Hardness of the (Approximate) Shortest Vector Problem: A Simple Proof via Reed-Solomon Codes*

Huck Bennett
Oregon State University, Corvallis, OR, USA

Chris Peikert
University of Michigan, Ann Arbor, MI, USA
Algorand, Inc., Boston, MA, USA

Abstract

We give a *simple* proof that the (approximate, decisional) Shortest Vector Problem is NP-hard under a randomized reduction. Specifically, we show that for any $p \geq 1$ and any constant $\gamma < 2^{1/p}$, the γ-approximate problem in the ℓ_p norm (γ-GapSVP$_p$) is not in RP unless NP $\subseteq$ RP. Our proof follows an approach pioneered by Ajtai (STOC 1998), and strengthened by Micciancio (FOCS 1998 and SICOMP 2000), for showing hardness of γ-GapSVP$_p$ using *locally dense lattices*. We construct such lattices simply by applying "Construction A" to Reed-Solomon codes with suitable parameters, and prove their local density via an elementary argument originally used in the context of Craig lattices.

As in all known NP-hardness results for GapSVP$_p$ with $p < \infty$, our reduction uses randomness. Indeed, it is a notorious open problem to prove NP-hardness via a deterministic reduction. To this end, we additionally discuss potential directions and associated challenges for derandomizing our reduction. In particular, we show that a close deterministic analogue of our local density construction would improve on the state-of-the-art explicit Reed-Solomon list-decoding lower bounds of Guruswami and Rudra (STOC 2005 and IEEE Transactions on Information Theory 2006).

As a related contribution of independent interest, we also give a polynomial-time algorithm for decoding n-dimensional "Construction A Reed-Solomon lattices" (with different parameters than those used in our hardness proof) to a distance within an $O(\sqrt{\log n})$ factor of Minkowski's bound. This asymptotically matches the best known distance for decoding near Minkowski's bound, due to Mook and Peikert (IEEE Transactions on Information Theory 2022), whose work we build on with a somewhat simpler construction and analysis.

2012 ACM Subject Classification Theory of computation → Problems, reductions and completeness; Theory of computation → Error-correcting codes; Theory of computation → Pseudorandomness and derandomization

Keywords and phrases Lattices, Shortest Vector Problem, Reed-Solomon codes, NP-hardness, derandomization

Digital Object Identifier 10.4230/LIPIcs.APPROX/RANDOM.2023.37

Category RANDOM

Related Version *Full Version*: https://arxiv.org/abs/2202.07736 [6]

Funding *Huck Bennett*: Part of this work was completed while the author was at the University of Michigan and supported by NSF Grant No. CCF-2006857. The views expressed are those of the authors and do not necessarily reflect the official policy or position of the NSF.
Chris Peikert: This author's work was supported by NSF Grant No. CCF-2006857.

Acknowledgements We thank Swastik Kopparty [29] for very helpful answers to several of our questions.

* Due to space constraints, this version of the paper omits some material. We strongly encourage the reader to view the full version [6].

1 Introduction

> [I]t may easily happen that other, perhaps in some sense simpler, lattices also have the properties that are required from L to complete the proof... There are different reasons which may motivate the search for such a lattice: to make the proof deterministic; to improve the factor in the approximation result; to make the proof simpler.
>
> Miklós Ajtai, [3, Remark 2]

A *lattice* $\mathcal{L}$ is the set of all integer linear combinations of some n linearly independent vectors $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n \in \mathbb{R}^m$. The matrix $B = (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)$ whose columns are these vectors is called a *basis* of $\mathcal{L}$, and n is called its *rank*. Formally, the lattice $\mathcal{L}$ generated by B is defined as

$$\mathcal{L} = \mathcal{L}(B) := \left\{ \sum_{i=1}^{n} a_i \boldsymbol{b}_i : a_1, \ldots, a_n \in \mathbb{Z} \right\}.$$

Lattices are classically studied mathematical objects, and have proved invaluable in many computer science applications, especially the design and analysis of cryptosystems. Indeed, the area of lattice-based cryptography, which designs cryptosystems whose security is based on the apparent intractability of certain computational problems on lattices, has flourished over the past quarter century. (See [36] and its bibliography for a comprehensive summary and list of references.)

The central computational problem on lattices is the Shortest Vector Problem (SVP): given a lattice basis B as input, the goal is to find a shortest non-zero vector in $\mathcal{L}(B)$. This paper is concerned with its γ-approximate decision version in the ℓ_p norm (γ-GapSVP$_p$), where $p \geq 1$ is fixed and the approximation factor $\gamma = \gamma(n) \geq 1$ is some function of the lattice rank n (often a constant). Here the input additionally includes a distance threshold $s > 0$, and the goal is to determine whether the length (in the ℓ_p norm) $\lambda_1^{(p)}(\mathcal{L}) := \min_{\boldsymbol{v} \in \mathcal{L} \setminus \{\boldsymbol{0}\}} \|\boldsymbol{v}\|_p$ of the shortest non-zero vector in $\mathcal{L}$ is at most s, or is strictly greater than γs, when one of the two cases is promised to hold. For the exact problem, where $\gamma = 1$, we often simply write GapSVP$_p$.

Motivated especially by its central role in the security of lattice-based cryptography, understanding the complexity of γ-GapSVP has been the subject of a long line of work. In an early technical report, van Emde Boas [38] initiated the study of the hardness of lattice problems more generally, and in particular showed that GapSVP$_\infty$ is NP-hard. Seventeen years later, Ajtai [3] finally showed similar hardness for the important Euclidean case of $p = 2$, i.e., he showed that exact GapSVP$_2$ is NP-hard, though under a *randomized* reduction. Subsequent work [10, 31, 27, 26, 23, 32] improved this by showing that γ-GapSVP$_p$ in any ℓ_p norm is NP-hard to approximate for any constant $\gamma \geq 1$, and hard for nearly polynomial factors $\gamma = n^{\Omega(1/\log\log n)}$ assuming stronger complexity assumptions, also using randomized reductions. Recent work [1, 7] has also shown the *fine-grained* hardness of γ-GapSVP$_p$ for small constants γ (again under randomized reductions). On the other hand, γ-GapSVP$_p$ for finite $p \geq 2$ is unlikely to be NP-hard for approximation factors $\gamma \geq C_p\sqrt{n}$ (where C_p is a constant depending only on p) [18, 2, 35], and the security of lattice-based cryptography relies on the conjectured hardness of GapSVP or other problems for even larger (but typically polynomial) factors.

While this line of work has been very successful in showing progressively stronger hardness of approximation and fine-grained hardness for γ-GapSVP$_p$, it leaves some other important issues unresolved. First, for $p \neq \infty$ the hardness reductions and their analysis are rather complicated, and second, they are randomized. Indeed, it is a notorious, long-standing open

problem to prove that GapSVP$_p$ is NP-hard, even in its exact form, under a deterministic reduction for some finite p. While there have been some potential steps in this direction [31, 32], e.g., using plausible number-theoretic conjectures that appear very hard to prove, there has been no new progress on this front for a decade.

1.1 Our Contributions

The primary contribution of this work is to give a substantially simpler proof that γ-GapSVP$_p$ is NP-hard under a randomized reduction, for any $p \geq 1$ and constant $\gamma < 2^{1/p}$. The heart of our reduction is a family of "gadget" lattices $\mathcal{L}$ derived from Reed-Solomon codes $\mathcal{C} \subseteq \mathbb{F}_q^n$ (for prime q) via the very natural "Construction A" [13], which simply sets $\mathcal{L} = \mathcal{C} + q\mathbb{Z}^n$. These lattices and their properties were previously studied in work of Karabed, Roth, and Siegel [25, 37]. Additionally, they are closely related to a family of algebraic lattices studied by Craig [14]. We take advantage of this prior work in our analysis (see Section 1.3 for details).

▶ **Theorem 1** (Hardness of γ-GapSVP$_p$)**.** *For any $p \geq 1$ and constant γ satisfying $1 \leq \gamma < 2^{1/p}$, γ-GapSVP$_p$ is not in* RP *unless* NP $\subseteq$ RP*.*

We note that Theorem 1 is actually identical to the main result in [31]. As such, it matches the best known NP-hardness of approximation for γ-GapSVP$_p$ (i.e., largest γ) achieved by a "one-shot" reduction for all sufficiently small p, including $p = 2$. By "one-shot," we mean that the reduction does not amplify the approximation factor from an initial fixed constant to an arbitrary constant (or more) via tensoring, as is done in [26, 23, 32]. (It is an interesting question whether our hard γ-GapSVP$_p$ instances are amenable to tensoring; see Section 1.4.)

Although our reduction still uses randomness, we believe that it may be easier to derandomize than previous reductions, both due to its simplicity, and because of its close connection to prior work showing hardness of minimum distance problem on codes via a deterministic reduction [12]. To that end, in the full version of our paper [6] we also describe two approaches to potentially derandomizing our reduction, both of which aim to deterministically construct a particular lattice coset and lower bound the number of short vectors in it (see Section 1.2 for the motivation for this). The first approach is based on Fourier analysis, using similar techniques to those in [12], and the second is based on "smooth" proxies for point-counting functions.

In the full version of our paper [6] we also show that a close deterministic analog of our randomized local-density construction would imply improved explicit Reed-Solomon list-decoding lower bounds, going beyond the current state of the art from [20]. One may interpret this implication either pessimistically, as a barrier to a very strong derandomization of our reduction, or optimistically, as a potential route to improve Reed-Solomon list-decoding lower bounds. Here there is a further connection between the two problems, in that [20] obtains its list-decoding lower bounds by using the same Fourier-analytic tool underlying one of our derandomization attempts – specifically, the Weil bound for character sums . Unfortunately, the Weil bound falls just short of what we need in our context. (The Weil bound and related techniques were first used for counting Reed-Solomon code words in [11], and were also used in the deterministic hardness reduction for the minimum distance problem on codes in [12].)

Efficient decoding near Minkowski's bound. As a separate contribution of independent interest, in Appendix A we give a polynomial-time algorithm for decoding "Construction A Reed-Solomon lattices" of rank n – the same family of lattices as in our hardness reduction, but instantiated with different parameters – to a distance within a $O(\sqrt{\log n})$ factor of

Minkowski's bound.[1] The $O(\sqrt{\log n})$ factor in our result asymptotically matches the best factor known from prior work [34], which is for a different family of lattices. In fact, we rely on one of the main underlying theorems from that work, but give a simpler construction and analysis based on individual Reed-Solomon codes instead of towers of BCH codes.

Let $\mathrm{RS}_q[k, S]$ denote the dimension-k Reed-Solomon code over $\mathbb{F}_q$ with evaluation set S (defined below in Equation (3)). Note that $n = q$ is the rank of the lattice $\mathcal{L}$ in the following theorem.

