



Generalized Compact Knapsacks are Collision Resistant

Vadim Lyubashevsky Daniele Micciancio

University of California, San Diego
 9500 Gilman Drive, La Jolla, CA 92093-0404, USA
 {vlyubash,daniele}@cs.ucsd.edu

Abstract

The generalized knapsack problem is the following: given m random elements $a_1, \dots, a_m \in R$ for some ring R , and a target $t \in R$, find elements $z_1, \dots, z_m \in D$ such that $\sum a_i z_i = t$ where D is some given subset of R . In (Micciancio, FOCS 2002), it was proved that for appropriate choices of R and D , solving the generalized compact knapsack problem *on the average* is as hard as solving certain *worst-case* problems for cyclic lattices even for almost constant values of m . This immediately yields very efficient one-way functions whose security is based on worst-case hardness assumptions. A problem left open in (Micciancio, FOCS 2002) is whether these functions satisfy stronger security guarantees, such as collision resistance.

We show that the function proposed in (Micciancio, 2002) is not collision resistant, but it can be easily modified to achieve collision resistance under essentially the same complexity assumptions on cyclic lattices. Our modified function is obtained as a special case of a more general result, which yields efficient collision resistant hash functions that are at least hard to break as solving the worst case instance of various new problems. These include new problems from algebraic number theory, as well as classic lattice problems (e.g., the shortest vector problem) over *ideal lattices*, a new class of lattices that includes cyclic lattices as a special case.

Keywords: hash functions, lattices, worst-case to average-case reductions, knapsacks

1 Introduction

Ever since Ajtai's discovery of a function whose average-case hardness can be proved based on a worst-case complexity assumptions about lattices [2], the possibility of building cryptographic functions whose security is based on worst-case problems has been very alluring. Ajtai's initial discovery [2] and subsequent developments [5, 12, 14] are very interesting from a theoretical point of view because they are essentially the only problems for which such a worst-case / average-case connection is known. Unfortunately, the cryptographic functions proposed in these works are not efficient enough to be practical. The source of impracticality is the use of lattices, geometric arrangements of points that can be described as an $n \times n$ integer matrix. This results in cryptographic functions with key size and computation time at least quadratic in the security parameter n .

A step in the direction of creating cryptographic functions based on worst-case hardness that are efficient in practice was taken by Micciancio in [11]. In that paper, the author showed how to create a family of efficiently computable *one-way functions* (namely, the generalized compact knapsack functions described in the abstract) whose security is based on a certain problem for a particular class of lattices, called cyclic lattices. These lattices admit a much more compact representation than general ones, and the resulting functions can be described and evaluated in time almost linear in n . However, one-wayness is a rather weak security property, interesting mostly from a theoretical point of view, because it is sufficient to prove the existence (via polynomial time, but rather impractical, constructions) of many other important cryptographic

primitives, like commitment schemes, digital signatures, and private key encryption. By contrast, the (inefficient) functions based on general lattices considered in [2, 5, 12, 14] are collision resistant hash functions, a considerably stronger and much more useful cryptographic primitive.

In this work, we take the next step in creating efficient cryptographic functions based on worst-case assumptions. We show how to create efficient, collision resistant *hash functions* whose security is based on standard lattice problems for *ideal lattices* (i.e. lattices that can be described as ideals of certain polynomial rings). With current hash functions that are not based on any hardness assumptions, but used in practice, being broken [19], [20], [4], we believe that it may be a good time to consider using efficient hash functions which do have an underlying hardness assumption, especially one based on worst-case instances of problems.

Our contributions and comparison with related work In [11], it was shown how to create an efficient one-way function based on worst case hardness of problems for lattices which can be represented as ideals in the ring $\mathbb{Z}[x]/\langle x^n - 1 \rangle$. In our work, we show how to construct collision-resistant hash functions based on the hardness of problems for lattices that can be represented as ideals of the ring $\mathbb{Z}[x]/\langle f \rangle$ where f can be one of infinitely many other polynomials (including $x^n - 1$). Thus our result has two desirable features: it weakens the complexity assumption while strengthening the cryptographic primitive. As in [11], our functions are an instance of the generalized compact knapsack problem described in the abstract, but with the ring R and subset D instantiated in a different way. The way we change the ring R and subset D is simple, but essential, as we can show that the generalized compact knapsack instances considered in [11] are not collision resistant.

Concurrently with, and independently from our work, Peikert and Rosen [15] have shown that the one-way function in [11] is not collision resistant and showed how to construct collision resistant hash functions based on the hardness of finding the shortest vector for lattices which correspond to ideals in the ring $\mathbb{Z}[x]/\langle x^n - 1 \rangle$. While our more general result is interesting from a purely theoretical standpoint, it turns out that choices of certain f other than $x^n - 1$ result in somewhat better hash function, making our generalization also of practical use. Also, our hardness assumptions are formulated in a way that leads to natural connections with algebraic number theory, and we are able to relate our complexity assumptions to problems from that area. We believe that this will further our understanding of the hardness of problems about ideal lattices.

The hash function. We now give an informal description of the hash function families that we will be proving collision resistant. Given a ring $R = \mathbb{Z}_p[x]/\langle f \rangle$ (with the usual polynomial addition and multiplication operations) where $f \in \mathbb{Z}[x]$ is some monic, irreducible polynomial of degree n (for an algebra refresher, the reader may refer to subsection 2.1) and p is an integer of size roughly n^2 , generate m random elements $a_1, \dots, a_m \in R$ where m is some constant. The ordered m -tuple $h = (a_1, \dots, a_m) \in R^m$ is our hash function. It will map elements from D^m , where D is a strategically chosen subset of R , to R . For an element $b = (b_1, \dots, b_m) \in D^m$, the hash is $h(b) = \sum_{i=1}^m a_i \cdot b_i$. Notice that the size of the key (the hash function) is $O(mn \log p) = O(n \log n)$, and the operation $a_i \cdot b_i$ can be done in time $O(n \log n \log \log n)$ by using the fast Fourier transform (for appropriate choice of the polynomial f). Since m is a constant, we can hash a message in time $O(n \log n \log \log n)$. Then to prove that our hash function family is collision resistant, we will show that if there is a polynomial time algorithm that (for a randomly chosen hash function $h \in R^m$), succeeds with non-negligible probability in finding $b \neq b' \in D^m$ such that $h(b) = h(b')$, then a certain problem that we call the “shortest polynomial problem” is solvable in polynomial time for *every* ideal of the ring $\mathbb{Z}[x]/\langle f \rangle$. We then show that the shortest polynomial problem is equivalent to some lattice and algebraic number theory problems.

Paper outline. In section 2, we recall definitions and results from previous papers that will be used in our work, and prove a new bound on Gaussian distribution on lattices. Our main result and techniques rely on a connection between lattices and ideals of certain rings, which we describe in section 3. In section 4, we define the worst case problem on which we will be basing the security of our hash function. We then show

the equivalence of this problem to standard lattice problems as well as a problem from algebraic number theory.

Having established this equivalence between instances of problems for lattices, ideals, and number fields, we proceed to the construction of collision resistant hash functions that are at least as hard to break (on the average) as the worst instance of any of those problems. We formally define the hash function families in section 5.1 and show the worst-case to average case reduction in section 5.2.

2 Preliminaries

In this section we review some basic notions about algebra, lattices, and Gaussian distributions that will be used in the rest of the paper.

2.1 Algebra

Let $\mathbb{Z}[x]$ and $\mathbb{R}[x]$ be the sets of polynomials (in an indeterminate variable x) with integer and real coefficients respectively. A polynomial is *monic* if the coefficient of the highest power of x is one. A polynomial (in $\mathbb{Z}[x]$) is *irreducible* if it cannot be represented as a product of lower degree polynomials (in $\mathbb{Z}[x]$). In this paper we identify polynomials (of degree less than n) with the corresponding n -dimensional vectors having the coefficients of the polynomial as coordinates. This allows to translate notation and definitions from one setting to the other. E.g., we define the ℓ_p norm $\|g(x)\|_p$ of a polynomial $g(x) \in \mathbb{Z}[x]$ as the norm of the corresponding vector, and the product of two n -dimensional vectors $\mathbf{x} \cdot \mathbf{y}$ as the $(2n - 1)$ -dimensional vector associated to the product of the corresponding polynomials.

Let R be a ring. An *ideal* I of R is an additive subgroup of R closed under multiplication by arbitrary ring elements. The smallest ideal of R containing a subset $S \subseteq R$ is denoted $\langle S \rangle$. In particular, for any ring element $f \in R$, $\langle f \rangle$ denotes the set of all multiples of f . Two ring elements $g, h \in R$ are equivalent modulo an ideal $I \subseteq R$ if $g - h \in I$. When $I = \langle f \rangle$ is the ideal generated by a single ring element f , then we say that g and h are equivalent modulo f . The quotient R/I is the set of all equivalence classes $(g + I)$ of R modulo I .

Much of our work deals with the rings $\mathbb{Z}[x]/\langle f \rangle$ where f is monic and irreducible. When f is a monic polynomial of degree n , then every equivalence class $(g + \langle f \rangle) \in (\mathbb{Z}[x]/\langle f \rangle)$ has a unique representative $g' \in (g + \langle f \rangle)$ of degree less than n . This representative is denoted $(g \bmod f)$ and can be efficiently computed using the standard division algorithm. We endow the ring $\mathbb{Z}[x]/\langle f \rangle$ with the (infinity) norm $\|(g + \langle f \rangle)\|_f = \|g \bmod f\|_\infty$. Notice that the function $\|\cdot\|_f$ is well defined (i.e., it does not depend on the choice of representative g) and it is indeed a norm (i.e., it satisfies the positivity and triangle inequality properties). As shorthand, we will sometimes write $\|g\|_f$ instead of $\|g + \langle f \rangle\|_f$. Another shorthand that we use is denoting the quotient ring $\mathbb{Z}[x]/\langle p, f \rangle$ for some positive integer p and polynomial f as $\mathbb{Z}_p[x]/\langle f \rangle$. Also, whenever there is no confusion from context, instead of writing $g + \langle f \rangle$ for elements of $\mathbb{Z}[x]/\langle f \rangle$, we just write g .

2.2 Lattices

An n -dimensional *lattice* is the set of all integer combinations $\{\sum_{i=1}^n x_i \mathbf{b}_i : x_i \in \mathbb{Z}\}$ of n linearly independent vectors $\mathbf{b}_1, \dots, \mathbf{b}_n$ in \mathbb{R}^n . The set of vectors $\mathbf{b}_1, \dots, \mathbf{b}_n$ is called a *basis* for the lattice, and can be compactly represented by the matrix $\mathbf{B} = [\mathbf{b}_1 | \dots | \mathbf{b}_n] \in \mathbb{R}^{n \times n}$ having the basis vectors as columns. The lattice generated by \mathbf{B} is denoted $\mathcal{L}(\mathbf{B})$. For any basis \mathbf{B} , we define the fundamental parallelepiped $\mathcal{P}(\mathbf{B}) = \{\mathbf{B}\mathbf{x} : \forall i. 0 \leq x_i < 1\}$. The following lemma shows how to sample lattice points uniformly at random from the fundamental parallelepiped associated to a given sublattice.

Lemma 2.1 ([13, Proposition 8.2]). *There is a probabilistic polynomial time algorithm that on input a lattice basis \mathbf{B} and a full rank sublattice $\mathbf{S} \subset \mathcal{L}(\mathbf{B})$, outputs a lattice point $\mathbf{x} \in \mathcal{L}(\mathbf{B}) \cap \mathcal{P}(\mathbf{S})$ chosen uniformly at random.*

The lattices that are most relevant to us are *integer lattices*, i.e., lattices $\mathcal{L}(\mathbf{B}) \subseteq \mathbb{Z}^n$ all of whose vectors have integer coordinates. The dual of a lattice $\mathcal{L}(\mathbf{B})$ (denoted $\mathcal{L}(\mathbf{B})^*$) is the lattice generated by the matrix \mathbf{B}^{-T} , and consists of all vectors that have integer scalar product with all lattice vectors. For any vector $\mathbf{x} = (x_1, \dots, x_n)^T$, define the cyclic rotation $rot(\mathbf{x}) = (x_n, x_1, \dots, x_{n-1})^T$. A lattice $\mathcal{L}(\mathbf{B})$ is cyclic if it is closed under the rotation operation, i.e., if $\mathbf{x} \in \mathcal{L}(\mathbf{B})$ implies $rot(\mathbf{x}) \in \mathcal{L}(\mathbf{B})$.

The *minimum distance* of a lattice $\mathcal{L}(\mathbf{B})$ is the minimum distance between any two (distinct) lattice points and equals the length of the shortest nonzero lattice vector. The minimum distance can be defined with respect to any norm. For any $p \geq 1$, the ℓ_p norm of a vector \mathbf{x} is defined by $\|\mathbf{x}\|_p = \sqrt[p]{\sum_i |x_i|^p}$ and the corresponding minimum distance is denoted

$$\lambda_1^p(\mathcal{L}(\mathbf{B})) = \min\{\|\mathbf{x} - \mathbf{y}\|_p : \mathbf{x} \neq \mathbf{y} \in \mathcal{L}(\mathbf{B})\} = \min\{\|\mathbf{x}\|_p : \mathbf{x} \in \mathcal{L}(\mathbf{B}) \setminus \{\mathbf{0}\}\}.$$

Each norm gives rise to a corresponding computational problem SVP_γ^p (the γ -approximate *Shortest Vector Problem* in the ℓ_p norm): given a lattice $\mathcal{L}(\mathbf{B})$, find a nonzero vector $\mathbf{v} \in \mathcal{L}(\mathbf{B})$ such that $\|\mathbf{v}\|_p \leq \gamma \lambda_1^p(\mathcal{L}(\mathbf{B}))$. We also consider the restriction of SVP to specific classes of lattices. The restriction of SVP to a class of lattices Λ is denoted Λ - SVP . (E.g, [11] considers *Cyclic-SVP*).

The notion of minimum distance can be generalized to define the i th successive minimum (in the ℓ_p norm) $\lambda_i^p(\mathcal{L}(\mathbf{B}))$ as the smallest radius r such that the closed sphere $\bar{\mathcal{B}}_p(r) = \{\mathbf{x} : \|\mathbf{x}\|_p \leq r\}$ contains i linearly independent lattice points: $\lambda_i^p(\mathcal{L}(\mathbf{B})) = \min\{r : \dim(\text{span}(\mathcal{L}(\mathbf{B}) \cap \bar{\mathcal{B}}_p(r))) \geq i\}$.

In this work, we focus on the infinity norm $\|\mathbf{x}\|_\infty = \lim_{p \rightarrow \infty} \|\mathbf{x}\|_p = \max_i |x_i|$ since it is the most natural and convenient norm when dealing with polynomials, but most of our results are easily translated to other norms as well. The shortest vector problem in the infinity norm SVP_γ^∞ was proved to be NP -hard by van Emde Boas for $\gamma = 1$ [18] and shown to be NP -hard for factor up to $\gamma(n) = n^{1/\log \log n}$ by Dinur [7], where n is the dimension of the lattice. The asymptotically fastest algorithm for computing the shortest vector exactly takes time $2^{O(n)}$ [3] and the best polynomial time algorithm approximates the shortest vector to within a factor of $2^{O(\frac{n \log \log n}{\log n})}$ [3],[17],[10]. It is conjectured that approximating the shortest vector to within a polynomial factor is a hard problem, although it is shown that (under standard complexity assumptions) for small polynomial factors it is not NP -hard [1], [9].

