One-Sided-Error Parameterized Reductions for the Minimum Distance and Shortest Vector Problems*

Shuichi Hirahara
National Institute of Informatics, Tokyo, Japan

Kazuki Ogitsuka
The Graduate University for Advanced Studies (SOKENDAI), Tokyo, Japan

Abstract

It is notoriously difficult to obtain deterministic reductions for the Minimum Distance Problem (MDP) and the Shortest Vector Problem (SVP). Under two-sided-error randomized reductions, Bennett, Cheraghchi, Guruswami, and Ribeiro (STOC 2023) proved parameterized hardness of approximation for these problems. We partially derandomize their reductions and present one-sided-error randomized reductions: MDP is W[1]-hard to approximate within an arbitrary constant factor under FPT many-one one-sided-error randomized reductions; For every fixed $p \geq 1$, SVP in the ℓ_p norm is W[1]-hard to approximate within an arbitrary constant factor below $2^{1/p}$.

We demonstrate the usefulness of one-sided-error randomized reductions by showing that they can be conditionally derandomized when the target problem has an OR function. Under a standard hardness-vs-randomness assumption, namely a plausible lower-bound assumption against nondeterministic circuits, we prove a general theorem formalizing this derandomization. Here, an OR function combines several instances into one instance that preserves their disjunction. We construct such OR functions for the relevant MDP and SVP gap problems, and thereby obtain deterministic W[1]-hardness for approximating MDP over every fixed finite field within every constant factor, and for approximating SVP in ℓ_p norms for every fixed integer p within every factor below $2^{1/p}$. Applying the same framework to Micciancio's one-sided-error randomized reduction (ToC 2012) yields, under the same circuit lower-bound assumption, deterministic polynomial-time NP-hardness of approximating Euclidean SVP within every constant factor.

2012 ACM Subject Classification Theory of computation → Problems, reductions and completeness

Keywords and phrases Codes, Lattices, Minimum Distance Problem, Shortest Vector Problem, Parameterized complexity, derandomization

Digital Object Identifier 10.4230/LIPIcs.APPROX/RANDOM.2026.46

Category RANDOM

Related Version *Full Version*: https://arxiv.org/abs/2608.14305

Funding This work was supported by JSPS KAKENHI Grant Number JP26KJ1224.

1 Introduction

As fundamental computational problems on codes and lattices, the Minimum Distance Problem (MDP) and the Shortest Vector Problem (SVP) have long been studied. In the gap version, γ-GapMDP$_q$ asks whether a linear code over $\mathbb{F}_q$ has a nonzero codeword of Hamming weight at most k, or whether every nonzero codeword has weight larger than γk. Similarly, γ-GapSVP$_p$ asks whether an integer lattice has a nonzero vector of ℓ_p norm at most d, or whether every nonzero vector has norm larger than γd. For further background, see surveys and standard textbooks [3, 31, 35, 41].

* Due to space limitations, some details are omitted from this version.

For MDP, Dumer, Micciancio, and Sudan [18] proved randomized NP-hardness for every constant approximation factor. Cheng and Wan [13] derandomized this result, Austrin and Khot [5] and Micciancio [34] gave simpler deterministic reductions. For SVP, van Emde Boas [39] proved NP-hardness of the decision version in the ℓ_∞ norm and conjectured hardness in the Euclidean norm. Ajtai [4] proved randomized NP-hardness of Euclidean SVP. Subsequent work by Khot [27, 28], Haviv and Regev [23], Micciancio [32, 33], and Bennett and Peikert [9] established stronger randomized hardness results for GapSVP$_p$ in several norms and approximation regimes. More recently, Hecht and Safra [24], Hair and Sahai [22, 21], and Wan [40] obtained deterministic hardness results for SVP in finite ℓ_p norms.