▶ **Theorem 2** (Decoding near Minkowski's bound, informal)**.** *Let q be prime and let $k := \lfloor q/(2\log_2 q) \rfloor \le q/2$. Then for the "Construction A Reed-Solomon" lattice $\mathcal{L} := \mathrm{RS}_q[q-k, \mathbb{F}_q] + q\mathbb{Z}^q \subseteq \mathbb{Z}^q$:*

1. *We have $\Omega(\sqrt{q/\log q}) \le \lambda_1(\mathcal{L}) \le \sqrt{q} \cdot \det(\mathcal{L})^{1/q} \le O(\sqrt{q})$, i.e., the minimum distance is within a $O(\sqrt{\log q})$ factor of Minkowski's bound.*
2. *There is an algorithm that, on input q and a vector $\boldsymbol{y} \in \mathbb{R}^q$, outputs all lattice vectors $\boldsymbol{v} \in \mathcal{L}$ satisfying $\|\boldsymbol{y} - \boldsymbol{v}\| \le C\sqrt{k} \approx C\sqrt{q/(2\log_2 q)}$ in time polynomial in q, for some universal constant $C > 0$.*

This result adds to a separate line of work on efficient (list) decoding for various families of lattices [33, 19, 15, 34]. Recently, Ducas and van Woerden [16] further motivated this study by showing cryptographic applications of lattices that can be efficiently decoded near Minkowski's bound. (However, their application is most compelling when the minimum distances of both the lattice and its dual are close to Minkowski's bound, which is not the case in the present setting.)

1.2 Technical Overview

Here we give an overview of the key new elements in the proof of our main hardness theorem (Theorem 1), which are the focus of Section 3. For concision, we defer the technical aspects of our efficient decoding algorithm to Appendix A and of our derandomization attempts to the full version of our paper [6], respectively.

Besides using randomness, another common feature in nearly all prior hardness results for GapSVP_p is the use of *locally dense lattices* as advice (the only exception being [27]). Roughly speaking, a locally dense lattice for relative distance $\alpha \in (0,1)$ in the ℓ_p norm is a lattice $\mathcal{L}$ and a coset $\boldsymbol{x} + \mathcal{L}$ (i.e., the lattice "shifted by" some vector $\boldsymbol{x}$) such that there are at least subexponentially many (in the lattice rank) vectors $\boldsymbol{v} \in \boldsymbol{x} + \mathcal{L}$ satisfying $\|\boldsymbol{v}\|_p \le \alpha \cdot \lambda_1^{(p)}(\mathcal{L})$. One may view such a coset $\boldsymbol{x} + \mathcal{L}$ as a "bad" configuration for list-decoding $\mathcal{L}$ to within relative distance α in the ℓ_p norm, because there are many lattice vectors relatively close to $-\boldsymbol{x}$.[2]

Prior works have obtained locally density from a variety of lattice families: the Schnorr-Adelman prime number lattices [3, 10, 31]; a variant of Construction A [26] and Construction D [32] applied to (towers of) BCH codes; and random sublattices of $\mathbb{Z}^n$ and lattices with exponential kissing number [1, 7]. In this work, we give a simple construction of locally dense lattices from Reed-Solomon codes, as described below.

---

[1] Minkowski's bound gives an upper bound on the "normalized density" of a lattice $\mathcal{L}$. Specifically, it asserts that $\lambda_1^{(2)}(\mathcal{L}) \le \sqrt{n} \cdot \det(\mathcal{L})^{1/n}$ for all rank-n lattices $\mathcal{L}$, where $\det(\mathcal{L}) = \sqrt{\det(B^T B)}$ for any basis B of $\mathcal{L}$.

[2] For technical reasons, the formal definition of local density, given in Definition 8, also requires a linear transform that maps the short vectors in $\boldsymbol{x} + \mathcal{L}$ onto the set of all binary vectors of a given dimension. Such a transform can be obtained by random sampling using a probabilistic version of Sauer's Lemma (see Theorem 9) that is now standard in this context [3, 31]. Therefore, we defer further discussion of this issue to the main body.

Our main reduction (Theorem 12) shows how to use a locally dense lattice for relative distance α in the ℓ_p norm to prove NP-hardness (via a randomized reduction) of γ-GapSVP$_p$ for any constant $\gamma > 1/\alpha$. This reduction is very similar to those from prior works, so for the remainder of this section we focus on summarizing our new construction of locally dense lattices.

Locally dense lattices from Reed-Solomon codes. We start with some basic definitions and facts used in our construction. Recall that the Construction A lattice obtained from a linear code $\mathcal{C} \subseteq \mathbb{F}_q^n$ for some prime q is defined as $\mathcal{L} := \mathcal{C} + q\mathbb{Z}^n$, i.e., an integer vector $\boldsymbol{z} \in \mathbb{Z}^n$ is in the lattice if and only if $\boldsymbol{z} \bmod q$ is a code word. In fact, it will often be convenient to work with an equivalent "dual view" of Construction A lattices. Namely, if $H \in \mathbb{F}_q^{k \times n}$ is a parity-check matrix of a linear code $\mathcal{C} := \ker(H) \subseteq \mathbb{F}_q^n$ for prime q, then the *parity-check lattice* $\mathcal{L}^\perp(H)$ obtained from H is defined as

$$\mathcal{L}^\perp(H) := \{\boldsymbol{z} \in \mathbb{Z}^n : H\boldsymbol{z} = \boldsymbol{0} \in \mathbb{F}_q^k\} = \ker(H) + q\mathbb{Z}^n = \mathcal{C} + q\mathbb{Z}^n \ . \tag{1}$$

Such lattices have determinant $\det(\mathcal{L}^\perp(H)) = |\mathbb{Z}^n/\mathcal{L}^\perp(H)| \leq q^k$, with equality exactly when H has full row rank (see Lemma 4).

We next define the family of parity-check matrices $H = H_q(k, S)$ that we use to construct our family of locally dense lattices. Such a matrix is parameterized by a prime q, a positive integer k, and a set $S \subseteq \mathbb{F}_q$. Letting $s_0, \ldots, s_{n-1}$ be the elements of S in some arbitrary order, we define

$$H = H_q(k, S) := \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ s_0 & s_1 & s_2 & \cdots & s_{n-1} \\ s_0^2 & s_1^2 & s_2^2 & \cdots & s_{n-1}^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ s_0^{k-1} & s_1^{k-1} & s_2^{k-1} & \cdots & s_{n-1}^{k-1} \end{pmatrix} \in \mathbb{F}_q^{k \times n} \ . \tag{2}$$

That is, $H_q(k, S)$ is the transposed Vandermonde matrix whose (i, s)th entry is s^i, where for convenience we index the rows and columns of $H_q(k, S)$ by $i \in \{0, \ldots, k-1\}$ and $s \in S$, respectively, and define $0^0 := 1$.

The matrix $H = H_q(k, S)$ defined in Equation (2) is a *generator matrix* of the dimension-k Reed-Solomon code

$$\mathrm{RS}_q[k, S] := \{(p(s))_{s \in S} : p \in \mathbb{F}_q[x], \deg(p) < k\} \tag{3}$$

over $\mathbb{F}_q$ with evaluation set S, and hence is a parity-check matrix of its dual code, which is a so-called *generalized* Reed-Solomon (GRS) code (see [22, Theorem 5.1.6]). Moreover, in the special case where $S = \mathbb{F}_q$, it turns out that $H_q(k, S)$ is a parity-check matrix for the (ordinary) Reed-Solomon code $\mathrm{RS}_q[q-k, \mathbb{F}_q]$ of dimension $q-k$ with evaluation set $S = \mathbb{F}_q$. So, $\mathcal{L}^\perp(H_q(k, \mathbb{F}_q)) = \mathrm{RS}_q[q-k, \mathbb{F}_q] + q\mathbb{Z}^q$ is the Construction A lattice corresponding to the Reed-Solomon code $\mathrm{RS}_q[q-k, \mathbb{F}_q]$. For simplicity, in this overview we restrict to these "Construction A Reed-Solomon" lattices by taking $S = \mathbb{F}_q$, but note that our results generalize to any sufficiently large $S \subseteq \mathbb{F}_q$.

It is easy to see that for $k < q$, the GRS code having parity-check matrix H has minimum distance (in the Hamming metric) $k+1$: any k columns of H are linearly independent, because they form a transposed Vandermonde matrix, while any $k+1$ obviously are not. Therefore, the corresponding Construction A lattice $\mathcal{L} := \ker(H) + q\mathbb{Z}^q$ has minimum distance $\lambda_1^{(1)}(\mathcal{L}) \geq k+1$ in the ℓ_1 norm. The key to our local density construction and its $\alpha \approx 1/2^{1/p}$

relative distance is that the ℓ_1 minimum distance is in fact almost *twice* this large (at least): in Theorem 14 we show that $\lambda_1^{(1)}(\mathcal{L}) \geq 2k$ when $k \leq q/2$. The proof is short and elementary, proceeding via Newton's identities. Essentially the same result and proof originally appeared in work by Roth and Siegel [37], and closely related analysis also appeared in work on Craig lattices [14] (see Section 1.3).

Obtaining a dense coset. Because the determinant of $\mathcal{L}$ (i.e., the number of its integer cosets) is q^k, the pigeonhole principle immediately implies that there exists an integer coset of $\mathcal{L}$ containing at least $\binom{q}{h}/q^k$ *binary* vectors in $\{0,1\}^q$ with Hamming weight h, which have ℓ_1 norm h. By setting parameters appropriately, this yields a coset with subexponentially many vectors of ℓ_1 norm at most $\alpha \cdot \lambda_1^{(1)}(\mathcal{L})$, for any constant $\alpha > 1/2$.

More specifically, set $h := \alpha \cdot (2k) \leq \alpha \cdot \lambda_1^{(1)}(\mathcal{L})$ and $q \approx k^{1/\varepsilon}$ for some positive constant $\varepsilon < 1 - 1/(2\alpha)$. (For simplicity, assume that h is an integer.) Then there must exist an integer coset of $\mathcal{L}$ containing at least

$$\frac{\binom{q}{h}}{q^k} \geq \left(\frac{q}{h}\right)^h \cdot q^{-k} = \frac{q^{(2\alpha-1)k}}{(2\alpha k)^{2\alpha k}} \approx \frac{q^{(2\alpha-1)k}}{q^{2\varepsilon\alpha k}} = q^{(2(1-\varepsilon)\alpha-1)k} = q^{\Omega(k)} = q^{\Omega(q^\varepsilon)} \tag{4}$$

weight-h binary vectors, which is subexponentially large in q.