2.3 Gaussian distribution

In this paper we use techniques from [14] that involve Gaussian distributions over lattices. In this subsection we recall all the relevant definitions and results from [14]. Let X and Y be random variables over a set A with probability density functions δ_X and δ_Y respectively. The statistical distance between X and Y , denoted $\Delta(X, Y)$, is

$$\Delta(X, Y) = \frac{1}{2} \int_{a \in A} |\delta_X(a) - \delta_Y(a)| da.$$

The statistical distance satisfies the following useful properties:

$$\Delta(f(X), f(Y)) \leq \Delta(X, Y) \tag{1}$$

$$\Delta((X_1, \dots, X_k), (Y_1, \dots, Y_k)) \leq \sum_{i=1}^k \Delta(X_i, Y_i) \tag{2}$$

$$\tag{3}$$

for any function f and independent random variables X_1, \dots, X_k and Y_1, \dots, Y_k .

For any vectors \mathbf{c}, \mathbf{x} and any $s > 0$, let $\rho_{s,\mathbf{c}}(\mathbf{x}) = e^{-\pi \|\mathbf{x}-\mathbf{c}\|/s\|^2}$ be a Gaussian function centered in \mathbf{c} scaled by a factor of s . The total measure associated to $\rho_{s,\mathbf{c}}$ is $\int_{\mathbf{x} \in \mathbb{R}^n} \rho_{s,\mathbf{c}}(\mathbf{x}) d\mathbf{x} = s^n$. So, $\int_{\mathbf{x} \in \mathbb{R}^n} (\rho_{s,\mathbf{c}}(\mathbf{x})/s^n) d\mathbf{x} = 1$ and $\rho_{s,\mathbf{c}}/s^n$ is a probability density function. The distribution $\rho_{s,\mathbf{c}}/s^n$ can be efficiently approximated using standard techniques (see [14]), so in the rest of the paper we make the simplifying assumption that we can sample from $\rho_{s,\mathbf{c}}/s^n$ exactly and work with real numbers.

Functions are extended to sets in the usual way; e.g., $\rho_{s,\mathbf{c}}(A) = \sum_{\mathbf{x} \in A} \rho_{s,\mathbf{c}}(\mathbf{x})$ for any countable set A . For any s, \mathbf{c} and lattice Λ , define the discrete probability distribution (over the lattice Λ) $D_{\Lambda,s,\mathbf{c}}(\mathbf{x}) = \frac{\rho_{s,\mathbf{c}}(\mathbf{x})}{\rho_{s,\mathbf{c}}(\Lambda)}$, where $\mathbf{x} \in \Lambda$. Intuitively, $D_{\Lambda,s,\mathbf{c}}$ is the conditional probability¹ that $(\rho_{s,\mathbf{c}}/s^n) = \mathbf{x}$ given $(\rho_{s,\mathbf{c}}/s^n) \in \Lambda$. For brevity, we sometimes omit s or \mathbf{c} from the notation $\rho_{s,\mathbf{c}}$ and $D_{\Lambda,s,\mathbf{c}}$. When \mathbf{c} or s are not specified, we assume that they are the origin and 1 respectively.

In [14] Gaussian distributions are used to define a new lattice invariant (called the *smoothing parameter*) defined below, and many important properties of this parameter are established. The following properties will be used in this paper.

Definition 2.2. *For an n -dimensional lattice Λ , and positive real $\epsilon > 0$, the smoothing parameter $\eta_\epsilon(\Lambda)$ is the smallest s such that $\rho_{1/s}(\Lambda^* \setminus \{\mathbf{0}\}) \leq \epsilon$.*

Lemma 2.3 ([14, Lemma 4.1]). *Let $\rho_s/s^n \bmod \mathbf{B}$ be the distribution obtained by sampling a point according to the probability density function ρ_s/s^n and reducing the result modulo \mathbf{B} . For any lattice $\mathcal{L}(\mathbf{B})$, the statistical distance between $\rho_s/s^n \bmod \mathbf{B}$ and the uniform distribution over $\mathcal{P}(\mathbf{B})$ is at most $\frac{1}{2}\rho_{1/s}(\mathcal{L}(\mathbf{B})^* \setminus \{\mathbf{0}\})$. In particular, if $s \geq \eta_\epsilon(\mathcal{L}(\mathbf{B}))$, then the distance $\Delta(\rho_s/s^n \bmod \mathbf{B}, U(\mathcal{P}(\mathbf{B})))$ is at most $\epsilon/2$.*

Lemma 2.4 ([14, Lemma 3.3]). *For any n -dimensional lattice Λ and positive real $\epsilon > 0$,*

$$\eta_\epsilon(\Lambda) \leq \sqrt{\frac{\ln(2n(1+1/\epsilon))}{\pi}} \cdot \lambda_n^2(\Lambda) \leq \sqrt{\frac{n \ln(2n(1+1/\epsilon))}{\pi}} \cdot \lambda_n^\infty(\Lambda).$$

Lemma 2.5 ([14]). *Let Λ be any n -dimensional lattice and let s be such that $s > 2\eta_\epsilon(\Lambda)$ for $\epsilon \leq 1/100$, and let $\mathbf{c} \in \mathbb{R}^n$ be any point. Then for all $\mathbf{x}' \in \Lambda$, $\Pr_{\mathbf{x} \sim D_{\Lambda,s,\mathbf{c}}}[\mathbf{x} = \mathbf{x}'] \leq 99/100$.*

2.4 New lemmas for the Gaussian distribution over lattices

In this subsection, we state a new result for Gaussian distributions over lattices which strengthens a result from [14], and thus might be of independent interest. In [14], the authors showed that for any \mathbf{c} and a large enough s , the first few moments of the distribution $D_{\Lambda,s,\mathbf{c}}$ behave essentially the same as the moments of the continuous Gaussian distribution ρ_s/s^n . In this work, though, we need much higher moments of $D_{\Lambda,s,\mathbf{c}}$. In appendix D we prove that *all* the moments of $D_{\Lambda,s,\mathbf{c}}$ behave like the moments of ρ_s/s^n plus a little error. The precise statement of this is given in lemma D.6. This result allows us to prove the following lemma, whose proof can also be found in appendix D.

Lemma 2.6. *For any n -dimensional lattice Λ , point $\mathbf{c} \in \mathbb{R}^n$, a vector \mathbf{u} such that $\|\mathbf{u}\| = 1$, positive real $s > 2\eta_\epsilon(\Lambda)$ where $\epsilon < (\log n)^{-2 \log n}$,*

$$\Pr_{\mathbf{x} \sim D_{\Lambda,s,\mathbf{c}}}[\langle \mathbf{x} - \mathbf{c}, \mathbf{u} \rangle \geq s \log n] = n^{-\omega(1)}$$

Lemma 2.7. *For any n -dimensional lattice Λ , positive reals $\epsilon < (\log n)^{-2 \log n}$, $s > 2\eta_\epsilon(\Lambda)$, and polynomials $c, z \in \mathbb{R}[x]$ of degree less than n ,*

$$\Pr_{d \sim D_{\Lambda,s,\mathbf{c}}}[\|(d - c)z\|_\infty \geq \|z\|s \log n] = n^{-\omega(1)}$$

Proof. Consider the vector $\mathbf{d} - \mathbf{c} = (d_0 - c_0, \dots, d_{n-1} - c_{n-1})$ corresponding to the coefficients of the difference of $d - c$. Also, define the vectors $\mathbf{z}^{(i)}$ as follows:

$$\mathbf{z}^{(i)} = \begin{cases} (z_i, z_{i-1}, \dots, z_0, 0, \dots, 0) & \text{for } 0 \leq i \leq n-1 \\ (0, \dots, 0, z_{n-1}, \dots, z_{i+2-n}, z_{i+1-n}) & \text{for } n \leq i \leq 2n-2 \end{cases}$$

With the above notation, the polynomial product of $(d-c)z$ can be written as

$$(d - c)z = \sum_{i=0}^{2n-2} \langle \mathbf{d} - \mathbf{c}, \mathbf{z}^{(i)} \rangle x^i$$

¹We are conditioning on an event that has probability 0; this can be made rigorous by standard techniques.

Thus,

$$\|(d - c)z\|_\infty = \max_i |\langle \mathbf{d} - \mathbf{c}, \mathbf{z}^{(i)} \rangle| = \max_i \left| \|\mathbf{z}^{(i)}\| \left\langle \mathbf{d} - \mathbf{c}, \frac{\mathbf{z}^{(i)}}{\|\mathbf{z}^{(i)}\|} \right\rangle \right| \leq \|z\| \max_i \left| \left\langle \mathbf{d} - \mathbf{c}, \frac{\mathbf{z}^{(i)}}{\|\mathbf{z}^{(i)}\|} \right\rangle \right|$$

By lemma 2.6 and the union bound, we get

$$Pr_{d \sim D_{\Lambda, s, c}} \left[\max_i \left| \left\langle \mathbf{d} - \mathbf{c}, \frac{\mathbf{z}^{(i)}}{\|\mathbf{z}^{(i)}\|} \right\rangle \right| \geq s \log n \right] \leq 2n \cdot n^{-\omega(1)} = n^{-\omega(1)}$$

and so the claim in the lemma follows. \square

3 Generalized compact knapsacks and ideal lattices

In [11], Micciancio introduced the following generalization of the compact knapsack problem. Let R be a ring, $D \subset R$ a subset, and $m \geq 1$ a positive integer. The generalized knapsack function family $\mathcal{H}(R, D, m)$ is the collection of all functions $\mathfrak{h}_{\mathbf{a}} : D^m \rightarrow R$ indexed by $\mathbf{a} \in R^m$ mapping $\mathbf{b} \in D^m$ to $\mathfrak{h}_{\mathbf{a}}(\mathbf{b}) = \sum_{i=1}^m b_i \cdot a_i \in R$.

For any function family \mathcal{H} , define the problem $\text{Collision}_{\mathcal{H}}$ as follows: given a function $\mathfrak{h} \in \mathcal{H}$, find a collision, i.e., a pair of inputs $\mathbf{b}, \mathbf{c} \in D^m$ such that $\mathbf{b} \neq \mathbf{c}$ and $\mathfrak{h}(\mathbf{b}) = \mathfrak{h}(\mathbf{c})$. If there is no polynomial time algorithm that can solve $\text{Collision}_{\mathcal{H}}$ with non-negligible probability when given an \mathfrak{h} which is distributed uniformly at random in \mathcal{H} , then we say that \mathcal{H} is a collision resistant family of hash functions.

[11] considers the instantiation of the generalized compact knapsack where $R = \mathbb{Z}_p[x]/\langle x^n - 1 \rangle$ (for some integers p and n), and proves that the resulting function family is *one-way* (a weaker security property than collision resistance) under a worst-case complexity assumption on cyclic lattices.

In this paper we show that the generalized compact knapsack function proposed in [11] is not collision resistant (see appendix A), and consider a more general class of rings that allows us to build provably collision resistant generalized compact knapsack functions based on worst-case computational assumptions on *ideal lattices*, a new class of lattices that includes cyclic lattices as a special case.

Let $f \in \mathbb{Z}[x]$ be a monic polynomial of degree n , and consider the quotient ring $\mathbb{Z}[x]/\langle f \rangle$. Using the standard set of representatives $\{(g \bmod f) : g \in \mathbb{Z}[x]\}$, and our identification of polynomials with vectors, the quotient ring $\mathbb{Z}[x]/\langle f \rangle$ is isomorphic (as an additive group) to the integer lattice \mathbb{Z}^n , and any ideal $I \subseteq \mathbb{Z}[x]/\langle f \rangle$ defines a corresponding integer sublattice $\mathcal{L}(I) \subseteq \mathbb{Z}^n$. Notice that not every integer lattice $\mathcal{L}(\mathbf{B}) \subseteq \mathbb{Z}^n$ can be represented this way.² We define ideal lattices as lattices that admit such a representation.

Definition 3.1. *An ideal lattice is an integer lattice $\mathcal{L}(\mathbf{B}) \subseteq \mathbb{Z}^n$ such that $\mathcal{L}(\mathbf{B}) = \{g \bmod f : g \in I\}$ for some monic polynomial f of degree n and ideal $I \subseteq \mathbb{Z}[x]/\langle f \rangle$.*

It is easy to see that cyclic lattices, as considered in [11], are a special case of ideal lattices where $f = x^n - 1$. Here we study ideal lattices for other choices of the polynomial f . It turns out that the relevant properties of f for the resulting function to be collision resistant are:

- f should be irreducible.
- the ring norm $\|g\|_f$ is not much bigger than $\|g\|_\infty$ for any polynomial g , in a quantitative sense to be explained later.

The first property implies that every ideal of the ring $\mathbb{Z}[x]/\langle f \rangle$ defines a full-rank lattice in \mathbb{Z}^n , (Lemma 3.2 below) and plays a fundamental role in our proofs. The second property affects the strength of our security proofs: the smaller the ratio $\|g\|_f / \|g\|_\infty$ is, the harder to break our functions seem to be. After the lemma, we elaborate on the second property by defining a quantitative parameter (the expansion factor) that captures the relation between $\|\cdot\|_\infty$ and $\|\cdot\|_f$, and proving bounds on this parameter for a wide class of polynomials f .

²Take, for example, the 2-dimensional lattice generated by the vectors $(2, 0)$ and $(0, 1)$ (or in terms of polynomials, by $2x$ and 1). This lattice cannot be represented by an ideal, because any ideal containing 1 must necessarily contain also the polynomial $1 \cdot x$, but the vector $(1, 0)$ (corresponding to the polynomial x) does not belong to the lattice.

Lemma 3.2. *Every ideal I of $\mathbb{Z}[x]/\langle f \rangle$, where f is a monic, irreducible integer polynomial of degree n , is isomorphic to a full-rank lattice in \mathbb{Z}^n .*

Proof. Let $I = \langle g_1, \dots, g_m \rangle$. One of the g_i 's must be non-zero, so assume it's g_1 . We will show that the $g_1, g_1x, \dots, g_1x^{n-1}$ are linearly independent over \mathbb{Z} . This will show that the lattice corresponding to I contains n linearly independent vectors, and thus must have dimension n .

Without loss of generality, assume that $\deg(g_1)$ is less than n . If $g_1, g_1x, \dots, g_1x^{n-1}$ are linearly dependent, then $g_1(a_0 + a_1x + \dots + a_{n-1}x^{n-1}) \in \langle f \rangle = fh$ for some polynomial h . Since f is irreducible and $\mathbb{Z}[x]$ is a unique factorization domain, f is then also prime. Thus either $f|g_1$ or $f|a_0 + a_1x + \dots + a_{n-1}x^{n-1}$. But both of those polynomials have degree less than f , and since f is irreducible, this cannot be unless either g_1 or $a_0 + a_1x + \dots + a_{n-1}x^{n-1}$ is 0. \square

3.1 The expansion factor

Notice that when we reduce a polynomial g modulo f , the maximum coefficient of g can increase by quite a bit, and thus $\|g\|_f$ could be a lot bigger than $\|g\|_\infty$. For example if $f = x^n - 2x^{n-1}$, then $x^{2n} \equiv 2^{n+1}x^{n-1}$ modulo f . On the other hand, if $f = x^n - 1$, we can never have such an exponential growth of coefficients. We capture this property of f by defining the *expansion factor* of f as

$$EF(f, k) = \max_{g \in \mathbb{Z}[x], \deg(g) \leq k(\deg(f)-1)} \|g\|_f / \|g\|_\infty$$

The below theorem gives tight bounds for the expansion factor of certain polynomials.

