + m^2 p^{-n}.$$

The lemma follows easily from the following well-known large deviations bound, see e.g., [MU17, Corollary 4.6].

Proposition 3.11 (Chernoff bound)**.** *For any $\eta \in (0,1)$ and any m identically distributed independent Bernoulli random variables $Y_1,\ldots,Y_m$, the sum $Y \stackrel{\text{def}}{=} \sum_{i=1}^m Y_i$ satisfies*

$$\Pr\left(|Y-\mu| \geq \eta\mu\right) \leq 2e^{-\frac{\eta^2\mu}{3}}, \tag{49}$$

where $\mu \stackrel{\text{def}}{=} \mathbb{E}(Y)$.

Proof of Lemma 3.10. Let $X_i \overset{i.i.d}{\sim} \text{Uniform}(\mathbb{F}_p^n)$ for $i=1,\ldots,m$, and $S=\{X_1,\ldots,X_m\}$. For any $x \in \mathbb{F}_p^n$ let $Y_{i,x}$ be the indicator of the event that $x+X_i \in A$. We clearly have that the random variables $\{Y_{i,x}\}_{i=1}^m$ are i.i.d. Bernoulli with $\Pr(Y_{i,x}=1)=\frac{|A|}{p^n}$. Thus, $Y_x=\sum_{i=1}^m Y_{i,x}$ satisfies the conditions of Proposition 3.11, and applying it with $\mu=\mathbb{E}(Y_x)=\frac{m|A|}{p^n}$ and $\eta=\tau$, gives that if $\frac{m|A|}{p^n} > \frac{3}{\tau^2}\left(n\log p-\log\frac{\delta}{2}\right)$ then

$$\begin{aligned}&\Pr\left(\left|\frac{|(x+S)\cap A|}{m\cdot|A|p^{-n}}-1\right|\geq\tau\right)\\ &\quad=\Pr(|Y_x-\mu|\geq\tau\mu)\leq 2e^{-\frac{\tau^2}{3}\frac{3}{\tau^2}\left(n\log p-\log\frac{\delta}{2}\right)}=\delta\cdot p^{-n}.\end{aligned}$$

Applying the union bound, this implies that

$$\Pr\left(\max_{x\in\mathbb{F}_p^n}\left|\frac{|(x+S)\cap A|}{m\cdot|A|p^{-n}}-1\right|\geq\tau\right)\leq\delta.$$

Finally, noting that

$$\Pr(|S|\neq m)\leq\sum_{1\leq i<j\leq m}\Pr(X_i=X_j)=\binom{m}{2}p^{-n}<m^2p^{-n},$$

and applying the union bound again, we obtain the claimed result. □

Proof of Theorem 1.7. Let $\mathcal{K} \in \mathrm{Conv}_n$, $\frac{320n}{\tau} < p < \frac{640n}{\tau}$ be a prime number for some $\tau \in (0,1)$ to be chosen later, and $c = 40$. Let L be a lattice so that $(L, (1+\frac{c}{p})\mathcal{K})$ is a packing and $(L, c\mathcal{K})$ is a covering. Such a lattice exists by Proposition 3.6. Note further, that for such a lattice we have that $\frac{\mathrm{covol}(L)}{\mathrm{vol}(\mathcal{K})} < c^n = 40^n$. Denote $\rho = \frac{c}{p} < \frac{\tau}{8n}$, such that in particular $0 < \rho < \frac{1}{2n}$. We follow the derivations in the proof of Theorem 3.4 up to equation (32), where instead of assuming $S \in \mathrm{Gr}_{n,r}(\mathbb{F}_p)$, we assume $S \subset \mathbb{F}_p^n$ is an arbitrary subset of m points in $\mathbb{F}_p^n$. This derivation does not rely on S being a subspace and therefore holds verbatim, where the only difference is that we replace the definitions of the sets E_0 and E_1 from (26) and (27) with

$$E_0 \stackrel{\mathrm{def}}{=} \left\{ S \in \mathcal{R}_{m,n}(\mathbb{F}_p) \ : \ \eta_{\mathbb{F}_p}(A_0, S) > \tau \right\},$$
$$E_1 \stackrel{\mathrm{def}}{=} \left\{ S \in \mathcal{R}_{m,n}(\mathbb{F}_p) \ : \ \eta_{\mathbb{F}_p}(A_1, S) > \tau \right\},$$

where $\mathcal{R}_{m,n}(\mathbb{F}_p) = \{S \subset \mathbb{F}_p^n \ : \ |S| = m\}$. We therefore have that

$$\eta(\mathcal{K}, L(S)) \le \tau + 8\rho n \le 2\tau, \quad \forall S \in E^c. \tag{50}$$

We proceed to upper bound $\Pr(S \in E)$ for the case where S consists of m points drawn i.i.d. from the uniform distribution over $\mathbb{F}_p^n$. By (25), we have that for $i = 0, 1$

$$\frac{|A_i|}{p^n} \ge (1-2\rho)^n \frac{\mathrm{vol}(\mathcal{K})}{\mathrm{covol}(L)} \ge (1-2n\rho)\frac{\mathrm{vol}(\mathcal{K})}{\mathrm{covol}(L)} \ge \left(1 - \frac{\tau}{4}\right)\frac{\mathrm{vol}(\mathcal{K})}{\mathrm{covol}(L)}, \tag{51}$$

where the second inequality is due to (31), and the third follows since $\rho < \frac{\tau}{8n}$. Thus, by Lemma 3.10, for any $\delta \in (0,1)$, if

$$\left(1 - \frac{\tau}{4}\right) \cdot \mathrm{vol}(\mathcal{K}) \cdot \frac{m}{\mathrm{covol}(L)} > \frac{3}{\tau^2}\left(n \log p - \log \frac{\delta}{2}\right) \tag{52}$$