The above shows the *existence* of a suitable coset, but following previous works, it is straightforward to show that a *randomly sampled* coset from a suitable distribution is likely to have enough short vectors (see Lemma 16). Indeed, the difference between showing that such a coset exists, versus sampling one efficiently, versus deterministically computing one efficiently, is the main technical difference between getting a non-uniform, versus randomized, versus deterministic hardness reduction (respectively) for GapSVP_p using these techniques.

The above argument generalizes to arbitrary ℓ_p norms for finite p, albeit for larger relative distances $\alpha > 1/2^{1/p}$. Because $\mathcal{L}$ is integral, $\lambda_1^{(1)}(\mathcal{L}) \geq 2k$ implies that $\lambda_1^{(p)}(\mathcal{L}) \geq (2k)^{1/p}$ for any finite $p \geq 1$. Moreover, reparameterizing the calculation in Equation (4) by choosing $\alpha > 1/2^{1/p}$ and setting $h := \alpha^p \cdot (2k)$ shows that some coset of $\mathcal{L}$ contains subexponentially many binary vectors of Hamming weight h, and hence of ℓ_p norm $h^{1/p} = \alpha \cdot (2k)^{1/p} \leq \alpha \cdot \lambda_1^{(p)}(\mathcal{L})$. Therefore, this construction yields locally dense lattices in the ℓ_p norm for any constant relative distance $\alpha > 1/2^{1/p}$, which by our main reduction implies Theorem 1, i.e., randomized NP-hardness of γ-GapSVP_p for any constant $\gamma < 2^{1/p}$.

1.3 Additional Related Work

First, we note that after this work was first published [5] used the properties of the gadget lattices $\mathcal{L} = \mathcal{L}^\perp(H_q(k,S))$ we construct to show improved results and answer an open question about the *parameterized* complexity of GapSVP. Somewhat more specifically, [5] gave a parameterized analog of Theorem 1 by showing W[1]-hardness (under randomized reductions) of γ-GapSVP_p for any $p \geq 1$ and any γ satisfying $1 \leq \gamma < 2^{1/p}$. This in particular answered a question from [17, 9], which asked whether γ-GapSVP was W[1]-hard in the ℓ_1 norm. Prior to [5] (which crucially relied on this work), such hardness was not known even in the exact case of $\gamma = 1$.

The key lower bound of $\lambda_1^{(1)}(\mathcal{L}) \geq 2k$ for $\mathcal{L} = \mathcal{L}^\perp(H_q(k,S))$ follows immediately from works by Karabed, Roth, and Siegel [25, 37], which adapted an argument by Immink and Beenker [24]. In fact, [25, 37] showed their lower bounds for the *Lee* minimum distance of a family of BCH codes, including ones that are Reed-Solomon codes with parity check matrices of the form $H_q(k,S)$. However, their results immediately apply to the ℓ_1 minimum

distance of $\mathcal{L} = \mathcal{L}^{\perp}(H_q(k, S))$ as well, because Lee distance is essentially "ℓ_1 distance with wrap-around."[3] Even earlier, Berlekamp [8, Chapter 9] gave an argument using Newton's identities to prove a similar lower bound on the Lee minimum distance of negacyclic codes, which are codes whose parity check matrices are of the form in Equation (2) but with its even-power rows deleted (i.e., with only its odd-power rows). Additionally, our Construction A Reed-Solomon lattices $\mathcal{L}$ are closely related to a family of algebraic lattices studied by Craig [14]; see also [13, Chapter 8, Section 6].[4] Indeed, [13, Chapter 8, Section 6, Theorem 7] again gives a very similar argument for lower bounding the minimum distance of Craig lattices using Newton's identities.Our proof of Theorem 14 is inspired by and similar to all of these "minimum distance lower bounds via Newton's identities" arguments, and in particular is very similar to the ones in [37] and [13, Chapter 8, Section 6, Theorem 7].

We omit further discussion of related work due to space constraints and encourage the reader to view the full version of this work [6].

1.4 Open Questions

The obvious question left open by our work is whether our reduction can be derandomized, using the same family of lattices. Addressing this is the main focus of Section 5 in the full version of this paper [6]. The full version also discusses several other open questions. We omit this material due to space constraints, but strongly encourage the reader to view [6].

2 Preliminaries

Throughout this work we adopt the convention that $0^0 := 1$ in any ring. For a positive integer k, define $[k] := \{0, 1, \ldots, k-1\}$.

In general, every vector or matrix is indexed by some specified set S. For example, $\boldsymbol{x} \in \mathbb{Z}^S$ is an integer vector indexed by S, having an entry $x_s \in \mathbb{Z}$ for each $s \in S$ (and no other entries). When the index set is $[n]$ for some non-negative integer n, we usually omit the brackets in the exponent and just write, e.g., $\mathbb{Z}^n$. We emphasize that in this case the indices start from zero. An object indexed by a finite set S of size $n = |S|$ can be reindexed by $[n]$, simply by enumerating $S = \{s_0, \ldots, s_{n-1}\}$ under some arbitrary order, and identifying index s_i with index i.

For a finite set S and a positive integer $h \le |S|$, let $B_{S,h} := \{\boldsymbol{v} \in \{0,1\}^S : \|\boldsymbol{v}\|_1 = h\}$ be the set of binary vectors indexed by S of Hamming weight h. As above, when $S = [n]$ we often write $B_{n,h}$. Finally, let $\mathcal{B}_p^n(r) := \{\boldsymbol{x} : \|\boldsymbol{x}\|_p \le r\} \subset \mathbb{R}^n$ denote the real n-dimensional ℓ_p ball of radius r centered at the origin.

2.1 Basic Lattice Definitions

Given a lattice $\mathcal{L} = \mathcal{L}(B)$ with basis $B \in \mathbb{R}^{m \times n}$, we define the *rank* of $\mathcal{L}$ to be n and the (ambient) *dimension* of $\mathcal{L}$ to be m. We denote the *minimum distance* of $\mathcal{L}$ in the ℓ_p norm, which is the length of a shortest non-zero vector in $\mathcal{L}$, by

[3] More precisely, the Lee distance of $\boldsymbol{x} \in \mathbb{F}_q^n$ is $\sum_{i=1}^n \min\{x_i, q - x_i\}$, where elements of the prime-order field $\mathbb{F}_q$ are identified in the natural way with the integers $\{0, 1, \ldots, q-1\}$. This is the natural analog of ℓ_1 distance on $\mathbb{F}_q$ (or $\mathbb{Z}_q$). Moreover, the ℓ_1 minimum distance of the Construction A lattice $\mathcal{C} + q\mathbb{Z}^n$ is equal to the minimum of q and the Lee minimum distance of $\mathcal{C}$.

[4] Specifically, [13] considers Craig lattices obtained from the coefficient vectors of polynomials in principal ideals of the form $(x-1)^m R$ in rings of the form $R = \mathbb{Z}[x]/(x^p - 1)$, for some prime p and integer $m \ge 1$. The original definition of [14] is slightly different, and uses the "canonical" (Minkowski) embedding of such ideals in the ring of integers $R = \mathbb{Z}[x]/(\Phi_p(x))$ of the pth cyclotomic number field.

$$\lambda_1^{(p)}(\mathcal{L}) := \min_{\boldsymbol{x} \in \mathcal{L} \setminus \{0\}} \|\boldsymbol{x}\|_p \ .$$

The central problem that we study in this work asks about the value of $\lambda_1^{(p)}(\mathcal{L})$ for a given input lattice $\mathcal{L}$.

▶ **Definition 3.** *For $p \geq 1$ and $\gamma = \gamma(n) \geq 1$, the decisional, γ-approximate Shortest Vector Problem in the ℓ_p norm (γ-GapSVP$_p$) is the promise problem defined as follows. The input consists of a basis $B \in \mathbb{Z}^{m \times n}$ of an integer lattice $\mathcal{L}$ and a distance threshold $s > 0$, and the goal is to determine whether the input is a YES instance or a NO instance, where these are defined as follows:*

- *YES instance: $\lambda_1^{(p)}(\mathcal{L}) \leq s$.*
- *NO instance: $\lambda_1^{(p)} > \gamma s$.*

We define the *determinant* of $\mathcal{L}$ to be $\det(\mathcal{L}) := \sqrt{\det(B^T B)}$, which is equal to $|\det(B)|$ when $m = n$ (i.e., when $\mathcal{L}$ is full-rank). We note that determinant is well defined because, although lattice bases are not unique, they are equivalent up to multiplication on the right by unimodular matrices.

The density of a rank-n lattice $\mathcal{L}$ is captured by its so-called *root Hermite factor* $\lambda_1(\mathcal{L})/\det(\mathcal{L})^{1/n}$.[5] The density of a lattice corresponds to its quality in various applications, including as the set of centers of a sphere packing and as an error-correcting code. Minkowski's bound asserts that the root Hermite factor of such a rank-n lattice is at most $\sqrt{n}$, which is convenient to write in expanded form as

$$\lambda_1(\mathcal{L}) \leq \sqrt{n} \cdot \det(\mathcal{L})^{1/n} \ . \tag{5}$$

2.2 Parity-Check Matrices and Lattices

For a prime q and a matrix $H \in \mathbb{F}_q^{k \times n}$, we define the *parity-check lattice* $\mathcal{L}^\perp(H)$ obtained from H as

$$\mathcal{L}^\perp(H) := \{\boldsymbol{z} \in \mathbb{Z}^n : H\boldsymbol{z} = \boldsymbol{0}\} = \ker(H) + q\mathbb{Z}^n \ . \tag{6}$$

Note that $\mathcal{L}^\perp(H)$ is simply the "Construction A" lattice [13, Chapter 5, Section 2] of the linear error-correcting code $\mathcal{C}$ having H as a parity-check matrix, i.e., $\mathcal{C} = \{\boldsymbol{c} \in \mathbb{F}_q^n : H\boldsymbol{c} = \boldsymbol{0}\}$. More generally, for any "syndrome" $\boldsymbol{u} \in \mathbb{F}_q^k$ we define

$$\mathcal{L}_{\boldsymbol{u}}^\perp(H) := \{\boldsymbol{x} \in \mathbb{Z}^n : H\boldsymbol{x} = \boldsymbol{u}\} \ .$$

If there exists some $\boldsymbol{x} \in \mathbb{Z}^n$ such that $H\boldsymbol{x} = \boldsymbol{u}$, then it follows immediately that $\mathcal{L}_{\boldsymbol{u}}^\perp(H)$ is simply the lattice coset $\boldsymbol{x} + \mathcal{L}^\perp(H)$. So, we can identify cosets of $\mathcal{L}^\perp(H)$ by their corresponding syndromes. We recall some standard properties of parity-check lattices, and give a proof for self-containment.