Theorem 3.3.

$$(1) EF(x^n - 1, k) \leq k \quad (2) EF(x^{n-1} + x^{n-2} + \dots + 1, k) \leq 2k \quad (3) EF(x^n + 1, k) \leq k$$

Proof. (1) Let $g = \sum_{i=0}^{k(n-1)} g_i x^i$ be a polynomial. Then it is in the same coset of $\mathbb{Z}[x]/\langle x^n - 1 \rangle$ as $h = \sum_{i=0}^{n-1} h_i x^i$

where $h_i = \sum_{j=0}^{\lfloor k(n-1)/n \rfloor} g_{i+jn}$. Thus

$$\|g\|_f = \|h\|_\infty \leq \|g\|_\infty (\lfloor k(n-1)/n \rfloor + 1) \leq k \|g\|_\infty.$$

Thus, we have $EF(x^n - 1, k) \leq k$.

(2) Let g be a polynomial of degree at most $k(n-1)$ and let h be the polynomial such that $\deg(g - h(x^n - 1)) < n$. By the proof of (1), we know that $\|g - h(x^n - 1)\|_\infty \leq k \|g\|_\infty$. Let α be the coefficient of the x^{n-1} term of $g - h(x^n - 1)$. The polynomial $g - h(x^n - 1) - \alpha(x^{n-1} + x^{n-2} + \dots + 1)$ has degree less than $n-1$ and infinity norm at most $2k \|g\|_\infty$ and is in the same coset of $\mathbb{Z}[x]/\langle x^{n-1} + x^{n-2} + \dots + 1 \rangle$ as g . Thus $EF(x^{n-1} + x^{n-2} + \dots + 1, k) \leq 2k$.

(3) The proof for this part is almost identical to the proof of part (1) \square

Now, we will bound the expansion factor of arbitrary polynomials. For this, we will first need to define another property of polynomials, we call the *gap*.

Definition 3.4. *We will say that a polynomial f of the form $f = x^n + \sum_{i=0}^{n-m} \alpha_i x^i$ for $0 < m \leq n$ where $\alpha_i \in \mathbb{Z}$ and $\alpha_{n-m} \neq 0$ has gap m . So we write $\text{gap}(f) = m$.*

We do not define the gap of a polynomial that has only one term because such polynomials are inconsequential for our purposes. Also, we do not define gap for polynomials that are not monic. The following two theorems are proved in appendix C.

Theorem 3.5. *If f is a polynomial in $\mathbb{Z}[x]$, then*

$$EF(f, k) \leq \min_{f' \in \mathbb{Z}[x]} 2 \|f\|_1 \|f'\|_1 (2 \|ff'\|_1)^{\left\lceil \frac{(k-1)\deg(f) - k}{\text{gap}(ff')} \right\rceil}$$

In certain cases, the next theorem is a bit tighter than the previous one.

Theorem 3.6. *If f is a polynomial in $\mathbb{Z}[x]$, then*

$$EF(f, k) \leq \min_{f' \in \mathbb{Z}[x]} (2 \|ff'\|_1)^{\left\lceil \frac{(k-1)\deg(f) - k - \deg(f')}{\text{gap}(ff')} \right\rceil + 1} (2 \|f\|_\infty)^{\deg(f')}$$

Intuitively, in order for f to have a “small” expansion factor, f needs to be a factor of some polynomial h with a large gap, and the quotient h/f should not have large coefficients. So for example, $x^n + x^{n-1} + \dots + 1$ is such a polynomial because it is a factor of $x^{n+1} - 1$. It’s an interesting problem whether it’s possible, in polynomial time, to find the expansion factor (or even bound it) of an arbitrary polynomial f . We do not know how to do this. But the above two theorems do allow us to verify in polynomial time that a certain polynomial has a small expansion factor. We will be only concerned with values of $EF(f, k)$ when $k = 2, 3$, so the fact that k appears in the exponent in the above two theorems is not cause for concern.

4 Worst case problems

In this section we define the worst case problems and provide reductions among them.

Because of the correspondence between ideals and integer lattices, we can use the successive minima notation used for lattices for ideals as well. So for any ideal I of $\mathbb{Z}[x]/\langle f \rangle$, where f is a monic integer polynomial, we’ll define $\lambda_i^p(I)$ to be $\lambda_i^p(\mathcal{L}(I))$.

Definition 4.1. *In the approximate Shortest Polynomial Problem ($SPP_\gamma(I)$), we are given an ideal $I \subseteq \mathbb{Z}[x]/\langle f \rangle$ where f is a monic polynomial of degree n , and we are asked to find a $g \in I$ such that $g \neq 0$ and $\|g\|_f \leq \gamma \lambda_1^\infty(I)$.*

As for the shortest vector problem, we can consider the restriction of SPP to specific classes of ideals. We will write f - SPP for SPP restricted to ideals of the ring $\mathbb{Z}[x]/\langle f \rangle$. The f - SPP problem for any monic, irreducible f is the main worst-case problem of this work, as it is the problem upon which the security of our hash functions will be based. Since SPP is a new problem whose hardness has not been explored, we show that other better-known problems can be reduced to it. If we denote by $\mathcal{I}(f)$ the set of lattices that are isomorphic (as additive groups) to ideals of $\mathbb{Z}[x]/\langle f \rangle$ where f is monic, then there’s a straightforward reduction from $\mathcal{I}(f)$ - SVP_γ to f - SPP_γ (and also the other way around).

Lattices in the class $\mathcal{I}(x^n - 1)$ (cyclic lattices) do not fall into the category of lattices that are isomorphic to ideals of $\mathbb{Z}[x]/\langle f \rangle$ for an irreducible f (since $x^n - 1$ is not irreducible). But in appendix B, we give a reduction from $(x^n - 1)$ - $SPP_{2\gamma}$ to $(x^{n-1} + x^{n-2} + \dots + 1)$ - SPP_γ . Thus we will be able to establish the security of hash functions based on the hardness of the shortest vector problem for cyclic lattices of prime dimension, which is essentially the complexity assumption used by Micciancio in [11] for his one-way functions.

Another problem that we reduce to SPP is the problem of finding complex numbers with small conjugates in ideals of subrings of a number field. This problem and the reduction is described in detail in appendix B as well.

Now we state a lemma which shows that if I is an ideal of $\mathbb{Z}[x]/\langle f \rangle$ where f is a monic and irreducible, then $\lambda_n^\infty(I)$ cannot be much bigger than $\lambda_1^\infty(I)$. For ideals of arbitrary rings, there is no reason why there should be such a connection between these two quantities. The reason that we have a connection here, is that f is irreducible.

Lemma 4.2. *For all ideals I of $\mathbb{Z}[x]/\langle f \rangle$ where f is a monic, irreducible polynomial of degree n , we have $\lambda_n^\infty(I) \leq EF(f, 2) \lambda_1^\infty(I)$*

Proof. Let g be a polynomial in I of degree less than n such that $\|g\|_\infty = \lambda_1^\infty(I)$. Then consider the polynomials g, gx, \dots, gx^{n-1} . By lemma 3.2, the polynomials g, gx, \dots, gx^{n-1} are linearly independent. And since the maximum degree of any of these polynomials is $2n - 2$, $\|gx^i\|_f \leq EF(f, 2)\|g\|_\infty \leq EF(f, 2)\|g\|_f = EF(f, 2)\lambda_1^\infty(I)$ for all $0 \leq i \leq n - 1$. \square

Now we define the incremental version of *SPP*. In this version, we are not looking for the shortest polynomial, but just for a polynomial that is smaller than one that is given to us. We will be reducing this problem to the average-case problem.

Definition 4.3. *In the approximate Incremental Shortest Polynomial Problem ($IncSPP_\gamma(I, g)$), we are given I and a $g \in I$ such that $\|g\|_f > \gamma\lambda_1^\infty(I)$ and are asked to return an $h \in I$ such that $\|h\|_f \neq 0$ and $\|h\|_f \leq \|g\|_f/2$.*

We define the restricted version of *IncSPP* in the same way as the restricted version for *SPP*.

Lemma 4.4. *There is a polynomial time reduction from f -*SPP* $_\gamma$ to f -*IncSPP* $_\gamma$.*

5 Collision resistant hash function families

In this section, we will define families of hash functions which are instances of generalized compact knapsacks and prove that finding collisions in these hash functions is at least as hard as solving the approximate shortest polynomial problem.

5.1 The hash function families

The hash function family $\mathcal{H}(R, D, m)$ we will be considering in this paper will be instances of generalized knapsacks instantiated as follows. Let $f \in \mathbb{Z}[x]$ be an irreducible, monic polynomial of degree n with expansion factor $EF(f, 3) \leq \mathcal{E}$. Such an upper bound for the expansion factor may be obtained using theorems 3.3, 3.5, or 3.6. Let the ring R be $\mathbb{Z}_p[x]/\langle f \rangle$ for some integer p , and let $D = \{g \in R : \|g\|_f \leq d\}$ for some positive integer d . The family of functions \mathcal{H} is mapping elements from D^m to R where $|D^m| = (2d + 1)^{nm}$ and $|R| = p^n$. So if $m > \frac{\log p}{\log 2d}$, then \mathcal{H} will be a family of functions that have collisions. We will only be interested in such families.

We will now state the main theorem.

Theorem 5.1. *Let \mathcal{H} be a hash function family as above with $m > \frac{\log p}{\log 2d}$ and $p > 2\mathcal{E}dmn^{1.5} \log n$. Then, for $\gamma = 8\mathcal{E}^2dmn \log^2 n$, there is a polynomial time reduction from f -*SPP* $_\gamma(I)$ for any I to $\text{Collision}_{\mathcal{H}}(\mathfrak{h})$ where \mathfrak{h} is chosen uniformly at random from \mathcal{H} .*

The proof of the theorem is given in the next subsection. To achieve the best approximation factor for f -*SPP* $_\gamma(I)$, we can set $m = \Theta(\log n, \log \mathcal{E})$ and $d = \Theta(\log n)$. This makes $\gamma = \tilde{O}(n)\mathcal{E}^2$. For purposes of being able to compute the function faster, though, it is useful to have m be smaller than $\Theta(\log n)$. It is possible to make m constant at the expense of being able to approximate f -*SPP* only to a factor of $\gamma = \tilde{O}(n^{1+\delta})\mathcal{E}^2$. To be able to set m to a constant, we can set $d = n^\delta$ for some $\delta > 0$. Then we can set $m = \frac{\log(\mathcal{E})}{\delta \log n} + \frac{2+\delta}{\delta} + o(1)$.

In order to get the “tightest” reduction, we should pick an f such that the bound \mathcal{E} on f ’s expansion factor is small. In theorem 3.3, we show that we can set \mathcal{E} to be 3 and 6 for polynomials of the form $x^n + 1$ and $x^{n-1} + x^{n-2} + \dots + 1$ respectively. The polynomial $x^n + 1$ is irreducible whenever n is a power of 2 and $x^{n-1} + x^{n-2} + \dots + 1$ is irreducible for prime n , so those are good choices for f . Among other possible f ’s with constant bounds for $EF(f, 3)$ are polynomials of the form $x^n \pm x \pm 1$ (see [16, Chapter 2.3.2] for sufficient conditions for the irreducibility of polynomials of this form). So one has many choices for which f to use in defining the hash function family and ending up with a “good” worst-case to average case connection.

Some sample instantiations of the hash function. If we let $f = x^{126} + \dots + x + 1$, $n = 126$, $d = 8$, $m = 8$, and $p \approx 2^{23}$, then our hash function is mapping $|2d|^{mn} = 4032$ bits to $|R_p| = p^n \approx 2900$ bits. If we want to base our hardness assumption on lattices of higher dimension, we can instantiate $f = x^{256} + \dots + x + 1$, $n = 126$, $p \approx 2^{25}$, $d = 8$, $m = 8$, and our hash function will be mapping 8192 bits to $p^n \approx 6400$ bits. If we instead let $f = x^{256} + 1$, we can let p be half as small (because the expansion factor for $x^n + 1$ is half of the expansion factor of $x^n + \dots + x + 1$) and thus we will be mapping 8192 bits to around 6150 bits.

5.2 Finding collisions is hard

In this section, we will provide the proof of theorem 5.1. Let \mathcal{H} be the family of hash functions described in the last subsection with $p > 2\mathcal{E}dmn^{1.5} \log n$. We will show that if one can solve in polynomial time, with non-negligible probability, the problem $\text{Collision}_{\mathcal{H}}(\mathfrak{h})$ where \mathfrak{h} is chosen uniformly at random from \mathcal{H} , then one can also solve $f\text{-IncSPP}_{\gamma}(I, g)$ for any ideal I for $\gamma = 8\mathcal{E}^2dmn \log^2 n$. And since by lemma 4.4, $f\text{-SPP}_{\gamma}(I) \leq f\text{-IncSPP}_{\gamma}(I, g)$, we will have a reduction from $f\text{-SPP}_{\gamma}(I)$ for any I to $\text{Collision}_{\mathcal{H}}(\mathfrak{h})$ for a random \mathfrak{h} . Let \mathcal{C} be an oracle such that when given a uniformly random $\mathfrak{h} \in \mathcal{H}$, $\mathcal{C}(\mathfrak{h})$ returns a solution to $\text{Collision}_{\mathcal{H}}(\mathfrak{h})$ with non-negligible probability in polynomial time. Now we proceed with giving an algorithm for $f\text{-IncSPP}_{\gamma}$ when given access to oracle \mathcal{C} .

Given: $I, g \in I$ such that $g \neq 0$ and $\|g\|_f > 8\mathcal{E}^2dmn \log^2 n \lambda_1^{\infty}(I)$
Find: $h \in I$, such that $h \neq 0$ and $\|h\|_f \leq \|g\|_f/2$.

Without loss of generality, assume that g has degree less than n and thus $\|g\|_{\infty} = \|g\|_f$. So we are looking for an h such that $\|h\|_f \leq \|g\|_{\infty}/2$. In this section, it will be helpful to think of ideals I and $\langle g \rangle$ as subgroups of \mathbb{Z}^n (or equivalently, as sublattices of \mathbb{Z}^n). Define a number s as

$$s = \frac{\|g\|_{\infty}}{8\mathcal{E}\sqrt{n} \log ndm} \geq \mathcal{E}\sqrt{n}(\log n)\lambda_1^{\infty}(I) \geq \sqrt{n}(\log n)\lambda_n^{\infty}(I) \geq \eta_{\epsilon}(I)$$

for $\epsilon = (\log n)^{-2 \log n}$, where the last inequality follows by lemma 2.4, and the inequality before that is due to lemma 4.2. By lemma 2.3, it follows that if $y \in \mathbb{R}^n$ where $y \sim \rho_s/s^n$, then $\Delta(y + I, U(\mathbb{R}^n/I)) \leq (\log n)^{-2 \log n}/2$. (That is, y is in an almost uniformly random coset of \mathbb{R}^n/I). By our definition of s , we have that $\|g\|_{\infty} = 8\mathcal{E}dms\sqrt{n} \log n$. Now we will try to create an $h \in I$ which is smaller than g using the procedure below. In the procedure, it may not be obvious how each step is performed, and the reader is referred to lemma 5.2 for a detailed explanation of each step.