then $\Pr(E_i) < \delta + m^2 p^{-n}$ for $i = 1, 2$. We take $\tau = \varepsilon/2$ and $\delta = 2e^{-2}$ and choose

$$\begin{aligned} m &= \left\lceil \frac{\mathrm{covol}(L)}{\mathrm{vol}(\mathcal{K})} \frac{1}{\left(1 - \frac{\varepsilon}{8}\right)} \frac{12}{\varepsilon^2} \left(n \log p + 2\right) \right\rceil \\ &< \frac{\mathrm{covol}(L)}{\mathrm{vol}(\mathcal{K})} \frac{14}{\varepsilon^2} \left(n \log p + 2\right) \end{aligned}$$

to be the smallest integer satisfying the above constraint, so that $\Pr(E) \le 2\delta + 2m^2 p^{-n} = 4e^{-2} + 2m^2 p^{-n}$. Recalling that $\frac{\mathrm{covol}(L)}{\mathrm{vol}(\mathcal{K})} < 40^n$

and that $\frac{640n}{\varepsilon} \le p \le \frac{1280n}{\varepsilon}$ we see that

$$\begin{aligned} m^2 p^{-n} &\le 40^{2n} \frac{14^2}{\varepsilon^4} \left(n \log \frac{2560n}{\varepsilon} \right)^2 \left(\frac{640n}{\varepsilon} \right)^{-n} \\ &< 40^{2n} \frac{14^2}{\varepsilon^4} \left(\frac{2560n^2}{\varepsilon} \right)^2 \left(\frac{640n}{\varepsilon} \right)^{-n} \\ &< \left(\frac{40^2}{640} \right)^n \left(\frac{n}{\varepsilon} \right)^{-(n-6)} (14 \cdot 2560)^2 \end{aligned}$$

and this is smaller than 0.08 for all $n \ge 20$, and so $\Pr(E) \le 4e^{-2} + 2m^2 p^{-n} < 1$ for all $n \ge 20$. We therefore see that there exists a discrete set $L(S)$ with asymptotic density $D(L(S)) = \frac{m}{\operatorname{covol}(L)}$ such that

$$\operatorname{vol}(\mathcal{K}) D(L(S)) < \frac{14}{\varepsilon^2} (n \log p + 2) \tag{53}$$

and $\eta(\mathcal{K}, L(S)) < \varepsilon$. Recalling that $p < \frac{1280n}{\varepsilon}$, we obtain the claimed result. □

References

[BLRL+18] S. Bai, T. Lepoint, A. Roux-Langlois, A. Sakzad, D. Stehlé, and R. Steinfeld, *Improved security proofs in lattice-based cryptography: using the Rényi divergence rather than the statistical distance*, J. Cryptology **31** (2018), no. 2, 610–640. MR3771421

[Bou87] J. Bourgain, *On lattice packing of convex symmetric sets in* $\mathbf{R}^n$, Geometrical aspects of functional analysis (1985/86), 1987, pp. 5–12. MR907681

[But72] G. J. Butler, *Simultaneous packing and covering in Euclidean space*, Proc. London Math. Soc. (3) **25** (1972), 721–735. MR0319054

[CFR59] H. S. M. Coxeter, L. Few, and C. A. Rogers, *Covering space with equal spheres*, Mathematika **6** (1959), 147–157. MR124821

[CS88] J. H. Conway and N. J. A. Sloane, *Sphere packing, lattices and groups*, Grundlehren de mathemtische wissenschaften, vol. 290, Springer, 1988.

[DADRT23] T. Debris-Alazard, L. Ducas, N. Resch, and J.-P. Tillich, *Smoothing codes and lattices: Systematic study and new bounds*, IEEE Transactions on Information Theory **69** (2023), no. 9, 6006–6027.

[DD22] M. Dhar and Z. Dvir, *Linear hashing with* ℓ_∞ *guarantees and two-sided Kakeya bounds*, 2022 IEEE 63rd Annual Symposium on Foundations of Computer Science—FOCS 2022, 2022, pp. 419–428. arXiv:2204.01665. MR4537223

[ER62] P. Erdős and C. A. Rogers, *Covering space with convex bodies*, Acta Arith. **7** (1962), 281–285 (English).

[Loe97] H.-A. Loeliger, *Averaging bounds for lattices and linear codes*, IEEE Trans. Inform. Theory **43** (1997), no. 6, 1767–1773. MR1481036

[MR07] D. Micciancio and O. Regev, *Worst-case to average-case reductions based on Gaussian measures*, SIAM J. Comput. **37** (2007), no. 1, 267–302. MR2306293

[MU17] M. Mitzenmacher and E. Upfal, *Probability and computing*, Second, Cambridge University Press, Cambridge, 2017. Randomization and probabilistic techniques in algorithms and data analysis. MR3674428

[ORW21] O. Ordentlich, O. Regev, and B. Weiss, *New bounds on the density of lattice coverings*, J. Amer. Math. Soc. **35** (2021), no. 1, 295–308. MR4322394

[Rog58] C. A. Rogers, *Lattice covering of space: The Minkowski-Hlawka theorem*, Proc. London Math. Soc. (3) **8** (1958), 447–465. MR0096639

[RS57] C. A. Rogers and G. C. Shephard, *The difference body of a convex body*, Arch. Math. (Basel) **8** (1957), 220–233. MR92172

[Sie45] C. L. Siegel, *A mean value theorem in geometry of numbers*, Ann. of Math. (2) **46** (1945), 340–347. MR0012093 (6,257b)

School of Computer Science and Engineering, Hebrew University

Courant Institute of Mathematical Sciences, New York University

School of Mathematical Sciences, Tel Aviv University