▶ **Lemma 4.** *Let q be a prime, let k and n be positive integers, and let $H \in \mathbb{F}_q^{k \times n}$ be a parity-check matrix. Then the parity-check lattice $\mathcal{L} = \mathcal{L}^\perp(H)$ has rank n and determinant $\det(\mathcal{L}) \leq q^k$, with equality if and only if the rows of H are linearly independent.*

[5] This ratio is the square root of the Hermite factor $\gamma(\mathcal{L}) := (\lambda_1(\mathcal{L})/\det(\mathcal{L})^{1/n})^2$, which is defined in this way for historical reasons.

Proof. The first claim follows simply by noting that $q\mathbb{Z}^n \subseteq \mathcal{L}^\perp(H) \subseteq \mathbb{Z}^n$. For the determinant, observe that the map $\boldsymbol{x} \mapsto H\boldsymbol{x}$ is an additive-group homomorphism from $\mathbb{Z}^n$ to $\mathbb{F}_q^k$, and that $\mathcal{L}^\perp(H)$ is its kernel by definition. So, by the first isomorphism theorem, the map induces an isomorphism from the quotient group $\mathbb{Z}^n/\mathcal{L}^\perp(H)$ to the image $\mathrm{Im}(H) = \{H\boldsymbol{x} : \boldsymbol{x} \in \mathbb{Z}^n\} \subseteq \mathbb{F}_q^k$, where the subset relation is an equality if and only if the rows of H are linearly independent. The claim then follows from the fact that $\det(\mathcal{L}^\perp(H)) = \left|\mathbb{Z}^n/\mathcal{L}^\perp(H)\right| = |\mathrm{Im}(H)|$. ◀

We next formally define the family of parity-check lattices that are at the heart of our construction of locally dense lattices.

▶ **Definition 5.** *For a prime q, positive integer k, and set $S \subseteq \mathbb{F}_q$, define $H_q(k,S) \in \mathbb{F}_q^{k\times S}$ to be the matrix H whose rows and columns are respectively indexed by $[k] = \{0,1,\ldots,k-1\}$ and S, and whose (i,s)th entry is*

$$H_{i,s} := s^i \in \mathbb{F}_q \ .$$

(Recall that $0^0 := 1$.) Equivalently, if we enumerate $S = \{s_0,\ldots,s_{n-1}\}$ in some arbitrary order, we have

$$H = H_q(k,S) := \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ s_0 & s_1 & s_2 & \cdots & s_{n-1} \\ s_0^2 & s_1^2 & s_2^2 & \cdots & s_{n-1}^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ s_0^{k-1} & s_1^{k-1} & s_2^{k-1} & \cdots & s_{n-1}^{k-1} \end{pmatrix} \in \mathbb{F}_q^{k\times n} \ . \tag{7}$$

Notice that H is a transposed Vandermonde matrix. In particular, if $k \le n$ then its rows are linearly independent, and so $\det(\mathcal{L}^\perp(H)) = q^k$ by Lemma 4.

We recall from the introduction that $H = H_q(k,S)$ is a generator matrix (of row vectors) of the dimension-k Reed-Solomon code over $\mathbb{F}_q$ with evaluation set S, and hence H is a parity-check matrix of its dimension-$(n-k)$ dual code. So, $\mathcal{L}^\perp(H)$ is the Construction A lattice of this dual code. These dual codes are in fact *generalized Reed-Solomon codes*, a family of codes that include Reed-Solomon codes as a special case and that are closed under taking duals (see [22, Theorem 5.1.6]). Moreover, in the special case where $S = \mathbb{F}_q$, the matrix $H = H_q(k,\mathbb{F}_q)$ is in fact a parity-check matrix of an (ordinary) Reed-Solomon code. For our hardness proof it suffices to use this special case; i.e., we show NP-hardness (under a randomized reduction) of GapSVP by using Construction A lattices of (ordinary) Reed-Solomon codes as gadgets. See Appendix A and the section on derandomization in the full version of this paper [6] for other connections between these lattices and Reed-Solomon codes.

2.3 Symmetric Polynomials

A *symmetric polynomial* $P(x_1,x_2,\ldots,x_m)$ is a polynomial that is invariant under any permutation of its variables, i.e., $P(x_1,\ldots,x_m) = P(x_{\pi(1)},\ldots,x_{\pi(m)})$ as formal polynomials for all permutations π of $\{1,2,\ldots,m\}$. Because the order of the variables is immaterial, we usually just write a symmetric polynomial as $P(X)$, where $X = \{x_1,\ldots,x_m\}$ is the set of variables, and we write $P(T)$ for its evaluation on a multiset T of values.

We next recall two important symmetric polynomials and the relationship between them. For a non-negative integer i, the ith *power sum* of a set X of variables is defined as

$$p_i(X) := \sum_{x\in X} x^i \ . \tag{8}$$

(Recall that $0^0 := 1$.) For $1 \leq i \leq |X|$, the ith *elementary symmetric polynomial* of X is defined as

$$e_i(X) := \sum_{\substack{Z \subseteq X, \\ |Z|=i}} \prod_{z \in Z} z \ . \tag{9}$$

That is, $e_i(X)$ is the multilinear polynomial whose monomials consist of all products of i distinct variables from X. We extend this definition to $i = 0$ by setting $e_0(X) := 1$ and to integers $i > |X|$ by setting $e_i(X) := 0$.

Power sums and elementary symmetric polynomials are related by *Newton's identities* (see, e.g., [30]), which assert that for $1 \leq i \leq |X|$,

$$i \cdot e_i(X) = \sum_{j=1}^{i} (-1)^{j-1} \cdot e_{i-j}(X) \cdot p_j(X) \ . \tag{10}$$

The following standard claim uses Newton's identities to show that if the first k power sums of two *multisets* of field elements coincide, then so do the first k elementary symmetric polynomials of those multisets.

▶ **Lemma 6.** *Let T, U be multisets over a prime field $\mathbb{F}_q$, let $k \leq q$ be a positive integer, and suppose that $p_i(T) = p_i(U)$ for all $i \in [k]$. Then $e_i(T) = e_i(U)$ for all $i \in [k]$.*

Proof. The proof is by (strong) induction. For the base case where $i = 0$, we have by definition that $e_0(T) = e_0(U) = 1$. For the inductive case where $1 \leq i < k$, because $i \neq 0 \in \mathbb{F}_q$ we have that

$$e_i(T) = i^{-1} \cdot \sum_{j=1}^{i} (-1)^{j-1} \cdot e_{i-j}(T) \cdot p_j(T) = i^{-1} \cdot \sum_{j=1}^{i} (-1)^{j-1} \cdot e_{i-j}(U) \cdot p_j(U) = e_i(U) \ ,$$

where the first and third equalities follow from Newton's identities (Equation (10)), and the second equality follows from the claim's hypothesis and the inductive hypothesis (note that the sums involve elementary symmetric polynomials e_{i-j} only for $i - j < i$). ◀

We define the *root polynomial* $f_T(x) \in \mathbb{F}[x]$ of a multiset T over a field $\mathbb{F}$ to be

$$f_T(x) := \prod_{t \in T} (x - t) = \sum_{i=0}^{|T|} (-1)^i \cdot e_i(T) \cdot x^{|T|-i} \ . \tag{11}$$

We then get the following result, which uses Lemma 6 to show that if sufficiently many of the initial power sums of two multisets are equal, then the multisets themselves are equal.

▶ **Proposition 7.** *Let q be a prime, let $k \leq q/2$ be a positive integer, let T, U be multisets over $\mathbb{F} = \mathbb{F}_q$ of total cardinality $|T| + |U| < 2k$, and suppose that $p_i(T) = p_i(U)$ for all $i \in [k]$. Then $T = U$.*

Proof. Because

$$|T| \equiv p_0(T) = p_0(U) \equiv |U| \pmod{q}$$

and $0 \leq |T| + |U| < 2k \leq q$, it follows that $|T| = |U|$ and hence both $f_T(x), f_U(x)$ have degree $|T| < k$.

Next, by the hypotheses and Lemma 6, we have that $e_i(T) = e_i(U)$ for all $i \leq |T|$. Therefore, by the equality in Equation (11), $f_T(x)$ and $f_U(x)$ are identical as formal polynomials in $\mathbb{F}[x]$. Finally, because the polynomial ring $\mathbb{F}[x]$ is a unique factorization domain, and because $f_T(x)$ and $f_U(x)$ split over $\mathbb{F}$ by construction, it follows that $T = U$. ◀

2.4 Locally Dense Lattices

Roughly speaking, *locally dense lattices* are lattices that have one or more cosets with many relatively short vectors. Somewhat more precisely, a locally dense lattice consists of an integer lattice $\mathcal{L} \subset \mathbb{Z}^n$ and a shift $\boldsymbol{x} \in \mathbb{Z}^n$ such that for some $\alpha \in (0,1)$, the number of points in the coset $\boldsymbol{x} + \mathcal{L}$ of norm at most $\alpha \cdot \lambda_1(\mathcal{L})$ is large (for our purposes, greater than 2^{n^ε} for some constant $\varepsilon > 0$). Therefore, locally dense lattices are not efficiently list decodable, even combinatorially, to within distance $\alpha \cdot \lambda_1(\mathcal{L})$ in the worst case (in particular, around center $-\boldsymbol{x}$). For the purposes of proving hardness, we also require a linear map T that projects the short vectors in $\boldsymbol{x} + \mathcal{L}$ onto a lower-dimensional hypercube $\{0,1\}^r$.

▶ **Definition 8.** *For $p \in [1,\infty)$, real $\alpha > 0$, and positive integers r and R, a (p, α, r, R)-*locally dense lattice *consists of an integer lattice of rank R (and some dimension n) represented by a basis matrix $A \in \mathbb{Z}^{n \times R}$, a positive integer ℓ, a shift $\boldsymbol{x} \in \mathbb{Z}^n$, and a matrix $T \in \mathbb{Z}^{r \times n}$, where*

1. $\lambda_1^{(p)}(\mathcal{L}(A)) \geq \ell^{1/p}$ *and*
2. $\{0,1\}^r \subseteq T(V) := \{T\boldsymbol{v} : \boldsymbol{v} \in V\}$, *where $V := (\boldsymbol{x} + \mathcal{L}(A)) \cap \mathcal{B}_p^n(\alpha \cdot \ell^{1/p})$ is the set of all vectors of ℓ_p norm at most $\alpha \cdot \ell^{1/p}$ in the lattice coset $\boldsymbol{x} + \mathcal{L}(A)$.*

A useful tool for satisfying Item 2 in the above definition is the following probabilistic version of Sauer's Lemma due to Micciancio [31]. It roughly says that for $n \gg r$, for any large enough collection of vectors $W \subseteq B_{n,h}$ (the weight-h slice of $\{0,1\}^n$), and for a random matrix $T \in \{0,1\}^{r \times n}$ whose coordinates are sampled independently with a suitable bias, $\{0,1\}^r \subseteq T(W)$ with good probability. We emphasize that all the arithmetic in this theorem is done over the integers (not over $\mathbb{F}_2$).