- (1) for $i = 1$ to m
 - (2) generate a uniformly random coset of $I/\langle g \rangle$ and let v_i be a polynomial in that coset
 - (3) generate $y_i \in \mathbb{R}^n$ such that y_i has distribution ρ_s/s^n and consider y_i as a polynomial in $\mathbb{R}[x]$
 - (4) let w_i be the unique polynomial in $\mathbb{R}[x]$ of degree less than n with coefficients in the range $[0, p)$ such that $p(v_i + y_i) \equiv gw_i$ in $\mathbb{R}^n/\langle pg \rangle$
 - (5) $a_i = [w_i] \bmod p$ (where $[w_i]$ means round each coefficient of w_i to the nearest integer)
- (6) call oracle $\mathcal{C}(a_1, \dots, a_m)$, and using its output, find polynomials z_1, \dots, z_m such that $\|z_i\|_f \leq 2d$ and $\sum z_i a_i \equiv 0$ in the ring $\mathbb{Z}_p[x]/\langle f \rangle$.
- (7) output $h = \sum \left(\frac{g(w_i - [w_i])}{p} - y_i \right) z_i$.

To complete the proof, we will have to show five things: first, we have to prove that the above procedure runs in polynomial time, this is done in lemma 5.2. Then, in lemma 5.3, we show that in step (6) we are feeding the oracle \mathcal{C} with an $\mathfrak{h} \in \mathcal{H}$ where the distribution of \mathfrak{h} is statistically close to uniform over \mathcal{H} . In lemma 5.4, we show that the resulting polynomial h is in the ideal I . We then show that if \mathcal{C} outputted a collision, then with non-negligible probability, $\|h\|_f \leq \|g\|_{\infty}/2$ and that $h \neq 0$. This is done in lemmas 5.5 and 5.6 respectively. These five things prove that with non-negligible probability, we will obtain a solution to IncSPP_{γ} . If we happen to fail, we can just repeat the procedure again. Since each run of the procedure is independent, we will obtain a solution to IncSPP_{γ} in polynomial time.

Lemma 5.2. *The above procedure runs in polynomial time.*

Proof. We will show that each step in the algorithm takes polynomial time. In step (2), we need to generate a random element of $I/\langle g \rangle$. By lemma 3.2, the ideals I and $\langle g \rangle$ can be thought of as \mathbb{Z} -modules of dimension n . Since $\langle g \rangle \subseteq I$, the group $I/\langle g \rangle$ is finite. Thus by lemma 2.1, we can efficiently generate a random element of $I/\langle g \rangle$. Step (4) of the algorithm will be justified in lemma 5.3. In step (5), we are just rounding each coefficient of w_i to the nearest integer and then reducing modulo p . Now each a_i can be thought of as an element of $\mathbb{Z}_p[x]/\langle f \rangle$, so in step (6) we can feed (a_1, \dots, a_m) to the algorithm that solves $\text{Collision}_{\mathcal{H}}(a_1, \dots, a_m)$. The algorithm will return $(\alpha_1, \dots, \alpha_m), (\beta_1, \dots, \beta_m)$ where $\alpha_i, \beta_i \in \mathbb{Z}[x]/\langle f \rangle$ such that $\|\alpha_i\|_f, \|\beta_i\|_f \leq d$ and $\sum a_i \alpha_i \equiv \sum a_i \beta_i$ in the ring $\mathbb{Z}_p[x]/\langle f \rangle$. Thus if we set $z_i = \alpha_i - \beta_i$, we will have $\|z_i\|_f \leq 2d$ and $\sum z_i a_i \equiv 0$ in the ring $\mathbb{Z}_p[x]/\langle f \rangle$. \square

Lemma 5.3. *Consider the polynomials a_i as elements in \mathbb{Z}_p^n . Then,*

$$\Delta((a_1, \dots, a_m), U(\mathbb{Z}_p^{n \times m})) \leq m\epsilon/2.$$

Proof. We know that v_i is in a uniformly random coset of $I/\langle g \rangle$ and let's assume for now that y_i is in a uniformly random coset of \mathbb{R}^n/I . This means that $v_i + y_i$ is in a uniformly random coset of $\mathbb{R}^n/\langle g \rangle$ and thus the distribution of $p(v_i + y_i)$ is in a uniformly random coset of $\mathbb{R}^n/\langle pg \rangle$. A basis for the additive group $\langle pg \rangle$ is $pg, pgx, \dots, pgx^{n-1}$, thus every element of $\mathbb{R}^n/\langle pg \rangle$ has a unique representative of the form $\alpha_0 pg + \alpha_1 pgx + \dots + \alpha_{n-1} pgx^{n-1} = g(p\alpha_0 + p\alpha_1 x + \dots + p\alpha_{n-1} x^{n-1})$ for $\alpha_i \in [0, 1)$. So step (4) of the algorithm is justified, and since $p(v_i + y_i)$ is in a uniformly random coset of $\mathbb{R}^n/\langle pg \rangle$, the coefficients of the polynomial $w_i = p\alpha_0 + p\alpha_1 x + \dots + p\alpha_{n-1} x^{n-1}$ are uniform over the interval $[0, p)$, and thus the coefficients of $[w_i]$ are uniform over the integers modulo p . The caveat is that y_i is not really in a uniformly random coset of \mathbb{R}^n/I , but is very close to it. By our choice of s , we have that $\Delta(\rho_s/s^n + I, U(\mathbb{R}^n/I)) \leq \epsilon/2$, and since a_i is a function of y_i , by equation 1 we have that $\Delta(a_i, U(\mathbb{Z}_p^n)) \leq \epsilon/2$. Since all the a_i 's are independent, by equation 2, we have that $\Delta((a_1, \dots, a_m), U(\mathbb{Z}_p^{n \times m})) \leq m\epsilon/2$. \square

Lemma 5.4. $h \in I$

Proof. In step (4) of the algorithm, assume that $p(v_i + y_i) + k_i gp = gw_i$ for some $k_i \in \mathbb{Z}[x]/\langle f \rangle$. Then,

$$h = \sum_{i=1}^m \left(\frac{g(w_i - [w_i])}{p} - y_i \right) z_i = \sum_{i=1}^m (v_i + y_i + gk_i - ga_i/p - y_i) z_i = \sum_{i=1}^m (v_i + gk_i) z_i - \frac{g \sum a_i z_i}{p}$$

Since $v_i \in I$ and $g \in I$, we have that $v_i + gk_i \in I$ and therefore $\sum (v_i + gk_i) z_i \in I$. Also, since $\sum a_i z_i \equiv 0 \pmod{p}$, we have that $\frac{\sum a_i z_i}{p} \in \mathbb{Z}[x]$, and since $g \in I$, we have that $\frac{g \sum a_i z_i}{p} \in I$. \square

Lemma 5.5. *With probability negligibly close to 1, $\|h\|_f \leq \frac{\|g\|_\infty}{2}$.*

Proof. We are interested in bounding $\|h\|_f$. To do this, we will first bound $\|h\|_\infty$.

$$\begin{aligned} \|h\|_\infty &= \left\| \sum_{i=1}^m \left(\frac{g(w_i - [w_i])}{p} - y_i \right) z_i \right\|_\infty \\ &\leq \sum_{i=1}^m \left\| \left(\frac{g(w_i - [w_i])}{p} \right) z_i \right\|_\infty + \sum_{i=1}^m \|y_i z_i\|_\infty \end{aligned}$$

We will first bound the term on the left.

$$\left\| \left(\frac{g(w_i - [w_i])}{p} \right) z_i \right\|_\infty \leq \frac{1}{p} \|g(w_i - [w_i])\|_\infty \|z_i\|_1$$

Assume for a moment that the coefficients of w_i are independently, uniformly distributed in the range $[0, p)$. Thus the coefficients of $w_i - [w_i]$ are independently, uniformly distributed in the range $[-1/2, 1/2]$. We also notice that w_i is completely independent from g . Thus we can apply lemma E.2 and conclude that $\|g(w_i - [w_i])\|_\infty \leq \omega(\sqrt{n \log n}) \|g\|_\infty$ with probability negligibly close to 1. The preceding is all based on the assumption that the distribution of the coefficients of w_i is uniform, and the coefficients are independent, but in lemma 5.3, we showed that the distribution of the n coefficients of w_i is statistically close to uniform over $[0, p)^n$. So, the preceding inequality still holds with probability negligibly close to 1. Thus, with probability negligibly close to 1,

$$\sum_{i=1}^m \left\| \left(\frac{g(w_i - [w_i])}{p} \right) z_i \right\|_\infty \leq \frac{\|g\|_\infty n^{1.5} \omega(\sqrt{\log n}) dm}{p} < \frac{\|g\|_\infty}{4\mathcal{E}}$$

where the last inequality follows because of our choice of p .

Now we will bound $\sum \|y_i z_i\|_\infty$. We will show

$$Pr_{y_i \sim \rho_s / s^n} [\|y_i z_i\|_\infty > \|z_i\|_\infty s \sqrt{n} \log n | (a_1, \dots, a_m), (z_1, \dots, z_m)] = n^{-\omega(1)} \quad (4)$$

for each i . First, we will make the following observation. For any fixed coset of \mathbb{R}^n / I , call it $y'_i + I$, the distribution of a_i given y_i is the same for all $y_i \in y'_i + I$. Thus, given that $y_i \in y'_i + I$, the distribution of y_i is independent of (a_1, \dots, a_m) because a_i is a randomized function of $y'_i + I$ and $a_{j \neq i}$ is independent of y_i . And thus given that $y_i \in y'_i + I$, the distribution of y_i is also independent of (z_1, \dots, z_m) because (z_1, \dots, z_m) is a (randomized) function of (a_1, \dots, a_m) . So we have

$$Pr[y_i | y_i \in y'_i + I] = \frac{\rho_s(y_i)}{\rho_s(y'_i + I)} = \frac{\rho_{s, -y'_i}(y_i - y'_i)}{\rho_{s, -y'_i}(I)}$$

and so the conditional distribution of $(y_i - y'_i) \in I$ is $D_{I, s, -y'_i}$. Thus, we have

$$Pr_{y_i \sim \rho_s / s^n} [\|y_i z_i\|_\infty > \|z_i\|_\infty s \sqrt{n} \log n | y_i \in y'_i + I] = Pr_{(y_i - y'_i) \sim D_{I, s, -y'_i}} [\|((y_i - y'_i) - (-y'_i)) z_i\|_\infty \geq \|z_i\|_\infty s \sqrt{n} \log n]$$

and by lemma 2.7, we have

$$Pr_{(y_i - y'_i) \sim D_{I, s, -y'_i}} [\|((y_i - y'_i) - (-y'_i)) z_i\|_\infty \geq \|z_i\|_\infty s \sqrt{n} \log n] = n^{-\omega(1)}$$

The bound on equation 4 follows by averaging over all possible $y'_i + I$. Summing for all i , we get

$$\Pr \left[\sum_{i=1}^m \|y_i z_i\|_\infty \geq 2dms \sqrt{n} \log n \right] = n^{-\omega(1)}$$

And since $\|g\|_\infty = 8\mathcal{E}dms \sqrt{n} \log n$, we get that with probability negligibly close to 1, $\|h\|_\infty < \frac{\|g\|_\infty}{2\mathcal{E}}$. And since by observing how the polynomial h was constructed, we see that the degree of h is less than $3(n-1)$, we get that $\|h\|_f \leq EF(f, 3) \|h\|_\infty \leq \frac{\|g\|_\infty}{2}$. \square

Lemma 5.6. $Pr[h = 0 | (a_1, \dots, a_m), (z_1, \dots, z_m)] = \Omega(1)$

Proof. Since some z_i has to be non-zero, assume without loss of generality that z_1 is a non-zero polynomial. Then $h = 0$ if and only if

$$y_1 z_1 = \sum_{i=1}^m \frac{g(w_i - [w_i]) z_i}{p} - \sum_{i=2}^m y_i z_i$$

Notice that as in lemma 5.5, if we are given the coset of \mathbb{R}^n / I that y_1 belongs to (call it $y'_1 + I$), then y_1 is independent of all a_i and z_i and all $y_{i > 1}$. So we want to bound

$$Pr_{y_1 \sim \rho_s / s^n} \left[y_1 z_1 = \sum_{i=1}^m \frac{g(w_i - [w_i]) z_i}{p} - \sum_{i=2}^m y_i z_i \mid y_1 \in y'_1 + I \right] \quad (5)$$

and averaging over all $y'_1 + I$ will give us the final result. Notice that if $y_1 z_1 = c$, then for each given z_1 , there is only one value that y_1 can have. This is because the vectors $z_1, z_1 x, \dots, z_1 x^{n-1}$ are linearly independent (by lemma 3.2 since we assumed that $z_1 \neq 0$). Thus equation 5 is equivalent to

$$Pr_{y_1 \sim \rho_s / s^n} [y_1 | y_1 \in y'_1 + I] = \frac{\rho_s(y_1)}{\rho_s(y'_1 + I)} = \frac{\rho_{s, -y'_i}(y_i - y'_i)}{\rho_{s, -y'_i}(I)}$$

which is the probability that $x = y_1 - y'_1$ given that $x \sim D_{I, s, -y'_1}$. By lemma 2.5, this probability is at most $99/100$. Thus with probability $\Omega(1)$, $h \neq 0$. \square

6 Conclusions and open problems

We gave constructions of efficient collision resistant hash functions that can be proven secure based on the conjectured worst case hardness of the shortest vector problem for ideal lattices, i.e., lattices that can be represented as an ideal of $\mathbb{Z}[x]/\langle f \rangle$ for some monic, irreducible polynomial f . Moreover, our results can be extended to certain polynomials f that are not irreducible, e.g., the polynomial $f = x^n - 1$ corresponding to the class of cyclic lattices previously considered in [11]. A number of questions are raised by our work.

One question is the hardness of $\mathcal{I}(f)$ -SVP, or equivalently, the hardness of f -SPP for different f 's. It is known that SVP is hard in the general case, and it was conjectured in [11] that $\mathcal{I}(x^n - 1)$ -SVP is hard as well. In our work we show worst case to average case reductions that work for many other f 's, so in essence, we are giving more "targets" that can be proved hard.

Since different choices of f lead to different hash function families, understanding the relationship between the worst case complexity of f -SPP $_\gamma$ for different values of f is an important problem as well. We showed a reduction from $(x^n - 1)$ -SPP $_{2\gamma}$ to $(x^{n-1} + x^{n-2} + \dots + 1)$ -SPP $_\gamma$, but we heavily relied on the fact that $x^{n-1} + x^{n-2} + \dots + 1$ is a factor of $x^n - 1$. It is an interesting open problem whether there is a reduction between f -SPP and f' -SPP when f and f' are irreducible, monic polynomials.

Determining the hardness of the SCP problem introduced in appendix B is also an interesting problem. It's conceivable that finding complex numbers with small conjugates is an easier problem than SPP. And since we could only establish connections between f -SPP and f -SCP for certain f , it's possible that f -SPP could be easier for those f .

Very little is currently known about the complexity of problems for ideal lattices. We hope that our constructions of efficient collision-resistant hash functions based on the worst case hardness of these problems provides motivation for their further study.