▶ **Theorem 9** ([31, Theorem 4])**.** *Let r, n, h be positive integers, let $W \subseteq B_{n,h}$, and let $\varepsilon > 0$. If $|W| \geq h! \cdot n^{24r\sqrt{h}/\varepsilon}$ and $T \in \{0,1\}^{r \times n}$ is sampled by setting each entry to 1 independently with probability $1/(4hr)$, then $\{0,1\}^r \subseteq T(W)$ with probability at least $1 - \varepsilon$.*

2.5 Hardness of GapSVP via Locally Dense Lattices

We next recall a variant of (the decision version of) the Closest Vector Problem (CVP), which will be the hard problem that we reduce to GapSVP_p. In this variant, called GapCVP'_p, the target vector is either within a specified distance of a lattice vector given by a *binary* combination of basis vectors, or *all non-zero integer multiples* of the target vector are more than a γ multiple of this distance from the lattice (where distance is measured in the ℓ_p norm).

▶ **Definition 10.** *For $p \in [1,\infty]$, an instance of the γ-GapCVP'_p problem consists of a rank-r lattice basis $B \in \mathbb{Z}^{d \times r}$, a target vector $\boldsymbol{t} \in \mathbb{Z}^d$, and a distance threshold $s > 0$. The goal is to determine whether an input is a YES instance or a NO instance, where these are defined as follows:*

- *YES instance: there exists a* binary *$\boldsymbol{c} \in \{0,1\}^r$ such that $\|B\boldsymbol{c} - \boldsymbol{t}\|_p \leq s$.*
- *NO instance: $\mathrm{dist}_p(w\boldsymbol{t}, \mathcal{L}(B)) > \gamma s$ for all $w \in \mathbb{Z} \setminus \{0\}$.*

The following hardness theorem follows via a reduction from Exact Set Cover to GapCVP'_p.

▶ **Theorem 11** ([4])**.** *For every $p \in [1,\infty)$ and every constant $\gamma \geq 1$, γ-GapCVP'_p is* NP*-hard.*

The following theorem gives a polynomial-time reduction from γ-GapCVP'_p to γ'-GapSVP_p for some approximation factors $\gamma > \gamma' \geq 1$, which uses a locally dense lattice as advice. In general, this advice makes the reduction non-uniform, but when the advice is efficiently computable by a (randomized) algorithm, as it is in this and prior works, the procedure is

an efficient (randomized) reduction. The reduction below is very similar to the one in [32, Theorem 5.1], but written so as to allow for using an arbitrary locally dense lattice as advice. Due to this similarity, and for concision we defer its proof to the full version of our paper [6].

▶ **Theorem 12.** *Let $p \geq 1$, r and n be positive integers, $\alpha > 0$ be a constant, and γ, γ' be constants satisfying*

$$1/\alpha > \gamma' \geq 1 \text{ and } \gamma \geq \gamma' \cdot \left(\frac{1}{1-(\alpha\gamma')^p}\right)^{1/p}.$$

There is a deterministic polynomial-time algorithm that, given a γ-GapCVP$'_p$ instance $(B, \boldsymbol{t}, s)$ of rank r and a (p, α, r, R)-locally dense lattice $(A, \ell, \boldsymbol{x}, T)$ as input, outputs a γ'-GapSVP$_p$ instance (B', s') of rank $R+1$ which is a YES (respectively, NO) instance if $(B, \boldsymbol{t}, s)$ is a YES (resp., NO) instance.

From these two theorems we get the following hardness results for GapSVP.

▶ **Corollary 13.** *Let $p \geq 1$, let r be a positive integer, let $\alpha > 0$ be a constant, and suppose that there is an algorithm A that computes a $(p, \alpha, r, \mathrm{poly}(r))$-locally dense lattice in $\mathrm{poly}(r)$ time. Let γ be a constant satisfying $1 \leq \gamma < 1/\alpha$. Then:*

1. *If A is deterministic, then γ-GapSVP$_p$ is NP-hard (and exact GapSVP$_p$ is NP-complete).*
2. *If A is randomized and its output satisfies Item 1 of Definition 8 with probability 1 and Item 2 of Definition 8 with probability at least $2/3$, then γ-GapSVP$_p$ is not in RP unless NP $\subseteq$ RP.*[6]
3. *If A is randomized, and its output satisfies Items 1 and 2 of Definition 8 with probability at least $2/3$, then there is no* randomized *polynomial-time algorithm for γ-GapSVP$_p$ unless NP $\subseteq$ BPP.*

Proof. Items 1 and 3 follow immediately by combining Theorems 11 and 12. Inspection of the proof of Theorem 12 shows that for NO instances to be mapped to NO instances, only Item 1 of Definition 8 is needed, from which Item 2 of the claim follows. ◀

3 Local Density from Reed-Solomon Codes

In this section we show how to obtain locally dense lattices from Reed-Solomon codes with appropriate parameters. More specifically, we show to satisfy Definition 8 using a lattice $\mathcal{L} := \mathcal{L}^{\perp}(H)$ corresponding to a parity-check matrix $H = H_q(k, S)$ from Definition 5. (Recall that H is the parity-check matrix of a Reed-Solomon code when $S = \mathbb{F}_q$, and of a generalized Reed-Solomon code for any $S \subseteq \mathbb{F}_q$.)

The overall structure of the argument is as follows. First, in Section 3.1 we give a lower bound of $\lambda_1^{(p)}(\mathcal{L}) \geq (2k)^{1/p}$, which corresponds to Item 1 of Definition 8, by using the connection between power sums and symmetric polynomials (see Section 2.3). Then, in Section 3.2 we use the upper bound $\det(\mathcal{L}) \leq q^k$ from Lemma 4 and the pigeonhole principle to show that there exists a lattice coset with many short (binary) vectors, and in fact a suitably sampled random coset has this property with good probability. Finally, in Section 3.3 we set parameters and use Theorem 9 to satisfy Item 2 of Definition 8 with good probability.

[6] The condition "γ-GapSVP$_p$ is not in RP" is a slight abuse of notation, since γ-GapSVP$_p$ for $\gamma > 1$ is a promise problem rather than a language. However, the definition of RP can naturally be extended to encompass promise problems, which is the intended meaning here.

3.1 Minimum Distance

The following theorem says that for any $k \le |S|/2$, the ℓ_1 minimum distance of $\mathcal{L} = \mathcal{L}^\perp(H)$ for $H = H_q(k, S)$ is at least $2k$. Essentially the same result and proof appeared in works of Karabed, Roth, and Siegel [25, 37], and a very similar theorem and proof for lower bounding the minimum distance of Craig lattices appears in [14] and [13, Chapter 8, Theorem 7]. We reprove the result here in a slightly different form for completeness.

Note that a weaker bound of $\lambda_1^{(1)}(\mathcal{L}) \ge k+1$ (for any $k < q$) follows trivially from the minimum Hamming distance $k+1$ of the (generalized Reed-Solomon) code having parity-check matrix H. However, this bound is not strong enough for the rest of the local-density argument below, which requires $\lambda_1^{(1)}(\mathcal{L}) \ge (1+\Omega(1))k$.

▶ **Theorem 14.** *Let q be a prime, let $S \subseteq \mathbb{F}_q$, let $k \le |S|/2$ be a positive integer, and let $H := H_q(k, S) \in \mathbb{F}_q^{k \times S}$ be the matrix from Definition 5. Then $\mathcal{L} = \mathcal{L}^\perp(H)$ has ℓ_1 minimum distance $\lambda_1^{(1)}(\mathcal{L}) \ge 2k$.*
As a consequence, for any $p \in [1, \infty)$ the ℓ_p minimum distance satisfies $\lambda_1^{(p)}(\mathcal{L}) \ge (2k)^{1/p}$.

We point out that the $2^{1/p}$ factor in Theorem 14 propagates to the relative-distance bound for local density in Theorem 17 below, and then to the GapSVP approximation factor in our main hardness theorem, Theorem 1.

Proof. The consequence follows immediately from the fact that $\mathcal{L} \subseteq \mathbb{Z}^S$ and $\|\boldsymbol{v}\|_p \ge \|\boldsymbol{v}\|_1^{1/p}$ for all $\boldsymbol{v} \in \mathbb{Z}^S$.

Now consider some arbitrary $\boldsymbol{x} \in \mathcal{L} \subseteq \mathbb{Z}^S$ for which $\|\boldsymbol{x}\|_1 < 2k$; we will show that $\boldsymbol{x} = \boldsymbol{0}$. Let $\boldsymbol{x}^+, \boldsymbol{x}^- \in \mathbb{Z}^S$ be the unique non-negative integer vectors satisfying $\boldsymbol{x} = \boldsymbol{x}^+ - \boldsymbol{x}^-$. Define multisets T^+ and T^- over S that respectively depend on $\boldsymbol{x}^+$ and $\boldsymbol{x}^-$ as follows. For each $s \in S$ with $x_s^+ > 0$ (respectively, $x_s^- > 0$), let T^+ (respectively, T^-) contain s with multiplicity x_s^+ (respectively, x_s^-).[7]

Note that $|T^+| + |T^-| = \|\boldsymbol{x}\|_1 < 2k$. Because $H\boldsymbol{x} = H(\boldsymbol{x}^+ - \boldsymbol{x}^-) = \boldsymbol{0} \in \mathbb{F}_q^k$, by definition of H we have that $p_i(T^+) = p_i(T^-)$ for all $i \in [k]$ (where recall that p_i denotes the ith power sum). Because $k \le |S|/2 \le q/2$, by Proposition 7 it follows that $T^+ = T^-$. Since $T^+ \cap T^- = \emptyset$ by construction, we must have $T^+ = T^- = \emptyset$, and hence $\boldsymbol{x} = \boldsymbol{0}$, as desired. ◀

The following lemma (which is well known in other forms) shows that the lower bound $\lambda_1^{(p)}(\mathcal{L}^\perp(H)) \ge (2k)^{1/p}$ from Theorem 14 is in fact an equality under mild conditions on the parameters, by giving an explicit lattice coset that has multiple short vectors. However, because it proves only that the number of such vectors is polynomial in the dimension, it is insufficient to establish local density.