References

- [1] Dorit Aharonov and Oded Regev. Lattice problems in $\text{NP} \cap \text{coNP}$. In *FOCS*, pages 362–371, 2004.
- [2] Miklos Ajtai. Generating hard instances of lattice problems. In *STOC*, pages 99–108, 1996.
- [3] Miklos Ajtai, Ravi Kumar, and D. Sivakumar. A sieve algorithm for the shortest lattice vector problem. In *STOC*, pages 601–610, 2001.
- [4] Eli Biham, Rafi Chen, Antoine Joux, Patrick Carribault, William Jalby, and Christophe Lemuet. Collisions of SHA-0 and reduced SHA-1. In *EUROCRYPT*, 2005.
- [5] Jin-Yi Cai and Ajay Nerurkar. An improved worst-case to average-case connection for lattice problems. In *FOCS*, pages 468–477, 1997.
- [6] Henri Cohen. *A Course in Computational Algebraic Number Theory*. Springer, 1996.
- [7] Irit Dinur. Approximating SVP $_\infty$ to within almost-polynomial factors is NP-hard. *Theor. Comput. Sci.*, 285(1):55–71, 2002.

- [8] Wolfgang Ebeling. *Lattices and Codes*. Friedr. Vieweg & Sohn., 2002.
- [9] Oded Goldreich and Shafi Goldwasser. On the limits of nonapproximability of lattice problems. *J. Comput. Syst. Sci.*, 60(3), 2000.
- [10] Arjen K. Lenstra, Hendrik W. Lenstra Jr., and Laszlo Lovasz. Factoring polynomials with rational coefficients. *Mathematische Annalen*, (261):513–534, 1982.
- [11] Daniele Micciancio. Generalized compact knapsaks, cyclic lattices, and efficient one-way functions from worst-case complexity assumptions. In *FOCS*, pages 356–365, 2002.
- [12] Daniele Micciancio. Almost perfect lattices, the covering radius problem, and applications to Ajtai’s connection factor. *SIAM Journal on Computing*, 34(1):118–169, 2004.
- [13] Daniele Micciancio and Shafi Goldwasser. *Complexity Of Lattice Problems: A Cryptographic Perspective*. Kluwer Academic Publishers, 2002.
- [14] Daniele Micciancio and Oded Regev. Worst-case to average-case reductions based on Gaussian measures. In *FOCS*, pages 372–381, 2004.
- [15] Chris Peikert and Alon Rosen. Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices. In *TCC*, 2006. (To appear).
- [16] Victor V. Prasolov. *Polynomials*, volume 11 of *Algorithms and Computation in Mathematics*. Springer-Verlag Berlin Heidelberg, 2004.
- [17] Claus Peter Schnorr. A hierarchy of polynomial time basis reduction algorithms. *Theoretical Computer Science*, 53:201–224, 1987.
- [18] Peter van Emde Boas. Another NP-complete problem and the complexity of computing short vectors in a lattice. Technical Report Technical Report 81-04, University of Amsterdam, <http://turing.wins.uva.nl/peter/>, 1981.
- [19] Xiaoyun Wang, Xuejia Lai, Dengguo Feng, Hui Chen, and Xiuyuan Yu. Cryptanalysis for hash functions MD4 and RIPEMD. In *EUROCRYPT*, 2005.
- [20] Xiaoyun Wang and Hongbo Yu. How to break MD5 and other hash functions. In *EUROCRYPT*, 2005.

A Finding collisions in $\mathbb{Z}_p[x]/\langle x^n - 1 \rangle$

In this subsection we show how to find collisions if the family of hash functions \mathcal{H} is instantiated as in section 5 (which is the same as in [11]) with $f = x^n - 1$. This answers an open problem posed in [11] as well as illustrates a weakness of using an f that is not irreducible. The intuitive reason we can find collisions is that the ring $\mathbb{Z}_p[x]/\langle f \rangle$ has an ideal that is small and consists of elements with small norms. That ideal is $J = \langle x^{n-1} + x^{n-2} + \dots + 1 \rangle + \langle f \rangle$. It’s not hard to see that $|J| = p$ and that all elements of J have the form $\alpha(x^{n-1} + x^{n-2} + \dots + 1) + \langle f \rangle$ for integers $0 \leq \alpha \leq p-1$. So the idea for solving $\text{Collision}_{\mathcal{H}}(\mathfrak{h})$ for a random $\mathfrak{h} \in \mathcal{H}$ is to choose $(y_1, \dots, y_m) \neq (z_1, \dots, z_m)$ such that $y_i, z_i \in J$ and $\|y_i\|_f \leq d$, $\|z_i\|_f \leq d$. This would force both $\mathfrak{h}(y_1, \dots, y_m)$ and $\mathfrak{h}(z_1, \dots, z_m)$ to be in J . There are $2d$ possibilities for each y_i , thus there are a total of $(2d+1)^m$ possibilities for (y_1, \dots, y_m) . Thus if $(2d+1)^m \geq p$, then a collision is guaranteed to exist and will take time on the order of p to find. But in order for h to be a hash function, we needed $(2d+1)^{nm}$ to be greater than p^n , and thus $(2d+1)^m > p$, which is exactly the condition we need to find a collision in J .

B Other worst case problems

B.1 Cyclic lattices

A cyclic lattice of dimension n is isomorphic to an ideal I in the ring $\mathbb{Z}[x]/\langle x^n - 1 \rangle$. We will show that finding the approximate shortest polynomial in an ideal of the ring $\mathbb{Z}[x]/\langle x^n - 1 \rangle$ for prime n reduces to finding the approximate shortest polynomial in an ideal of the ring $\mathbb{Z}[x]/\langle \Phi(n) \rangle$ where $\Phi(n) = x^{n-1} + \dots + 1$. (Since n is prime, $\Phi(n)$ is irreducible.) This shows that if we can solve the approximate shortest polynomial problem in ideals of the ring $\mathbb{Z}[x]/\langle f \rangle$ for monic, irreducible f , then we can solve the approximate shortest vector problem in cyclic lattices of prime dimension.

First, we will recall a standard lemma about finding the basis for the additive group of an ideal. It states that if I is an ideal of $\mathbb{Z}[x]/\langle f \rangle$, where f is a monic polynomial of degree n , then a basis for the lattice $\mathcal{L}(I)$ can be found in polynomial time.

Lemma B.1. *Let I be an ideal of $\mathbb{Z}[x]/\langle f \rangle$ where $f \in \mathbb{Z}[x]$ is a monic polynomial of degree n . Given the generators for I , there is a polynomial time algorithm that finds a basis for $\mathcal{L}(I)$.*

Proof. I is given to us as a set of generators g_1, \dots, g_m . Consider the set $G = \{g_1, g_1x, \dots, g_1x^{n-1}, g_2, g_2x, \dots, g_2x^{n-1}, \dots, g_m, g_mx, \dots, g_mx^{n-1}\}$. Every element of I can be written as an integer combination of the elements of G . Thus I is a \mathbb{Z} -module. By using the Hermite Normal Form algorithm [6, Chapter 2.4], we can find the basis for I as an additive group. \square

Theorem B.2. *There is a polynomial time reduction from the problem of approximating the shortest vector in a cyclic lattice of dimension n within a factor of 2γ to approximating the shortest polynomial in an ideal of the ring $\mathbb{Z}[x]/\langle \Phi(n) \rangle$ within factor γ .*

Proof. A cyclic lattice of dimension n is an ideal I of the ring $\mathbb{Z}[x]/\langle x^n - 1 \rangle$. Let v be the polynomial in I of degree less than n with the smallest infinity norm. There are two cases that will be handled separately.

Case 1: $\Phi(n) \nmid v$

In this case v is a polynomial in I in the ring $\mathbb{Z}[x]/\langle \Phi(n) \rangle$ that does not equal $0 + \langle \Phi(n) \rangle$. Since v is of degree at most $n - 1$ and $\Phi(n)$ is a degree $n - 1$ polynomial, $\|v\|_{\Phi(n)} \leq 2\|v\|_{\infty}$. So in this case, there exists a polynomial in I which is not 0 modulo $\Phi(n)$ whose infinity norm is at most $2\|v\|_{\infty}$, thus the algorithm for approximating the shortest polynomial problem to within γ in the ring $\mathbb{Z}[x]/\langle \Phi(n) \rangle$ should find a non-zero polynomial of infinity norm at most $2\gamma\|v\|_{\infty}$. And since every non-zero polynomial in $\mathbb{Z}[x]/\langle \Phi(n) \rangle$ is also non-zero in $\mathbb{Z}[x]/\langle x^n - 1 \rangle$, we are done.

Case 2: $\Phi(n) \mid v$

In this case, we can just find v directly. Since $v \in \langle \Phi(n) \rangle \cap I$, the only possibilities for v are polynomials of the form $c\Phi(n)$ for some integer c . By lemma B.1, we can find the basis for $\langle \Phi(n) \rangle \cap I$ as an additive group (\mathbb{Z} -module). And since this module has dimension 1, its generator will be the shortest polynomial in $\langle \Phi(n) \rangle \cap I$. \square

B.2 Algebraic number theory

In this subsection, we equate the problem of finding the shortest polynomial in an ideal to a certain problem from algebraic number theory. The connection between algebraic number theory and the ring $\mathbb{Z}[x]/\langle f \rangle$ comes from the following lemma.

Lemma B.3. *If $f \in \mathbb{Z}[x]$ is monic and is the minimum polynomial of θ , then $\mathbb{Z}[x]/\langle f \rangle \cong \mathbb{Z}[\theta]$.*

Proof. Let the degree of f be n and assume $\alpha \in \mathbb{Z}[\theta]$ is represented as an integer combination of powers of θ . That is, $\alpha = \alpha_0 + \alpha_1\theta + \dots + \alpha_{n-1}\theta^{n-1}$. Then the function $\sigma : \mathbb{Z}[\theta] \rightarrow \mathbb{Z}[x]/\langle f \rangle$ which maps α to $\alpha_0 + \alpha_1x + \dots + \alpha_{n-1}x^{n-1} + \langle f \rangle$ is an isomorphism. We will not prove this, but it is not hard to show using basic algebraic number theory. \square

Definition B.4. Let θ be an algebraic integer of degree n . Then for any $\alpha \in \mathbb{Q}(\theta)$ where $\alpha = \alpha_0 + \alpha_1\theta + \dots + \alpha_{n-1}\theta^{n-1}$, define the function $\max\text{Coeff}_\theta(\alpha)$ to be $\max(|\alpha_0|, \dots, |\alpha_{n-1}|)$.

From lemma B.3, we can see that finding an element with the smallest norm in an ideal I of $\mathbb{Z}[x]/\langle f \rangle$ is equivalent to finding the element α in the ideal $\sigma^{-1}(I)$ of $\mathbb{Z}[\theta]$ (where θ is a zero of f) such that $\max\text{Coeff}_{\mathbb{Q}(\theta)}(\alpha)$ is the smallest of all the $\alpha' \in \sigma^{-1}(I)$. This is not too interesting of a problem because it is exactly *SPP* with the indeterminate x replaced by θ . A more interesting result is relating the norm of elements in $\mathbb{Z}[x]/\langle f \rangle$ to the conjugates of elements in $\mathbb{Z}[\theta]$.

Definition B.5. For any $\alpha \in \mathbb{C}$, define the function $\max\text{Conj}(\alpha)$ to be $\max(|\phi_1|, \dots, |\phi_n|)$ where ϕ_i are the zeros of the minimum polynomial of α over \mathbb{Q} .

Notice that $\max\text{Coeff}_\theta(\alpha)$ depends on the particular representation of α , while $\max\text{Conj}(\alpha)$ does not. Now we define the smallest conjugate problem.

Definition B.6. Let θ be an algebraic integer of degree n . Let $K = \mathbb{Q}(\theta)$ be a number field, and let $\mathbb{Z}[\theta]$ be a subring of K . Let I be any ideal of $\mathbb{Z}[\theta]$. In the approximate Smallest Conjugate Problem $\text{SCP}_\gamma(I)$, we are asked to find an element $\alpha \in I$ such that $\max\text{Conj}(\alpha) \leq \gamma \cdot \max\text{Conj}(\alpha')$ for all $\alpha' \in I$.

The problem of finding elements with small conjugates is somewhat related to the ‘‘Polynomial Reduction Problem’’ in [6, Section 4.4.2] for which no polynomial time algorithm seems to be known.

As we did for *SVP* and *SPP*, we can consider the restriction of *SCP* to certain classes of ideals. Let f be an irreducible integer polynomial. We will write *f-SCP* to mean the problem *SCP* restricted to ideals of the ring $\mathbb{Z}[\theta]$ where θ is a zero of f .

Now we will prove a theorem relating *f-SCP* to *f-SPP* when $f = x^n + x^{n-1} + \dots + 1$. The key reason that we are able to get such a relationship is that when θ is a zero of such an f , then for any $\alpha \in \mathbb{Q}(\theta)$, $\max\text{Conj}(\alpha)$ and $\max\text{Coeff}_\theta(\alpha)$ differ by at most a factor of n . This is proved by lemmas B.8, B.9, and B.10. Lemmas B.8, B.9 give us the sufficient conditions under which there is such a close relationship, and lemma B.10 shows that when the minimum polynomial of θ is $x^n + x^{n-1} + \dots + 1$, then those conditions are satisfied.

Theorem B.7. Let $f = x^n + x^{n-1} + \dots + 1$ be irreducible, and let $\sigma : \mathbb{Z}[\theta] \rightarrow \mathbb{Z}[x]/\langle f \rangle$ be an isomorphism as in lemma B.3. Then $f\text{-SPP}_{\gamma n^2} \leq f\text{-SCP}_\gamma(\sigma^{-1}(I))$ and $f\text{-SCP}_{\gamma n^2} \leq f\text{-SPP}_\gamma(I)$.

Proof. Let θ be a zero of f . First, we will show $f\text{-SCP}_{\gamma n^2} \leq f\text{-SPP}_\gamma$. Consider an ideal I of $\mathbb{Z}[\theta]$ given to us by its generators g_1, \dots, g_k represented as a linear combination of powers of θ . That is $g_i = g_{i,0} + g_{i,1}\theta + \dots + g_{i,n-1}\theta^{n-1}$. We use the oracle for *f-SPP* $_\gamma$ to find the element $h \in \sigma(I)$ whose norm is less than $\gamma \lambda_1^\infty(\sigma(I))$ and let $\alpha = \sigma^{-1}(h)$. Thus $\max\text{Coeff}_\theta(\alpha) \leq \gamma \cdot \max\text{Coeff}_\theta(\alpha')$ for all $\alpha' \in I$. And so applying lemma B.10 twice, we get

$$\begin{aligned} \max\text{Conj}(\alpha) &\leq n \cdot \max\text{Coeff}_\theta(\alpha) \\ &\leq n\gamma \cdot \max\text{Coeff}_\theta(\alpha') \text{ for all } \alpha' \in I \\ &\leq n^2\gamma \cdot \max\text{Conj}(\alpha') \text{ for all } \alpha' \in I \end{aligned}$$

and so we have a γn^2 approximation for *SCP*.

Now we show $f\text{-SPP}_{\gamma n^2} \leq f\text{-SCP}_\gamma$. Consider an ideal I of $\mathbb{Z}[x]/\langle x^n + x^{n-1} + \dots + 1 \rangle$ given to us by its generators g_1, \dots, g_k . We use the oracle for *f-SCP* $_\gamma$ to find the element $\alpha \in \sigma^{-1}(I)$ such that $\max\text{Conj}(\alpha) \leq \gamma \cdot \max\text{Conj}(\alpha')$ for all $\alpha' \in \sigma^{-1}(I)$. And by applying lemma B.10 twice, we get

$$\begin{aligned} \max\text{Coeff}_\theta(\alpha) &\leq n \cdot \max\text{Conj}(\alpha) \\ &\leq n\gamma \cdot \max\text{Conj}(\alpha') \text{ for all } \alpha' \in \sigma^{-1}(I) \\ &\leq n^2\gamma \cdot \max\text{Coeff}_\theta(\alpha') \text{ for all } \alpha' \in \sigma^{-1}(I) \end{aligned}$$

This means that the infinity norm of $\sigma(\alpha)$ is at most $\gamma n^2 \lambda_1^\infty(I)$, and thus we have a γn^2 approximation of *f-SPP*. \square

We mention that $x^n + x^{n-1} + \dots + 1$ is not the only polynomial for which we can get the connection in the above theorem. For example, similar connections can be shown for irreducible polynomials of the form $x^n + \beta$ for $\beta \in \mathbb{Z}$ by applying lemma B.11 analogously to the way lemma B.10 was used in theorem B.7. We think that it would be very interesting to explore this further and see whether techniques from algebraic number theory can yield better algorithms for the shortest polynomial problem.

Lemma B.8. *Let $f \in \mathbb{Z}[x]$ be a monic irreducible polynomial of degree n with zeros $\theta_1, \dots, \theta_n \in \mathbb{C}$ such that for all i , $|\theta_i^{n-1}| \leq t$. Let $K = \mathbb{Q}(\theta_1)$ and $\alpha = \alpha_0 + \alpha_1\theta_1 + \dots + \alpha_{n-1}\theta_1^{n-1} \in K$. Then $\max\text{Conj}(\alpha) \leq nt \cdot \max\text{Coeff}_{\theta_1}(\alpha)$.*

Proof. Let $\sigma_1, \dots, \sigma_n : K \rightarrow \mathbb{C}$ be the n distinct embeddings of K into \mathbb{C} . Then the field polynomial of α is $f_{ld_\alpha}(x) = \prod_{i=1}^n (x - \sigma_i(\alpha))$. Since the field polynomial is a power of the minimum polynomial of α , the set of zeros of the minimal polynomial of α is exactly the set $\{\sigma_i(\alpha)\}$. Since $\sigma_i(\theta_1) = \theta_i$, we have that $\sigma_i(\alpha) = \alpha_0 + \alpha_1\theta_i + \dots + \alpha_{n-1}\theta_i^{n-1}$. Since $|\theta_i^{n-1}| \leq t$, we have the claim in the lemma. \square

Lemma B.9. *Let $f \in \mathbb{Z}[x]$ be a monic, irreducible polynomial of degree n with zeros $\theta_1, \dots, \theta_n \in \mathbb{C}$. Let $K = \mathbb{Q}(\theta_1)$ be a number field. If there exists an integer $m \geq n$ such that for all $1 \leq i \leq n$ and $j \leq m-1$ we have $1 \leq |\theta_i^j| \leq t$, and $\left| \sum_{i=1}^n \theta_i^m \right| \geq n$ and for all $j \neq 0 \pmod{m}$, we have $\left| \sum_{i=1}^n \theta_i^j \right| \leq s \leq 1$, then for all $\alpha \in K$, we have $\max\text{Coeff}_{\theta_1}(\alpha) \leq \frac{nt}{n(1-s)+s} \max\text{Conj}(\alpha)$.*

Proof. Let $\sigma_1, \dots, \sigma_n : K \rightarrow \mathbb{C}$ be the n distinct embeddings of K into \mathbb{C} . Then the set of zeros of the minimum polynomial of α is $\{\sigma_i(\alpha)\}$. Let $k = \max_i(|\sigma_i(\alpha)|)$. For each $0 \leq j \leq n-1$, we can set up the following system of n inequalities: for $1 \leq i \leq n$, $|\sigma_i(\alpha)\theta_i^{m-n+j}| \leq tk$. The preceding is true because $|\sigma_i(\alpha)| \leq k$ and $|\theta_i^{m-n+j}| \leq t$. Now we take a closer look at the system of inequalities for a particular j . Let $\alpha = \alpha_0 + \alpha_1\theta_1 + \dots + \alpha_{n-1}\theta_1^{n-1}$.

$$\begin{aligned} |\sigma_1(\alpha)\theta_1^{m-n+j}| &= |\alpha_0\theta_1^{m-n+j} + \dots + \alpha_{n-j}\theta_1^m + \dots + \alpha_{n-1}\theta_1^{m+j-1}| \leq kt \\ |\sigma_2(\alpha)\theta_2^{m-n+j}| &= |\alpha_0\theta_2^{m-n+j} + \dots + \alpha_{n-j}\theta_2^m + \dots + \alpha_{n-1}\theta_2^{m+j-1}| \leq kt \\ &\dots = \dots \\ |\sigma_n(\alpha)\theta_n^{m-n+j}| &= |\alpha_0\theta_n^{m-n+j} + \dots + \alpha_{n-j}\theta_n^m + \dots + \alpha_{n-1}\theta_n^{m+j-1}| \leq kt \end{aligned}$$

If we let $A = \sum_{i=1}^n |\alpha_i|$ and $S_j = \sum_{i=1}^n \theta_i^{m-n+j}$ then

$$\begin{aligned} n|\alpha_{n-j}| - s(A - |\alpha_{n-j}|) &= \\ n|\alpha_{n-j}| - s(|\alpha_0| + \dots + |\alpha_{n-j-1}| + |\alpha_{n-j+1}| + \dots + |\alpha_{n-1}|) &\leq \\ |\alpha_{n-j}S_n| - (|\alpha_0S_j| + \dots + |\alpha_{n-j-1}S_{n-1}| + |\alpha_{n-j+1}S_{n+1}| + \dots + |\alpha_{n-1}S_{n-1+j}|) &\leq \\ |\alpha_{n-j}S_n| - |\alpha_0S_j + \dots + \alpha_{n-j-1}S_{n-1} + \alpha_{n-j+1}S_{n+1} + \dots + \alpha_{n-1}S_{n-1+j}| &\leq \\ |\alpha_0S_j + \dots + \alpha_{n-j-1}S_{n-1} + \alpha_{n-j}S_n + \alpha_{n-j+1}S_{n+1} + \dots + \alpha_{n-1}S_{n-1+j}| &\leq \\ |\sigma_1(\alpha)\theta_1^{m-n+j}| + \dots + |\sigma_n(\alpha)\theta_n^{m-n+j}| &\leq nkt \end{aligned}$$

So for all α_i , we have the inequality

$$|\alpha_i| \leq \frac{nkt + sA}{n + s}$$

Setting $B = \frac{nkt+sA}{n+s}$, we get that $A \leq nB$, and thus $B \leq \frac{nkt}{n(1-s)+s}$ and since $|\alpha_i| \leq B$, we get the claim in the lemma. \square

Lemma B.10. *Let $f = x^n + x^{n-1} + \dots + 1$ be an irreducible polynomial and $\theta \in \mathbb{C}$ be one of its zeros. Let $K = \mathbb{Q}(\theta)$ and let α be an element of K . Then $\max\text{Coeff}_\theta(\alpha) \leq n \cdot \max\text{Conj}(\alpha)$ and $\max\text{Conj}(\alpha) \leq n \cdot \max\text{Coeff}_\theta(\alpha)$.*

Proof. To prove that $\maxConj(\alpha) \leq n \cdot \maxCoeff_\theta(\alpha)$, we will apply lemma B.8. Since f is the cyclotomic polynomial, all of its zeros have norm 1 and so we apply lemma B.8 with $t = 1$ and we obtain the desired inequality.

To show that $\maxCoeff_\theta(\alpha) \leq n \cdot \maxConj(\alpha)$, we will need to apply lemma B.9. In that lemma, we will set $t = 1$ and $m = n + 1$. If θ is a zero of $x^n + x^{n-1} + \dots + 1$, then $\theta^{n+1} = (\theta^n + \dots + 1)(\theta - 1) + 1 = 1$, and so $\left| \sum_{i=1}^n \theta_i^m \right| = n$. Since f is a cyclotomic polynomial, it has a zero, call it θ_1 , such that $\theta_i = \theta_1^i$ for all i . And since we already showed that $\theta_i^{n+1} = 1$, we know that $\theta_i^j = \theta_i^{j \bmod (n+1)}$. Thus for all j such that $j \bmod (n+1) \neq 0$, we have

$$\left| \sum_{i=1}^n \theta_i^j \right| = \left| \sum_{i=1}^n \theta_i^{j \bmod (n+1)} \right| = \left| \sum_{i=1}^n \theta_1^{i(j \bmod (n+1))} \right| = \left| \sum_{i=1}^n \theta_1^{j \bmod (n+1)} \right| = | -1 | = 1$$

Thus lemma B.9 applies with $s = 1$. And so we have $\maxCoeff_\theta(\alpha) \leq n \cdot \maxConj(\alpha)$ as claimed. \square

Lemma B.11. *Let $f = x^n + \beta \in \mathbb{Z}[x]$ be an irreducible polynomial and $\theta \in \mathbb{C}$ be one of its zeros. Let $K = \mathbb{Q}(\theta)$ and let α be an element of K . Then $\maxCoeff_\theta(\alpha) \leq |\beta| \cdot \maxConj(\alpha)$ and $\maxConj(\alpha) \leq |\beta|n \cdot \maxCoeff_\theta(\alpha)$.*

Proof. Let $\theta_1 = \theta, \theta_2, \dots, \theta_n$ be the zeros of f . To prove that $\maxConj(\alpha) \leq n|\beta| \cdot \maxCoeff_\theta(\alpha)$, we will apply lemma B.8. For any θ_i , we have $|\theta_i|^n = |\theta_i^n| = |\beta|$. Therefore, $|\theta_i^{n-1}| = |\theta_i|^{n-1} \leq |\beta|$, and we apply lemma B.8 with $t = |\beta|$. To show that $\maxCoeff_\theta(\alpha) \leq |\beta| \cdot \maxConj(\alpha)$, we will need to apply lemma B.9. We will apply that lemma with $t = |\beta|$, $s = 0$, and $m = n$. We already showed that $|\theta_i^j| \leq |\beta|$ for $0 \leq j \leq n-1$, and it's easy to see that $\left| \sum_{i=1}^n \theta_i^n \right| = |\beta n| \geq n$ (because $\theta_i^n = -\beta$). Now we will show that for all $j \neq 0 \pmod n$,

$$\sum_{i=1}^n \theta_i^j = 0. \tag{6}$$

First, assume that $1 \leq j < n$. Then equation 6 follows by applying Newton's formulas for symmetric polynomials [6, Proposition 4.3.3]. If $j > n$ and $j \neq 0 \pmod n$, then there exists an integer k such that $1 \leq j - kn \leq n-1$ and we have

$$\sum_{i=1}^n \theta_i^j = \sum_{i=1}^n (\theta_i^{kn} \theta_i^j - kn) = \sum_{i=1}^n (\theta_i^{kn} \theta_i^{j-kn}) = -\beta \sum_{i=1}^n \theta_i^{j-kn} = 0$$

Thus lemma B.9 applies with $t = |\beta|$, $s = 0$, and $m = n$ and we have the claimed result. \square

C Bounding the expansion factor (Non-essential technical appendix)

This appendix is dedicated to proving theorems 3.5 and 3.6. Before proving the theorems, we will prove two auxiliary lemmas.

Proposition C.1. *If f and g are polynomials in $\mathbb{Z}[x]$, then $\|fg\|_\infty \leq \|f\|_1 \|g\|_\infty$.*

Lemma C.2. *If g is a polynomial in $\mathbb{Z}[x]$ and f is a monic polynomial in $\mathbb{Z}[x]$ such that $\deg(g) \geq \deg(f)$, then $\|g\|_f \leq \|g\|_\infty (2\|f\|_\infty)^{\deg(g)-\deg(f)+1}$.*

Proof. Suppose that $g = g_0 = \sum_{i=0}^{\deg(g_0)} \alpha_i x^i$ where $\alpha_i \in \mathbb{Z}$. Let $g_1 = g_0 - f\alpha_{\deg(g_0)}$. Since f is monic, we have that $\deg(g_1) < \deg(g_0)$ and $\|g_1\|_\infty \leq \|g_0\|_\infty + \|g_0\|_\infty \|f\|_\infty \leq 2\|g_0\|_\infty \|f\|_\infty$. If we continue in the same fashion by constructing $g_i = g_{i-1} - f\alpha_{\deg(g_{i-1})}$, we see that the polynomial $g_{\deg(g)-\deg(f)+1}$ has degree less than $\deg(f)$, and also since $\|g_i\|_\infty \leq \|g\|_\infty (2\|f\|_\infty)^i$, we have the claim in the lemma. \square

Lemma C.3. *If $f \in \mathbb{Z}[x]$ is a monic polynomial, then for every polynomial $g \in \mathbb{Z}[x]$ such that $\deg(g) \geq \deg(f)$, there exists a polynomial h such that $\deg(g - fh) < \deg(f)$ and $\|h\|_\infty \leq \|g\|_\infty (2\|f\|_1)^{\lceil \frac{\deg(g)-\deg(f)}{\text{gap}(f)} \rceil}$.*

Proof. For convenience, let $k = \deg(g)$, $n = \deg(f)$, and $m = \text{gap}(f)$. Suppose that $g = g_0 = \sum_{i=0}^k \alpha_i x^i$ where $\alpha_i \in \mathbb{Z}$. Let $g_1 = g_0 - fh_1$ where $h_1 = \sum_{i=0}^{m-1} \alpha_{k-n-i} x^{k-n-i}$. We see that since $\|fh_1\|_\infty \leq \|f\|_1 \|g_0\|_\infty$, we have $\|g_1\|_\infty \leq \|g_0\|_\infty + \|f\|_1 \|g_0\|_\infty \leq 2\|f\|_1 \|g_0\|_\infty$. Because $\text{gap}(f) = m$, the coefficients of g_0 and fh_1 for the terms x^k, \dots, x^{k-m+1} match exactly, thus the subtraction of the two polynomials causes those higher power terms to disappear. So now g_1 is a polynomial whose degree is at most $k - m$ and $\|g_1\|_\infty \leq 2\|f\|_1 \|g_0\|_\infty$.