▶ **Lemma 15.** *Let q be a prime, let k be a positive integer that divides $q-1$, and let $H := H_q(k, S) \in \mathbb{F}_q^{k \times S}$ where $\mathbb{F}_q^* \subseteq S \subseteq \mathbb{F}_q$. Then for $\boldsymbol{u} := (k, 0, \ldots, 0) \in \mathbb{F}_q^k$, the lattice coset $\mathcal{L}_{\boldsymbol{u}}^\perp(H) = \{\boldsymbol{x} \in \mathbb{Z}^S : H\boldsymbol{x} = \boldsymbol{u}\}$ contains $(q-1)/k$ binary vectors of Hamming weight k and pairwise disjoint support. As a consequence, when $k < q-1$, we have $\lambda_1^{(p)}(\mathcal{L}^\perp(H)) = (2k)^{1/p}$ for any $p \in [1, \infty)$.*

Proof. Let G be the order-k subgroup of the (cyclic, multiplicative) group $\mathbb{F}_q^*$, i.e., the subgroup of the kth roots of unity. Then the binary indicator vectors $\boldsymbol{x}_C \in \{0,1\}^S$ of each of the $(q-1)/k$ pairwise disjoint cosets $C = cG$ of G all belong to the coset $\mathcal{L}_{\boldsymbol{u}}^\perp(H)$. This

[7] For example, if $S = \{0,1,2,3,4\} = \mathbb{F}_q$ and $\boldsymbol{x} = (x_0, x_1, x_2, x_3, x_4)^t = (1, -2, 0, 1, 0)^t$, then $x^+ = (1,0,0,1,0)$, $x^- = (0,2,0,0,0)$, and accordingly $T^+ = \{0,3\}$, $T^- = \{1,1\}$.

is simply because for any such coset, the 0th power sum of its elements is k, and the ith power sum for $0 < i < k$ is zero; this can be seen by Newton's identities and the fact that the root polynomial of C is $f_C(x) = \prod_{c \in C}(x - c) = x^k - r_C$, where $r_C = c^k$ for every $c \in C$. Finally, when $k < q - 1$, there is more than one such vector $\boldsymbol{x}_C$, and the differences between distinct pairs of them are lattice vectors in $\{0, \pm 1\}^S$ of Hamming weight $2k$, and hence ℓ_p norm $(2k)^{1/p}$. ◀

3.2 Dense Cosets

Following an approach previously used in [31, 26, 32] (and implicitly in [3]), we first show via a pigeonhole argument that a dense lattice coset must exist, and then show how to sample such a coset efficiently (with good probability).

For a prime q, a positive integer k, and a set $S \subseteq \mathbb{F}_q$ of size n (with some arbitrary ordering of its elements), let $H = H_q(k, S) \in \mathbb{F}_q^{k \times n}$ be the parity-check matrix from Definition 5. By Lemma 4, the lattice $\mathcal{L} = \mathcal{L}^\perp(H) \subseteq \mathbb{Z}^n$ has $\det(\mathcal{L}) \leq q^k$ integer cosets. Recall that $B_{n,h}$ is the set of n-dimensional binary vectors of Hamming weight h, which has cardinality $|B_{n,h}| = \binom{n}{h}$. Therefore, by the pigeonhole principle, there must exist some integer coset $\boldsymbol{x} + \mathcal{L}$ with $|(\boldsymbol{x} + \mathcal{L}) \cap B_{n,h}| \geq \binom{n}{h}/q^k$ weight-h binary vectors. In particular, taking $n \approx q$, $h \approx \alpha^p \cdot (2k)$ for some constant $\alpha > 1/2^{1/p}$, and $k = q^\varepsilon$ for a suitable small constant $\varepsilon > 0$ implies the existence of a coset with roughly $q^{(2\alpha^p - 1)k} = q^{\Omega(q^\varepsilon)}$ such vectors. These vectors have ℓ_p norm $h^{1/p} \approx \alpha \cdot (2k)^{1/p}$, whereas by Theorem 14 the lattice minimum distance is at least $(2k)^{1/p}$, yielding a local-density relative distance of roughly α.

The following lemma extends the above existential result by showing that something very similar holds for a *uniformly random* shift $\boldsymbol{x} \in B_{n,h}$: for any $\delta > 0$, the coset $\boldsymbol{x} + \mathcal{L}$ contains at least $\delta \cdot \binom{n}{h}/q^k$ weight-h binary vectors with probability greater than $1 - \delta$. The proof given below closely follows the structure of the very similar one of [26, Lemma 4.3].

▶ **Lemma 16.** *For a prime q, positive integer k, and set $S \subseteq \mathbb{F}_q$ of size n, let $H = H_q(k, S) \in \mathbb{F}_q^{k \times n}$ be the parity-check matrix from Definition 5. There is an efficient randomized algorithm that, for any $\delta \geq 0$, and on input H and any $h \in [n]$, outputs a shift $\boldsymbol{x} \in B_{n,h}$ such that*

$$\Pr_{\boldsymbol{x}}\left[|(\boldsymbol{x} + \mathcal{L}) \cap B_{n,h}| \geq \delta \cdot \binom{n}{h}/q^k\right] > 1 - \delta \ .$$

Proof. The algorithm simply samples and outputs a uniformly random binary vector $\boldsymbol{x} \in B_{n,h}$. This is clearly efficient. To show correctness, we will use the syndromes of H. For each $\boldsymbol{u} \in \mathbb{F}_q^k$, define $K_{\boldsymbol{u}} := |\{\boldsymbol{z} \in B_{n,h} : H\boldsymbol{z} = \boldsymbol{u}\}|$, and define $\boldsymbol{s} := H\boldsymbol{x} \in \mathbb{F}_q^k$ to be the syndrome corresponding to $\boldsymbol{x}$. So, we need to prove that $K_{\boldsymbol{s}} \geq \delta \cdot \binom{n}{h}/q^k$ with probability greater than $1 - \delta$. Indeed, we have:

$$\begin{aligned}
\Pr_{\boldsymbol{x}}\left[|(\boldsymbol{x} + \mathcal{L}) \cap B_{n,h}| < \delta \cdot \binom{n}{h}/q^k\right] &= \Pr_{\boldsymbol{x}}\left[K_{\boldsymbol{s}} < \delta \cdot \binom{n}{h}/q^k\right] \\
&= \sum_{\boldsymbol{u} \in \mathbb{F}_q^k : K_{\boldsymbol{u}} < \delta \cdot \binom{n}{h}/q^k} \Pr_{\boldsymbol{x}}[H\boldsymbol{x} = \boldsymbol{u}] \\
&= \sum_{\boldsymbol{u} \in \mathbb{F}_q^k : K_{\boldsymbol{u}} < \delta \cdot \binom{n}{h}/q^k} \frac{K_{\boldsymbol{u}}}{\binom{n}{h}} \\
&< \sum_{\boldsymbol{u} \in \mathbb{F}_q^k : K_{\boldsymbol{u}} < \delta \cdot \binom{n}{h}/q^k} \frac{\delta}{q^k} \\
&\leq \delta \ ,
\end{aligned}$$

where the first inequality uses the fact that the sum is over syndromes $\boldsymbol{u}$ with $K_{\boldsymbol{u}} < \delta \cdot \binom{n}{h}/q^k$, and the second inequality uses the fact that there are at most q^k terms in the sum. ◀

3.3 The Main Argument

▶ **Theorem 17** (Locally dense lattices from Reed-Solomon codes). *For any $p \in [1, \infty)$ and constant $\alpha > 1/2^{1/p}$, there exists a randomized polynomial-time algorithm that, given any sufficiently large positive integer r in unary as input, outputs a $(p, \alpha, r, R = \mathrm{poly}(r))$-locally dense lattice (Definition 8) with probability at least $2/3$. Moreover, the algorithm's output satisfies Item 1 of Definition 8 with probability 1.*

Proof. The algorithm starts by setting its parameters as follows. It sets $\varepsilon := 2\alpha^p - 1 > 0$, and chooses:

- a $\mathrm{poly}(r)$-bounded integer $k \geq r^{1/(1/2-\delta)}$ for some arbitrary constant $\delta \in (0, 1/2)$, and
- a $\mathrm{poly}(r)$-bounded prime $q \geq k^{3(1+\varepsilon)/\varepsilon}$. (Such a prime q always exists by Bertrand's Postulate.)

The algorithm then computes the components of a $(p, \alpha, r, R = q)$-locally dense lattice $(A, \ell, \boldsymbol{x}, T)$ as follows. It lets:

- $A \in \mathbb{Z}^{q \times q}$ be a basis of $\mathcal{L} := \mathcal{L}^{\perp}(H)$, where $H = H(k, S) \in \mathbb{F}_q^{k \times q}$ for $S = \mathbb{F}_q$;[8]
- $\ell := 2k$;
- $\boldsymbol{x} \in B_{q,h}$ be a uniformly random q-dimensional binary vector of Hamming weight $h := \lfloor (1+\varepsilon)k \rfloor$;
- $T \in \{0,1\}^{r \times q}$ be chosen by independently setting each of its entries to be 1 with probability $1/(4hr)$, and to be 0 otherwise.

It then outputs $(A, \boldsymbol{x}, \ell, T)$.

We first analyze the algorithm's running time. A suitable prime q can be found in $\mathrm{poly}(r)$ time using, e.g., trial division (recall that r is given in unary). The basis A can be computed in deterministic polynomial time from the generating set of column vectors $(B \mid qI_q)$, where B is a basis of $\ker(H) \subseteq \mathbb{F}_q^q$ (lifted to the integers). It is clear that ℓ can be computed in deterministic polynomial time, and that $\boldsymbol{x}$ and T can be computed in randomized polynomial time. So, the algorithm runs in randomized polynomial time.

It remains to show correctness, i.e., that $(A, \boldsymbol{x}, \ell, T)$ satisfies the two conditions in Definition 8 with suitable probability over the random choices of $\boldsymbol{x}$ and T. First, Item 1 is always satisfied, because by Theorem 14 we have

$$\lambda_1(\mathcal{L}) \geq (2k)^{1/p} = \ell^{1/p} \ .$$

In the rest of the proof we consider Item 2 of Definition 8. Let $W := (\boldsymbol{x} + \mathcal{L}) \cap B_{q,h}$. Because

$$\|\boldsymbol{w}\|_p^p = h \leq (1+\varepsilon)k = \alpha^p \cdot \ell$$

for each $\boldsymbol{w} \in W$, we have $W \subseteq V := (\boldsymbol{x} + \mathcal{L}) \cap \mathcal{B}_p^q(\alpha \cdot \ell^{1/p})$.

By Lemma 16, $\Pr_{\boldsymbol{x}}[|W| \geq \binom{q}{h}/(10q^k)] > 1 - 1/10 = 9/10$. If this event holds, and

$$\frac{\binom{q}{h}}{10q^k} \geq h! \cdot q^{240r\sqrt{h}} \ , \tag{12}$$

[8] For appropriate parameters, our argument works more generally for any sufficiently large subset $S \subseteq \mathbb{F}_q$, with $R = |S|$; we use $S = \mathbb{F}_q$ for simplicity.

then by Theorem 9 we have $\{0,1\}^r \subseteq T(W) \subseteq T(V)$ with probability at least $1-1/10 = 9/10$ (over the choice of T). So, it suffices to show that the condition in Equation (12) holds for all sufficiently large k, and hence for all sufficiently large r. By taking a union bound over the $1/10$ failure probabilities from Lemma 16 and Theorem 9, we get that the algorithm's overall success probability is at least $1 - 2/10 > 2/3$ for all sufficiently large r, as needed.

Using the standard bound $\binom{q}{h} \geq (q/h)^h$ for binomial coefficients and that $h \geq (1+\varepsilon)k - 1$, we have that

$$\frac{\binom{q}{h}}{10q^k} \geq \frac{q^{h-k}}{10h^h} = \Omega\Big(\frac{q^{\varepsilon k - 1}}{h^h}\Big) \ . \tag{13}$$

Furthermore, by the choice of k relative to r and $h \leq (1+\varepsilon)k$, we have that

$$h! \cdot q^{240r\sqrt{h}} \leq h^h \cdot q^{240k^{1/2-\delta}\sqrt{(1+\varepsilon)k}} \leq h^h \cdot q^{o(k)} \ . \tag{14}$$

So, by combining Equations (13) and (14), in order to establish Equation (12) it suffices to show that $q^{(1-o(1))\varepsilon k} \geq h^{2h}$. By taking logs, this is equivalent to

$$(1 - o(1)) \cdot \varepsilon k \log q \geq 2h \log h \ . \tag{15}$$

Finally, using that $k^{3(1+\varepsilon)/\varepsilon} \leq q \leq \mathrm{poly}(k)$ and $h \leq (1+\varepsilon)k$, in order for Equation (15) to hold it suffices to have

$$(1 - o(1)) \cdot \varepsilon k \cdot \frac{3(1+\varepsilon)}{\varepsilon} \cdot \log k = (3 - o(1)) \cdot (1+\varepsilon) \cdot k \log k \geq 2(1+\varepsilon) \cdot k \log k + O(k) \ ,$$

which indeed holds for all sufficiently large k, as needed. ◀

We emphasize that Theorem 17 uses randomness only to sample $\boldsymbol{x}$ and T. As an immediate corollary, we obtain our main hardness result, Theorem 1 – which, to recall, asserts that for all constants $p \in [1,\infty)$ and $\gamma < 2^{1/p}$, there is no polynomial-time algorithm for γ-GapSVP$_p$ unless $\mathsf{NP} \subseteq \mathsf{RP}$.

Proof of Theorem 1. Combine Item 2 of Corollary 13 with Theorem 17. ◀

References

1 Divesh Aggarwal and Noah Stephens-Davidowitz. (Gap/S)ETH hardness of SVP. In *STOC*, 2018.

2 Dorit Aharonov and Oded Regev. Lattice problems in NP cap coNP. *J. ACM*, 52(5):749–765, 2005. Preliminary version in FOCS 2004.

3 Miklós Ajtai. The shortest vector problem in L_2 is NP-hard for randomized reductions (extended abstract). In *STOC*, pages 10–19, 1998.

4 Sanjeev Arora, László Babai, Jacques Stern, and Z. Sweedyk. The hardness of approximate optima in lattices, codes, and systems of linear equations. *J. Comput. Syst. Sci.*, 54(2):317–331, 1997. Preliminary version in FOCS 1993.

5 Huck Bennett, Mahdi Cheraghchi, Venkatesan Guruswami, and João Ribeiro. Parameterized inapproximability of the Minimum Distance Problem over all fields and the Shortest Vector Problem in all ℓ_p norms. In *STOC*, 2023.

6 Huck Bennett and Chris Peikert. Hardness of the (approximate) shortest vector problem: A simple proof via reed-solomon codes, 2023. `arXiv:2202.07736`.

7 Huck Bennett, Chris Peikert, and Yi Tang. Improved hardness of BDD and SVP under Gap-(S)ETH. In *ITCS*, 2022.

8 Elwyn Berlekamp. *Negacyclic Codes for the Lee Metric*, chapter 9, pages 207–217. World Scientific, 2015. Preliminary version in Symposium on Combinatorial Mathematics and its Applications, 1967. URL: `https://www.worldscientific.com/doi/abs/10.1142/9789814635905_0009`.

9 Arnab Bhattacharyya, Édouard Bonnet, László Egri, Suprovat Ghoshal, Karthik C.S., Bingkai Lin, Pasin Manurangsi, and Dániel Marx. Parameterized intractability of even set and shortest vector problem. *J. ACM*, 68(3), 2021. `doi:10.1145/3444942`.

10 Jin-yi Cai and Ajay Nerurkar. Approximating the SVP to within a factor $(1 + 1/\dim^{\epsilon})$ is NP-hard under randomized reductions. In *CCC*, 1998.

11 Qi Cheng and Daqing Wan. On the list and bounded distance decodibility of the Reed-Solomon codes (extended abstract). In *FOCS*, 2004.

12 Qi Cheng and Daqing Wan. A deterministic reduction for the gap minimum distance problem. *IEEE Trans. Inf. Theory*, 58(11):6935–6941, 2012. Preliminary version in STOC 2009.

13 John Conway and Neil J. A. Sloane. *Sphere packings, lattices, and groups*. Springer, 1999.

14 Maurice Craig. Automorphisms of prime cyclotomic lattices. Preprint.

15 Léo Ducas and Cécile Pierrot. Polynomial time bounded distance decoding near Minkowski's bound in discrete logarithm lattices. *Des. Codes Cryptogr.*, 87(8):1737–1748, 2019.

16 Léo Ducas and Wessel P. J. van Woerden. On the lattice isomorphism problem, quadratic forms, remarkable lattices, and cryptography. In *EUROCRYPT*, 2022.

17 Andreas Emil Feldmann, Karthik C. S., Euiwoong Lee, and Pasin Manurangsi. A survey on approximation in parameterized complexity: Hardness and algorithms. *Algorithms*, 13(6), 2020. `doi:10.3390/a13060146`.

18 Oded Goldreich and Shafi Goldwasser. On the limits of nonapproximability of lattice problems. *J. Comput. Syst. Sci.*, 60(3):540–563, 2000. Preliminary version in STOC 1998.

19 Elena Grigorescu and Chris Peikert. List-decoding Barnes-Wall lattices. *Comput. Complex.*, 26(2):365–392, 2017. Preliminary version in CCC 2012.

20 Venkatesan Guruswami and Atri Rudra. Limits to list decoding Reed-Solomon codes. *IEEE Trans. Inf. Theory*, 52(8):3642–3649, 2006. Preliminary version in STOC 2005.

21 Venkatesan Guruswami and Madhu Sudan. Improved decoding of Reed-Solomon and algebraic-geometry codes. *IEEE Trans. Inf. Theory*, 45(6):1757–1767, 1999. Preliminary version in FOCS 1998.

22 Jonathan I. Hall. Notes on coding theory. Available at `https://users.math.msu.edu/users/halljo/classes/CODENOTES/CODING-NOTES.HTML`.

23 Ishay Haviv and Oded Regev. Tensor-based hardness of the shortest vector problem to within almost polynomial factors. *Theory Comput.*, 8(1):513–531, 2012. Preliminary version in STOC 2007.

24 K. Immink and G. Beenker. Binary transmission codes with higher order spectral zeros at zero frequency (corresp.). *IEEE Transactions on Information Theory*, 33(3):452–454, 1987.

25 R. Karabed and P.H. Siegel. Matched spectral-null codes for partial-response channels. *IEEE Transactions on Information Theory*, 37(3):818–855, 1991.

26 Subhash Khot. Hardness of approximating the shortest vector problem in lattices. *J. ACM*, 52(5):789–808, 2005. Preliminary version in FOCS 2004.

27 Subhash Khot. Hardness of approximating the shortest vector problem in high ℓ_p norms. *J. Comput. Syst. Sci.*, 72(2):206–219, 2006. Preliminary version in FOCS 2003.

28 Ralf Koetter and Alexander Vardy. Algebraic soft-decision decoding of Reed-Solomon codes. *IEEE Trans. Inf. Theory*, 49(11):2809–2825, 2003.

29 Swastik Kopparty. Personal communication, 2020.

30 D. G. Mead. Newton's identities. *The American Mathematical Monthly*, 99(8):749, October 1992. `doi:10.2307/2324242`.

31 Daniele Micciancio. The shortest vector in a lattice is hard to approximate to within some constant. *SIAM J. Comput.*, 30(6):2008–2035, 2000. Preliminary version in FOCS 1998.

32 Daniele Micciancio. Inapproximability of the shortest vector problem: Toward a deterministic reduction. *Theory Comput.*, 8(1):487–512, 2012.

33 Daniele Micciancio and Antonio Nicolosi. Efficient bounded distance decoders for Barnes-Wall lattices. In *ISIT*, pages 2484–2488. IEEE, 2008.

34 Ethan Mook and Chris Peikert. Lattice (list) decoding near Minkowski's inequality. *IEEE Trans. Inf. Theory*, 68(2):863–870, 2022.

35 Chris Peikert. Limits on the hardness of lattice problems in ℓ_p norms. *Computational Complexity*, 17(2):300–351, May 2008. Preliminary version in CCC 2007.

36 Chris Peikert. A decade of lattice cryptography. *Found. Trends Theor. Comput. Sci.*, 10(4):283–424, 2016.

37 Ron M. Roth and Paul H. Siegel. Lee-metric BCH codes and their application to constrained and partial-response channels. *IEEE Trans. Inf. Theory*, 40(4):1083–1096, 1994. doi:10.1109/18.335966.

38 Peter van Emde Boas. Another NP-complete partition problem and the complexity of computing short vectors in a lattice. Technical Report, 1981. Available at https://staff.fnwi.uva.nl/p.vanemdeboas/vectors/mi8104c.html. URL: https://staff.fnwi.uva.nl/p.vanemdeboas/vectors/mi8104c.html.

A Efficient Decoding Near Minkowski's Bound

In this appendix, we show that a recent result of Mook and Peikert [34], which builds on work of Guruswami and Sudan [21] and Koetter and Vardy [28] on list-decoding Reed-Solomon codes, yields a polynomial-time algorithm for decoding lattices $\mathcal{L} = \mathcal{L}^{\perp}(H)$ with $H = H_q(k, \mathbb{F}_q)$ up to distance $\Theta(\sqrt{k})$. We additionally observe that by choosing $k = \Theta(q/\log q)$, such lattices are asymptotically nearly tight with Minkowski's bound (Equation (5)). Putting these observations together, we obtain an efficient algorithm for decoding to a distance within a $O(\sqrt{\log q})$ factor of Minkowski's bound (here $q = n$ is the lattice rank and dimension).