We proceed in the same fashion (i.e. keep constructing $g_i = g_{i-1} - fh_i$ such that $\deg(g_i) \leq \deg(g_{i-1}) - m$) until we end up with a polynomial of degree less than n . It will take at most $\lceil (k - n)/m \rceil + 1$ such subtractions. Notice that the infinity norm of g_i goes up by a factor of at most $2\|f\|_1$ with every subtraction, so $\|g_i\|_\infty \leq \|g\|_\infty (2\|f\|_1)^i$. Also notice that $\|h_i\|_\infty \leq \|g_{i-1}\|_\infty$. So at the end, we will get $g_{\lceil (k-n)/m \rceil + 1} = g - fh_1 - fh_2 - \dots - fh_{\lceil (k-n)/m \rceil + 1}$. Since none of the h_i 's have any powers of x in common, the $\|h_1 + \dots + h_{\lceil (k-n)/m \rceil + 1}\|_\infty = \max\{\|h_1\|_\infty, \dots, \|h_{\lceil (k-n)/m \rceil + 1}\|_\infty\} \leq \|g\|_\infty (2\|f\|_1)^{\lceil (k-n)/m \rceil}$. \square

Theorem C.4. *If f is a monic polynomial in $\mathbb{Z}[x]$, then for all polynomials $g \in \mathbb{Z}[x]$, we have*

$$\|g\|_f \leq \min_{f' \in \mathbb{Z}[x]} 2\|g\|_\infty \|f\|_1 \|f'\|_1 (2\|ff'\|_1)^{\lceil \frac{\deg(g)-\deg(f)}{\text{gap}(ff')} \rceil}$$

Proof. Consider the polynomial gf' . By Lemma C.3, there exists a polynomial h such that $\deg(gf' - hf') < \deg(ff')$ and

$$\begin{aligned} \|h\|_\infty &\leq \|gf'\|_\infty (2\|ff'\|_1)^{\lceil \frac{\deg(gf')-\deg(ff')}{\text{gap}(ff')} \rceil} \\ &= \|gf'\|_\infty (2\|ff'\|_1)^{\lceil \frac{\deg(g)-\deg(f)}{\text{gap}(ff')} \rceil} \end{aligned}$$

Now notice that the polynomial $\frac{gf'-hf'}{f'} = g - hf$ has degree less than $\deg(f)$, and is congruent to g in the ring $\mathbb{Z}[x]/\langle f \rangle$. Thus $\|g\|_f = \|g - hf\|_\infty$.

$$\begin{aligned} \|g\|_f &= \|g - hf\|_\infty \\ &\leq \|g\|_\infty + \|f\|_1 \|h\|_\infty \\ &\leq \|g\|_\infty + \|f\|_1 \|gf'\|_\infty (2\|ff'\|_1)^{\lceil \frac{\deg(g)-\deg(f)}{\text{gap}(ff')} \rceil} \\ &\leq 2\|g\|_\infty \|f\|_1 \|f'\|_1 (2\|ff'\|_1)^{\lceil \frac{\deg(g)-\deg(f)}{\text{gap}(ff')} \rceil} \end{aligned}$$

\square

In some cases, it may be possible to give a tighter bound for $\|g\|_f$ than the one given in the above theorem. The below bound is useful if $\deg(f')$ and $\|ff'\|_1$ are small constants and $\|f\|_1$ is much bigger than $\|f\|_\infty$.

Theorem C.5. *If f is a monic polynomial in $\mathbb{Z}[x]$, then for all polynomials $g \in \mathbb{Z}[x]$, we have*

$$\|g\|_f \leq \|g\|_\infty (2\|ff'\|_1)^{\left\lceil \frac{\deg(g) - \deg(ff')}{m} \right\rceil + 1} (2\|f\|_\infty)^{\deg(f')}$$

Proof. By Lemma C.3, there exists a polynomial h such that $\deg(g - hff') < \deg(ff')$ and

$$\|h\|_\infty \leq \|g\|_\infty (2\|ff'\|_1)^{\left\lceil \frac{\deg(g) - \deg(ff')}{\deg(ff')} \right\rceil}$$

If we let $r = g - hff'$, then

$$\begin{aligned} \|r\|_\infty &\leq \|g\|_\infty + \|hff'\|_\infty \\ &\leq \|g\|_\infty + \|h\|_\infty \|ff'\|_1 \\ &\leq \|g\|_\infty + \|g\|_\infty (2\|ff'\|_1)^{\left\lceil \frac{\deg(g) - \deg(ff')}{\deg(ff')} \right\rceil} \|ff'\|_1 \\ &\leq 2\|g\|_\infty (2\|ff'\|_1)^{\left\lceil \frac{\deg(g) - \deg(ff')}{\deg(ff')} \right\rceil} \|ff'\|_1 \\ &= \|g\|_\infty (2\|ff'\|_1)^{\left\lceil \frac{\deg(g) - \deg(ff')}{\deg(ff')} \right\rceil + 1} \end{aligned}$$

Since $r \equiv g$ in $\mathbb{Z}[x]/\langle f \rangle$, we have $\|g\|_f = \|r\|_f$. By Lemma C.2,

$$\|r\|_f \leq \|r\|_\infty (2\|f\|_\infty)^{\deg(r) - \deg(f) + 1}$$

Since $\deg(r) \leq \deg(ff') - 1$, we have that

$$\begin{aligned} \|r\|_f &\leq \|r\|_\infty (2\|f\|_\infty)^{\deg(f')} \\ &\leq \|g\|_\infty (2\|ff'\|_1)^{\left\lceil \frac{\deg(g) - \deg(ff')}{\deg(ff')} \right\rceil + 1} (2\|f\|_\infty)^{\deg(f')} \end{aligned}$$

□

We see that Theorem C.5 is tighter than Theorem C.4 whenever $\|f\|_1 \|f'\|_1 > (2\|f\|_\infty)^{\deg(f')} \|ff'\|_1$. An example of when this occurs is if $f = x^{n-1} + x^{n-2} + \dots + 1$ and $f' = x - 1$ and thus $ff' = x^n - 1$. We see that $\|f\|_1 \|f'\|_1 = 2n$ while $(2\|f\|_\infty)^{\deg(f')} \|ff'\|_1 = 4$. We also see that theorem 3.5 is a direct consequence of theorem C.4, and theorem 3.6 is a direct consequence of theorem C.5.

D Proof of lemma 2.6 (Non-essential technical appendix)

In this appendix, we will provide a proof of lemma 2.6. In all that follows, let ρ be defined the same way as in subsection 2.3, and let $\hat{\rho}$ be the fourier transform of ρ . That is, for vectors \mathbf{x} and \mathbf{y} , $\hat{\rho}(\mathbf{y}) = \int_{-\infty}^{\infty} \rho(\mathbf{x}) e^{-2\pi i \langle \mathbf{x}, \mathbf{y} \rangle} d\mathbf{x}$. Next, we state some general properties of the fourier transform. If h is defined by $h(\mathbf{x}) = g(\mathbf{x} + \mathbf{v})$ for some function g and vector \mathbf{v} then

$$\hat{h}(\mathbf{w}) = e^{2\pi i \langle \mathbf{v}, \mathbf{w} \rangle} \hat{g}(\mathbf{w}). \quad (7)$$

Another important fact is that the Gaussian is its own Fourier transform, i.e., $\hat{\rho} = \rho$. More generally, for any $s > 0$ it holds that $\hat{\rho}_s = s^n \rho_{1/s}$. We use the following formulation of the Poisson summation formula.

Lemma D.1. For any lattice Λ and any³ function $f : \mathbb{R}^n \rightarrow \mathbb{C}$, $f(\Lambda) = \det(\Lambda^*)\hat{f}(\Lambda^*)$ where \hat{f} denotes the Fourier transform of f .

The below proposition is just the value of the m^{th} moment of a standard normal gaussian. We do not provide a proof for it, although it is easily proved by integrating by parts.

Proposition D.2.

$$\int_{-\infty}^{\infty} x^m e^{-\pi x^2} dx = \begin{cases} \frac{m!}{(m/2)!(4\pi)^{m/2}} & \text{if } m \text{ is even,} \\ 0 & \text{if } m \text{ is odd.} \end{cases}$$

In the next lemma, we state the closed form of the fourier transform of the m^{th} moment of the standard normal gaussian.

Lemma D.3. For all values of y and integers $m \geq 0$, we have

$$\int_{-\infty}^{\infty} x^m e^{-\pi x^2} e^{-2\pi i x y} dx = \left((-i)^m m! \sum_{j=0}^{\lfloor \frac{m}{2} \rfloor} \frac{(-1)^j y^{m-2j}}{j!(m-2j)!(4\pi)^j} \right) \hat{\rho}(y)$$

(Note that when $y = 0$ and m is even, the term 0^0 will appear in the sum. But since when $y = 0$ proposition D.2 applies, in order to make this lemma include proposition D.2, we'll assume that $0^0 = 1$.)

Proof. The proof is by induction. We will need to establish base cases for $m = 0$ and $m = 1$. For $m = 0$, the equality clearly holds. For $m = 1$, we need to show that

$$\int_{-\infty}^{\infty} x e^{-\pi x^2} e^{-2\pi i x y} dx = -iy \hat{\rho}(y) \quad (8)$$

It's not difficult to show the above by integrating by parts.

Now we assume that the lemma is true for all values of y and all $k < m + 2$. We will prove that

$$\int_{-\infty}^{\infty} x^{k+2} e^{-\pi x^2} e^{-2\pi i x y} dx = \left((-i)^{k+2} (k+2)! \sum_{j=0}^{\lfloor \frac{k+2}{2} \rfloor} \frac{(-1)^j y^{k+2-2j}}{j!(k+2-2j)!(4\pi)^j} \right) \hat{\rho}(y) \quad (9)$$

Integrating the the above by parts and using the induction hypothesis, we get

$$\int_{-\infty}^{\infty} x^{k+2} e^{-\pi x^2} e^{-2\pi i x y} dx = \frac{k+1}{2\pi} \int_{-\infty}^{\infty} x^k e^{-\pi x^2} e^{-2\pi i x y} dx - iy \int_{-\infty}^{\infty} x^{k+1} e^{-\pi x^2} e^{-2\pi i x y} dx \quad (10)$$

$$= \frac{k+1}{2\pi} \left((-i)^k k! \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} \frac{(-1)^j y^{k-2j}}{j!(k-2j)!(4\pi)^j} \right) \hat{\rho}(y) - iy \left((-i)^{k+1} (k+1)! \sum_{j=0}^{\lfloor \frac{k+1}{2} \rfloor} \frac{(-1)^j y^{k+1-2j}}{j!(k+1-2j)!(4\pi)^j} \right) \hat{\rho}(y) \quad (11)$$

$$= (-i)^{k+2} (k+2)! \left(\frac{-1}{2\pi(k+2)} \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} \frac{(-1)^j y^{k-2j}}{j!(k-2j)!(4\pi)^j} + \frac{1}{k+2} \sum_{j=0}^{\lfloor \frac{k+1}{2} \rfloor} \frac{(-1)^j y^{k+2-2j}}{j!(k+1-2j)!(4\pi)^j} \right) \hat{\rho}(y) \quad (12)$$

We will show that equation (12) is equivalent to the right side of equation (9) by showing that the coefficients of like powers of y are equivalent. The $(-i)^{k+2} (k+2)! \hat{\rho}(y)$ part is the same in both equations, so we'll be ignoring it. Notice that to get the coefficient of the term y^{k+2-2l} , we need to look at the coefficient of the term we get for $j = l - 1$ in the first sum of equation (12) and for $j = l$ in the second sum. Some special cases occur when $l = 0$ or $l = \lfloor \frac{k+2}{2} \rfloor$ (then $j = l - 1$ and $j = l$ may not exist as terms in both sums) but let's

³For this formula to hold, f needs to satisfy certain niceness assumptions. These assumptions always hold in our applications. See [8] for more details.

first handle the general case first (i.e. the coefficient of y^{k+2-2l} comes from both terms of equation (12)). We need to show that

$$\frac{-1}{2\pi(k+2)} \cdot \frac{(-1)^{l-1} y^{k-2(l-1)}}{(k-2(l-1))!(l-1)!(4\pi)^{l-1}} + \frac{1}{k+2} \cdot \frac{(-1)^l y^{k+2-2l}}{(k+1-2l)!l!(4\pi)^l} = \frac{(-1)^l y^{k-2l+2}}{(k+2-2l)!l!(4\pi)^l} \quad (13)$$

The above equality is not too hard to show with a little algebra manipulation. Now we come to the special cases. If $l = 0$, then the coefficient of y^{k+2-2l} comes entirely from the second sum of equation (12). Plugging in, we get

$$\frac{1}{k+2} \cdot \frac{(-1)^0 y^{k+2-2 \cdot 0}}{0!(k+1-2 \cdot 0)!(4\pi)^0} = \frac{y^{k+2}}{(k+2)!}$$

and thus the coefficients of the y^{k+2} term are the same in equations (12) and (9). Now we consider the case when $l = \lfloor \frac{k+2}{2} \rfloor$. Here, two subcases arise. The simple one is if k is odd. In this subcase, $\lfloor \frac{k+2}{2} \rfloor = \lfloor \frac{k+1}{2} \rfloor$, and thus the coefficient of y^{k+2-2l} comes from both sums of equation (12) and this case has been already handled by equation (13). In the other subcase, $\lfloor \frac{k+2}{2} \rfloor \neq \lfloor \frac{k+1}{2} \rfloor$, and so k must be even, and thus $l = \frac{k}{2} + 1$. In this subcase, the coefficient of $y^{k+2-2l} = y^0$ comes from only the first sum of equation (12). That coefficient is what we get when $j = \frac{k}{2}$, and it's

$$\frac{-1}{2\pi(k+2)} \cdot \frac{(-1)^{\frac{k}{2}}}{(\frac{k}{2})!(4\pi)^{\frac{k}{2}}} = \frac{(-1)^{\frac{k}{2}+1}}{4\pi(\frac{k}{2}+1)(\frac{k}{2})!(4\pi)^{\frac{k}{2}}} = \frac{(-1)^{\frac{k}{2}+1}}{(\frac{k}{2}+1)!(4\pi)^{\frac{k}{2}+1}}$$

which is exactly the term in equation (9) when $j = \frac{k}{2} + 1$. \square

In the next two lemmas, we define the function $g_m(\mathbf{x}) = (x_1 - c_1)^m \rho_{\mathbf{c}}(\mathbf{x})$ (where x_1 and c_1 are the first coordinates of \mathbf{x} and \mathbf{c} respectively) and will bound the absolute value of its fourier transform. The reason for doing this will become clear in lemma D.6

Lemma D.4. *If $g_m(\mathbf{x}) = (x_1 - c_1)^m \rho_{\mathbf{c}}(\mathbf{x})$, then*

$$\widehat{g}_m(\mathbf{y}) = \left((-i)^m m! \sum_{j=0}^{\lfloor \frac{m}{2} \rfloor} \frac{(-1)^j y_1^{m-2j}}{j!(m-2j)!(4\pi)^j} \right) \widehat{\rho}_{\mathbf{c}}(\mathbf{y})$$

(The same caveat applies here as in Lemma D.3, i.e. if $y_1 = 0$ and m is even, then 0^0 will appear in the sum. And again for notational convenience, let $0^0 = 1$ in this case.)

Proof. Define the function

$$f_m(\mathbf{x}) = g_m(\mathbf{x} + \mathbf{c}) = x_1^m \rho_{\mathbf{c}}(\mathbf{x} + \mathbf{c}) = x_1^m \rho(\mathbf{x})$$

This means that the fourier transform of $g_m(\mathbf{x})$ is

$$\widehat{g}_m(\mathbf{y}) = \widehat{f}_m(\mathbf{y}) e^{-2\pi i \langle \mathbf{c}, \mathbf{y} \rangle} \quad (14)$$

Define \mathbf{x}' to be the vector \mathbf{x} with the first coordinate removed, and similarly let \mathbf{y}' be the vector \mathbf{y} with the first coordinate removed So,

$$f_m(\mathbf{x}) = x_1^m \rho(\mathbf{x}) = x_1^m \rho(x_1) \rho(\mathbf{x}') \quad (15)$$

and

$$\widehat{f}_m(\mathbf{y}) = \left(\int_{-\infty}^{\infty} x_1^m e^{-\pi x_1^2} e^{-2\pi i x_1 y_1} dx_1 \right) \widehat{\rho}(\mathbf{y}') \quad (16)$$

$$= \left((-i)^m m! \sum_{j=0}^{\lfloor \frac{m}{2} \rfloor} \frac{(-1)^j y_1^{m-2j}}{j!(m-2j)!(4\pi)^j} \right) \widehat{\rho}(y_1) \widehat{\rho}(\mathbf{y}') \quad (17)$$

$$= \left((-i)^m m! \sum_{j=0}^{\lfloor \frac{m}{2} \rfloor} \frac{(-1)^j y_1^{m-2j}}{j!(m-2j)!(4\pi)^j} \right) \widehat{\rho}(\mathbf{y}) \quad (18)$$

where the second equality follows from lemma D.3. And since

$$\widehat{\rho}_c(\mathbf{y}) = \widehat{\rho}(\mathbf{y})e^{-2\pi i\langle \mathbf{c}, \mathbf{y} \rangle}$$

we combine equations (14) and (18) to obtain the claim in the lemma. \square

Lemma D.5.

$$|\widehat{g}_m(\mathbf{y})| \leq \begin{cases} \frac{m!}{(m/2)!(4\pi)^{m/2}} & \text{if } m \text{ is even and } \mathbf{y} = \mathbf{0}, \\ 0 & \text{if } m \text{ is odd and } \mathbf{y} = \mathbf{0}, \\ m^{2m} \rho_2(\mathbf{y}) & \text{in all other cases.} \end{cases}$$

Proof. Since $|\widehat{\rho}_c(\mathbf{y})| = \rho(\mathbf{y})$, we have by lemma D.4,

$$|\widehat{g}_m(\mathbf{y})| = \left| (-i)^m m! \sum_{j=0}^{\lfloor \frac{m}{2} \rfloor} \frac{(-1)^j y_1^{m-2j}}{j!(m-2j)!(4\pi)^j} \right| \rho(\mathbf{y}) \quad (19)$$

Now we will quickly dispatch of the case where $\mathbf{y} = \mathbf{0}$. In this case $\rho(\mathbf{y}) = 1$ and all the terms in the sum in equation (19) will cancel out except possibly $y_1^{m-2\lfloor \frac{m}{2} \rfloor}$ (because remember that we assumed that $0^0 = 1$). If m is odd, then the exponent will not be 0, thus the sum will be 0, and if m is even, then the exponent will be 0. Thus, the sum will have the value of the term when $j = \frac{m}{2}$, which is what is claimed in the lemma. Now we will handle an easy subcase of the ‘‘all other cases.’’ The subcase is when $\mathbf{y} \neq \mathbf{0}$ but $y_1 = 0$. In this subcase, the sum in equation (19) is equal to 0 when m is odd and is equal to $\frac{m!}{(m/2)!(4\pi)^{m/2}}$ when m is even. Either way, the product of this sum with $\rho(\mathbf{y})$ is less than $m^{2m} \rho_2(\mathbf{y})$. Now we will handle all the remaining cases (i.e. when $y_1 \neq 0$).

$$|\widehat{g}_m(\mathbf{y})| = \left| (-i)^m m! \sum_{j=0}^{\lfloor \frac{m}{2} \rfloor} \frac{(-1)^j y_1^{m-2j}}{j!(m-2j)!(4\pi)^j} \right| \rho(\mathbf{y}) \quad (20)$$

$$\leq m! \sum_{j=0}^{\lfloor \frac{m}{2} \rfloor} \left| \frac{(-1)^j y_1^{m-2j}}{j!(m-2j)!(4\pi)^j} \right| \rho(\mathbf{y}) \quad (21)$$

Note that if $|y_1| \leq 1$, then $\left| \frac{(-1)^j y_1^{m-2j}}{j!(m-2j)!(4\pi)^j} \right| \leq 1$ and thus equation (21) is at most $(\lfloor \frac{m}{2} \rfloor + 1)m! \rho(\mathbf{y})$ which is less than $m^{2m} \rho_2(\mathbf{y})$. So let's now assume that $|y_1| \geq 1$. Then we have

$$\begin{aligned} |\widehat{g}_m(\mathbf{y})| &\leq m! \sum_{j=0}^{\lfloor \frac{m}{2} \rfloor} \left| \frac{(-1)^j y_1^{m-2j}}{j!(m-2j)!(4\pi)^j} \right| \rho(\mathbf{y}) \\ &\leq \left(\frac{m}{2} + 1 \right) m! y_1^m \rho(\mathbf{y}) \\ &= \left(\frac{m}{2} + 1 \right) m! m^{2m/3} \frac{y_1^m}{m^{2m/3}} \rho(y_1) \rho(\mathbf{y}') \\ &\leq m^{2m} \frac{y_1^m}{m^{2m/3}} \rho(y_1) \rho_2(\mathbf{y}') \end{aligned}$$

where we recall that \mathbf{y}' is defined as the vector \mathbf{y} with the first component removed. So all that is left to complete the proof of the lemma is to show that

$$\frac{y_1^m}{m^{2m/3}} \rho(y_1) \leq \rho_2(y_1) \quad (22)$$

Consider the case where $y_1 \leq m^{2/3}$. Then equation (22) is clearly true. In the case where $y_1 > m^{2/3}$, we need to show that

$$y_1^m e^{-\pi y_1^2} \leq e^{-\pi (\frac{y_1}{2})^2}$$

or equivalently that

$$m \log y_1 \leq \frac{3}{4} \pi y_1^2$$

Since $y_1 > m^{2/3}$, we have

$$\frac{3}{4} \pi y_1^2 = \frac{3}{4} \pi y_1^{\frac{1}{2}} y_1^{\frac{3}{2}} > \frac{3}{4} \pi y_1^{\frac{1}{2}} m > m \log y_1$$

This proves equation (22) and thus the lemma. \square

The next lemma is a generalization and closely follows the outline of lemma 4.2 of [14]. The main difference is the technique for bounding the function \widehat{g}_m , which was done in lemmas D.4 and D.5.

Lemma D.6. *For any n -dimensional lattice Λ , point $\mathbf{c} \in \mathbb{R}^n$, unit vector \mathbf{u} , positive real $s > 2\eta_\epsilon(\Lambda)$, and all positive integers m ,*

$$|\text{Exp}_{x \sim D_{\Lambda, s, \mathbf{c}}} [\langle \mathbf{x} - \mathbf{c}, \mathbf{u} \rangle^m]| \leq \begin{cases} s^m \left(\frac{\frac{m!}{(m/2)!(4\pi)^{m/2}} + m^{2m}\epsilon}{1-\epsilon} \right) & \text{if } m \text{ is even} \\ s^m \left(\frac{m^{2m}\epsilon}{1-\epsilon} \right) & \text{if } m \text{ is odd} \end{cases}$$

Proof. For any positive real $s > 0$, define $\Lambda' = \Lambda/s$, $\mathbf{c}' = \mathbf{c}/s$. Notice that, for any \mathbf{x} ,

$$\Pr\{D_{\Lambda, s, \mathbf{c}} = s\mathbf{x}\} = \frac{\rho_{s, \mathbf{c}}(s\mathbf{x})}{\rho_{s, \mathbf{c}}(\Lambda)} = \frac{\rho_{\mathbf{c}'}(\mathbf{x})}{\rho_{\mathbf{c}'}(\Lambda')} = \Pr\{D_{\Lambda', \mathbf{c}'} = \mathbf{x}\},$$

i.e., the distribution $D_{\Lambda, s, \mathbf{c}}$ is equal to $D_{\Lambda', \mathbf{c}'}$ scaled by a factor of s . Therefore, it is enough to prove the lemma for $s = 1$. The general case follows by scaling the lattice by a factor s .

In the rest of the proof, we assume $s = 1$. We want to estimate the quantity $\text{Exp}_{\mathbf{x} \sim D_{\Lambda, \mathbf{c}}} [\langle \mathbf{x} - \mathbf{c}, \mathbf{u} \rangle^m]$. Without loss of generality, assume that \mathbf{u} is the vector $(1, 0, \dots, 0)$. We will show the lemma true for $s = 1$ and the general case will follow by scaling the lattice by a factor s .

Notice that

$$\text{Exp}_{\mathbf{x} \sim D_{\Lambda, \mathbf{c}}} [\langle \mathbf{x} - \mathbf{c}, \mathbf{u} \rangle^m] = \text{Exp}_{\mathbf{x} \sim D_{\Lambda, \mathbf{c}}} [(x_1 - c_1)^m] = \frac{g_j(\Lambda)}{\rho_{\mathbf{c}}(\Lambda)}.$$

Applying Poisson's summation formula (Lemma D.1) to the numerator and denominator, the above fraction can be rewritten as

$$\text{Exp}_{\mathbf{x} \sim D_{\Lambda, \mathbf{c}}} [\langle \mathbf{x} - \mathbf{c}, \mathbf{u} \rangle^m] = \frac{\det(\Lambda^*) \cdot \widehat{g}_m(\Lambda^*)}{\det(\Lambda^*) \cdot \widehat{\rho}_{\mathbf{c}}(\Lambda^*)} = \frac{\widehat{g}_m(\Lambda^*)}{\widehat{\rho}_{\mathbf{c}}(\Lambda^*)}. \quad (23)$$

The Fourier transform $\widehat{\rho}_{\mathbf{c}}$ is easily computed using Equation 7: $\widehat{\rho}_{\mathbf{c}}(\mathbf{y}) = \rho(\mathbf{y})e^{-2\pi i \langle \mathbf{y}, \mathbf{c} \rangle}$. In particular, $\widehat{\rho}_{\mathbf{c}}(\mathbf{0}) = 1$, $|\widehat{\rho}_{\mathbf{c}}(\mathbf{y})| = \rho(\mathbf{y})$, and

$$|\widehat{\rho}_{\mathbf{c}}(\Lambda^*)| = \left| 1 + \sum_{\mathbf{y} \in \Lambda^* \setminus \{\mathbf{0}\}} \widehat{\rho}_{\mathbf{c}}(\mathbf{y}) \right| \geq 1 - \rho(\Lambda^* \setminus \{\mathbf{0}\}). \quad (24)$$

Thus, we get the equation

$$\text{Exp}_{x \sim D_{\Lambda, s, \mathbf{c}}} [\langle \mathbf{x} - \mathbf{c}, \mathbf{u} \rangle^m] = \frac{\widehat{g}_m(\Lambda^*)}{\widehat{\rho}_{\mathbf{c}}(\Lambda^*)} \leq \frac{\widehat{g}_m(\Lambda^*)}{1-\epsilon} = \frac{\sum_{\mathbf{y} \in \Lambda^*} \widehat{g}_m(\mathbf{y})}{1-\epsilon} = \frac{\widehat{g}_m(\mathbf{0}) + \sum_{\mathbf{y} \in \Lambda^* \setminus \{\mathbf{0}\}} \widehat{g}_m(\mathbf{y})}{1-\epsilon} \quad (25)$$

Now we apply lemma D.5 to get

$$|\text{Exp}_{x \sim D_{\Lambda, s, \mathbf{c}}} [\langle \mathbf{x} - \mathbf{c}, \mathbf{u} \rangle^m]| \leq \frac{|\widehat{g}_m(\mathbf{0})| + \sum_{\mathbf{y} \in \Lambda^* \setminus \{\mathbf{0}\}} m^{2m} \rho_2(\mathbf{y})}{1-\epsilon} = \frac{|\widehat{g}_m(\mathbf{0})| + m^{2m} \rho_2(\Lambda^* \setminus \{\mathbf{0}\})}{1-\epsilon}$$

which gives us the claim in the lemma. \square

The below lemma is a restatement and proof of lemma 2.6

Lemma D.7. For any n -dimensional lattice Λ , point $\mathbf{c} \in \mathbb{R}^n$, unit vector \mathbf{u} , positive real $s > 2\eta_\epsilon(\Lambda)$ where $\epsilon < (\log n)^{-2 \log n}$,

$$Pr_{x \sim D_{\Lambda, s, \mathbf{c}}} [|\langle \mathbf{x} - \mathbf{c}, \mathbf{u} \rangle| \geq s \log n] = n^{-\omega(1)}$$

Proof. For simplicity, assume that $\lfloor \log n \rfloor$ is an even integer. Then by lemma D.6 we have

$$\left| Exp_{x \sim D_{\Lambda, s, \mathbf{c}}} \left[\langle \mathbf{x} - \mathbf{c}, \mathbf{u} \rangle^{\lfloor \log n \rfloor} \right] \right| \leq s^{\lfloor \log n \rfloor} \left(\frac{\frac{(\log n)!}{((\log n)/2)!(4\pi)^{(\log n)/2}} + (\log n)^{2 \log n} \epsilon}{1 - \epsilon} \right) \leq 2s^{\lfloor \log n \rfloor} (\log n)^{\frac{\log n}{2}} \quad (26)$$

Using the above equation, we obtain

$$\begin{aligned} Pr_{x \sim D_{\Lambda, s, \mathbf{c}}} [|\langle \mathbf{x} - \mathbf{c}, \mathbf{u} \rangle| \geq s \log n] &= Pr_{x \sim D_{\Lambda, s, \mathbf{c}}} \left[\langle \mathbf{x} - \mathbf{c}, \mathbf{u} \rangle^{\lfloor \log n \rfloor} \geq (s \log n)^{\lfloor \log n \rfloor} \right] \\ &\leq \frac{\left| Exp_{x \sim D_{\Lambda, s, \mathbf{c}}} \left[\langle \mathbf{x} - \mathbf{c}, \mathbf{u} \rangle^{\lfloor \log n \rfloor} \right] \right|}{(s \log n)^{\lfloor \log n \rfloor}} \\ &\leq \frac{2s^{\lfloor \log n \rfloor} (\log n)^{\frac{\log n}{2}}}{(s \log n)^{\lfloor \log n \rfloor}} \\ &\leq n^{-\frac{\log \log n}{3}} = n^{-\omega(1)} \end{aligned}$$

where the first inequality follows by Markov's inequality. \square

E Random polynomial lemma (Non-essential technical appendix)

Proposition E.1 (Hoeffding Bound). Let X_1, \dots, X_n be independent random variables with mean μ taking values in the real interval $[a, b]$ and let $X = X_1 + \dots + X_n$. Then for any k , we have

$$Pr[|X - \mu n| \geq k] \leq 2e^{-\frac{2k^2}{n(b-a)^2}}$$

Lemma E.2. Let g be any polynomial of degree n . Let r be a polynomial of degree n where every coefficient of r is independently distributed in the range $[-a, a]$ with mean 0. Then

$$Pr[\|gr\|_\infty \geq \omega(\sqrt{n \log n}) \|g\|_\infty 2a] \leq 4ne^{-\omega(\log n)}$$

Proof. Since every coefficient of r is an independent random variable in the range $[-a, a]$ with mean 0, every coefficient of gr is a sum of at most n independent variables in the range $[-a\|g\|_\infty, a\|g\|_\infty]$. Applying proposition E.1, we get that the probability that the absolute value of any particular coefficient of gr is greater than $\omega(\sqrt{n \log n}) \|g\|_\infty 2a$ is less than $2e^{-\omega(\log n)}$. By applying the union bound over all the coefficients of gr , we get the claim in the lemma. \square