A.1 Construction and Algorithm

Define the additive quotient group $\mathbb{R}_q := \mathbb{R}/(q\mathbb{Z})$ and the Euclidean norm of any $\hat{\boldsymbol{y}} \in \mathbb{R}_q^n$ as

$$\|\hat{\boldsymbol{y}}\| := \min\{\|\boldsymbol{y}\| : \boldsymbol{y} \in \hat{\boldsymbol{y}} + q\mathbb{Z}^n\} \ . \tag{16}$$

Equivalently, $\|\hat{\boldsymbol{y}}\|$ is the standard $\mathbb{R}^n$ Euclidean norm of the unique real vector $\boldsymbol{y} \equiv \hat{\boldsymbol{y}} \pmod{q\mathbb{Z}^n}$ having coordinates in $[-q/2, q/2)$. In additive arithmetic that mixes elements of $\mathbb{F}_q$ and $\mathbb{R}_q$, we implicitly "lift" the former to the latter in the natural way.

We again use the fact that for evaluation set $S = \mathbb{F}_q$, the matrix $H = H_q(k, \mathbb{F}_q)$ defined in Equation (7) is a parity-check matrix of the Reed-Solomon code $\mathrm{RS}_q[q-k, \mathbb{F}_q]$, and therefore $\mathcal{L}^{\perp}(H_q(k, \mathbb{F}_q)) = \mathrm{RS}_q[q-k, \mathbb{F}_q] + q\mathbb{Z}^q$. This view lets us take advantage of the decoding algorithm from the following theorem of [34], which gives an efficient (list) decoder in the ℓ_2 norm for Reed-Solomon codes.[9]

[9] In fact, the cited result from [34] is more general, giving a decoder for $\mathbb{F}_p$-*subfield subcodes* of Reed-Solomon codes over finite fields of order $q = p^r$, for a prime p. Here we need only the special case where the Reed-Solomon code is over a prime field (i.e., where $r = 1$). On the other hand, we note that if Proposition 18 were extended to handle *generalized* Reed-Solomon codes, then we would get a corresponding strengthening of Corollary 19 for decoding lattices $\mathcal{L}^{\perp}(H_q(k, S))$ with general S, not just $S = \mathbb{F}_q$.

▶ **Proposition 18** ([34, Algorithm 1 and Theorem 3.4]). *Let q be a prime, $S \subseteq \mathbb{F}_q$ be an evaluation set of size $n := |S|$, $k \leq n$ be a nonnegative integer, and $\varepsilon > 0$. There is a deterministic algorithm that, on input q, S, k, ε, and a vector $\hat{\boldsymbol{y}} \in \mathbb{R}_q^n$, outputs all codewords $\boldsymbol{c} \in \mathrm{RS}_q[n-k, S]$ such that $\|\hat{\boldsymbol{y}} - \boldsymbol{c}\|^2 \leq (1-\varepsilon)(k+1)/2$, in time polynomial in n, $\log q$, and $1/\varepsilon$.*[10]

The following corollary, which is the main result of this section, says that by taking $S = \mathbb{F}_q$ and $k = \Theta(q/\log q)$, (1) the root Hermite factor of $\mathcal{L}^\perp(H)$ is within an $O(\sqrt{\log q})$ factor of Minkowski's bound (Equation (5)), and (2) it is possible to efficiently decode this lattice to a distance of $\Omega(\sqrt{k}) = \Omega(\sqrt{q/\log q})$, which is again within an $O(\sqrt{\log q})$ factor of Minkowski's bound.

We remark that by setting $\varepsilon \leq 1/(k+1)$ in Corollary 19, we get efficient decoding to a distance at least $\sqrt{k/2}$ but less than $\sqrt{(k+1)/2}$, which is slightly more than half the lower bound of $\sqrt{2k}$ on the minimum Euclidean distance of the lattice (Theorem 14). Recall that this lower bound is tight when k is a proper divisor of $q-1$ (see Lemma 15), so with this parameterization we get efficient *list* decoding (i.e., the algorithm may return more than one lattice vector) slightly beyond the unique-decoding bound of half the minimum distance.

▶ **Corollary 19** (Efficient decoding near Minkowski's bound). *Let $H = H_q(k, \mathbb{F}_q)$ for a prime q and $k := \lfloor q/(2\log q) \rfloor \leq q/2$, where all logarithms are base two. Then for $\mathcal{L} := \mathcal{L}^\perp(H) \subseteq \mathbb{Z}^q$:*

1. $\sqrt{q/\log q - 2} \leq \sqrt{2k} \leq \lambda_1(\mathcal{L}) \leq \sqrt{q} \cdot \det(\mathcal{L})^{1/q} \leq \sqrt{2q}$.
2. *For any $\varepsilon > 1/\operatorname{poly}(q)$, there is an algorithm that, on input q and a vector $\boldsymbol{y} \in \mathbb{R}^q$, outputs all lattice vectors $\boldsymbol{v} \in \mathcal{L}$ satisfying $\|\boldsymbol{y} - \boldsymbol{v}\| \leq \sqrt{(1-\varepsilon)(k+1)/2}$ in time polynomial in q.*

Proof. For Item 1, we have

$$\sqrt{q/\log q - 2} \leq \sqrt{2k} \leq \lambda_1(\mathcal{L}) \leq \sqrt{q} \cdot \det(\mathcal{L})^{1/q} = \sqrt{q} \cdot q^{k/q} \leq \sqrt{2q}\ .$$

The first inequality follows from the choice of k, the second inequality is by Theorem 14, the third inequality is Minkowski's bound (Equation (5)), the equality follows from Lemma 4 (recall that the rows of H are linearly independent), and the final inequality again follows from the choice of k.[11]

The algorithm claimed in Item 2 works as follows. First, it computes k and $\hat{\boldsymbol{y}} = \boldsymbol{y} \bmod q\mathbb{Z}^q \in \mathbb{R}_q^q$ from the input q and $\boldsymbol{y}$. It then calls the algorithm from Proposition 18 on q, $S = \mathbb{F}_q$, k, ε, and $\hat{\boldsymbol{y}}$, and receives as output zero or more codewords $\boldsymbol{c} \in \mathrm{RS}_q[q-k, \mathbb{F}_q]$. For each such $\boldsymbol{c}$, it outputs the unique vector $\boldsymbol{v} := \arg\min_{\boldsymbol{v}' \in \boldsymbol{c} + q\mathbb{Z}^q} \|\boldsymbol{y} - \boldsymbol{v}'\| \in \mathcal{L}$.

The value k and vectors $\hat{\boldsymbol{y}}$, $\boldsymbol{v}$ can be computed efficiently (assuming that $\boldsymbol{v}$ is well defined), so it is clear from Proposition 18 that this algorithm runs in time polynomial in q (recall that the dimension $n = q$). It remains to show correctness. First, it is immediate from the definitions that for any $r < q/2$, the function $f(\boldsymbol{v}) = \boldsymbol{v} \bmod q\mathbb{Z}^q$ is a bijection from the set of lattice vectors

$$\{\boldsymbol{v} \in \mathcal{L} : \|\boldsymbol{y} - \boldsymbol{v}\| \leq r\}\ ,$$

[10] Formally, the runtimes of the decoding algorithms in Proposition 18 and Corollary 19 additionally depend on the lengths of the respective "received words" $\hat{\boldsymbol{y}}$ and $\boldsymbol{y}$ that they take as input, which must be specified to finite precision. However, for simplicity we describe the algorithms in the "Real RAM model," while noting that their runtime dependence on the encoding lengths of $\hat{\boldsymbol{y}}, \boldsymbol{y}$ is polynomial.

[11] Analyzing the derivative of $\log(\sqrt{2k}/q^{k/q})$ with respect to k shows that our choice of k is asymptotically optimal for maximizing the root Hermite factor of $\mathcal{L}^\perp(H_q(k, \mathbb{F}_q))$.

to the set of codewords

$$\{\boldsymbol{c} \in \mathrm{RS}_q[q-k, \mathbb{F}_q] : \|\hat{\boldsymbol{y}} - \boldsymbol{c}\| \leq r\} \ ,$$

and that $g(\boldsymbol{c}) := \arg\min_{\boldsymbol{v}' \in \boldsymbol{c}+q\mathbb{Z}^q} \|\boldsymbol{y} - \boldsymbol{v}'\|$ is the inverse function of f, i.e., $g = f^{-1}$. Moreover, because $q \geq 2$, we have that the decoding distance r satisfies

$$r := \sqrt{(1-\varepsilon)(k+1)/2} \leq \sqrt{(1-\varepsilon)(q/(2\log q)+1)/2} \leq \sqrt{1-\varepsilon} \cdot q/2 < q/2 \ .$$

Because the algorithm from Proposition 18 outputs (exactly) $\{\boldsymbol{c} \in \mathrm{RS}_q[q-k, \mathbb{F}_q] : \|\hat{\boldsymbol{y}} - \boldsymbol{c}\| \leq r\}$, it follows that the algorithm described above outputs (exactly) $\{\boldsymbol{v} \in \mathcal{L} : \|\boldsymbol{y} - \boldsymbol{v}\| \leq r\}$, as needed. ◀

▶ Remark 20. We remark that the main consequence of Item 1 of Corollary 19 – namely, an explicit construction of a family of lattices having root Hermite factors within a $O(\sqrt{\log n})$ factor of Minkowski's bound, obtained via Construction A (where n is the lattice dimension) – only needs a family of codes satisfying milder conditions than what (generalized) Reed-Solomon codes satisfy. Namely, achieving this result only requires a family of linear q-ary codes $\mathcal{C}$ for prime q with block length n, codimension $k = \Theta(n/\log n)$, and minimum distance (in the Hamming metric) $d = \Omega(k)$. The latter is a weaker condition than *maximum distance separability* (MDS), which requires that $d = k + 1$. Indeed, $d = \Omega(k)$ implies that the corresponding Construction-A lattice $\mathcal{C} + q\mathbb{Z}^n$ has an ℓ_2 minimum distance of $\Omega(\min\{\sqrt{k}, q\})$, which is $\Omega(\sqrt{k})$ when $k = O(q^2)$. So, unlike our main hardness result, Corollary 19 does not use Theorem 14 in any essential way.

Finally, we also note that obtaining a direct analog of Item 2 of Corollary 19 – i.e., efficiently decoding to within an $O(\sqrt{\log n})$ factor of Minkowski's bound on $\mathcal{C} + q\mathbb{Z}^n$ – additionally requires an efficient algorithm for decoding $\mathcal{C}$ to an ℓ_2 distance of $\Omega(\sqrt{k})$, but that this is in turn a weaker requirement than what Proposition 18 fulfills.