Parameterized complexity emerged as a systematic framework in the late 1980s and early 1990s, mainly through the work of Downey and Fellows [15, 16, 17], building on earlier work with Langston; see also [14]. In this framework, the running time of an algorithm is measured not only as a function of the input length n, but also as a function of an additional parameter k. A parameterized problem is *fixed-parameter tractable* if it can be solved in time $f(k) \cdot n^{O(1)}$ for some computable function f. The class of such problems is denoted by FPT. The standard hardness notion used to rule out fixed-parameter tractability is W[1]-hardness, which plays a role analogous to NP-hardness in classical complexity theory. For γ-GapMDP$_q$ and γ-GapSVP$_p$, one of the natural parameters is the distance threshold. Bhattacharyya, Bonnet, Egri, Ghoshal, Karthik C. S., Lin, Manurangsi, and Marx [11] proved that γ-GapMDP$_2$ is W[1]-hard under randomized reductions for every constant $\gamma \geq 1$. They also proved that, for every fixed $p > 1$, γ-GapSVP$_p$ is W[1]-hard for every $\gamma \in [1, (1/2 + 1/2^p)^{-1/p})$, again under randomized reductions. Bennett, Cheraghchi, Guruswami, and Ribeiro [7] extended these parameterized hardness results to GapMDP$_q$ over every fixed finite field and to GapSVP$_p$ in finite ℓ_p norms. More precisely, for every fixed $p > 1$, they proved W[1]-hardness for every constant approximation factor $\gamma \geq 1$. For the remaining case $p = 1$, they proved W[1]-hardness for every $\gamma \in [1, 2)$. Except for binary MDP in [11], these parameterized reductions have two-sided error. In the classical setting, randomized reductions with one-sided error were already used by Micciancio [32, 33] and Bennett and Peikert [9]; Wan [40] subsequently derandomized this line for approximation factors $\gamma \in [1, 2^{1/p})$.

1.1 Our Results

Our first contribution is to strengthen the parameterized hardness reductions of Bennett, Cheraghchi, Guruswami, and Ribeiro [7] from two-sided error to one-sided error.

Our first theorem proves this for γ-GapMDP$_q$ over every fixed finite field, without losing their hardness [7] for every constant approximation factor.

▶ **Theorem 1.** *For every fixed prime power $q \geq 2$ and every constant $\gamma \geq 1$, γ-GapMDP$_q$ is* W[1]*-hard under randomized* FPT *many-one reductions with one-sided error.*

Our second theorem proves the corresponding statement for γ-GapSVP$_p$ in the range $\gamma < 2^{1/p}$.

▶ **Theorem 2.** *For any fixed $p \in [1, \infty)$ and constant $\gamma \in [1, 2^{1/p})$, γ-GapSVP$_p$ is* W[1]*-hard under randomized* FPT *many-one reductions with one-sided error.*

In the classical setting, Micciancio [33] viewed his randomized reduction with one-sided error for the NP-hardness of γ-GapSVP$_2$ as a *partial derandomization*. Following this terminology, Theorems 1 and 2 can be viewed as a partial derandomization of the randomized parameterized hardness reductions of MDP and SVP.

The significance of one-sidedness is that it provides a route to removing the remaining randomness under standard hardness-vs-randomness assumptions. Our second contribution is to show that, for MDP and SVP, the randomized hardness results with one-sided error above can be converted into deterministic hardness results under a standard circuit lower-bound assumption. We assume that there exists an $\varepsilon > 0$ such that

$$\mathsf{E} := \mathsf{DTIME}(2^{O(n)}) \not\subseteq i.o.\text{-}\mathrm{NSIZE}(2^{\varepsilon n}).$$

Here, $\mathrm{NSIZE}(s(n))$ denotes the class of languages decidable by nondeterministic circuits of size $O(s(n))$, and i.o. stands for "infinitely often". Under this assumption, we show in Section 4 that suitable one-sided-error randomized reductions to promise problems with OR functions can be made deterministic. An OR function combines a finite list of instances into a single instance that is YES if at least one input is YES, and is NO if all inputs are NO. In the parameterized setting, we additionally require the output parameter to be bounded by a computable function of the largest input parameter.

To apply this framework to MDP and SVP, we show that the relevant gap problems have the required OR functions.

▶ **Proposition 3** (Informal; see Lemmas 36–38)**.** *Let $\gamma \geq 1$ be a constant. The following hold.*

1. *For every fixed prime power $q \geq 2$, γ-GapMDP_q, parameterized by the distance threshold, has an FPT OR function.*
2. *For every fixed $p \geq 1$, γ-GapSVP_p has a polynomial-time OR function. Moreover, when parameterized by the distance threshold, γ-GapSVP_p has an FPT OR function.*

Combining the general derandomization framework with the OR functions for MDP and SVP yields the following deterministic hardness results. They show that one-sidedness is not merely a stronger error guarantee.

▶ **Theorem 4.** *Assume that there exists an $\varepsilon > 0$ such that*

$$\mathsf{E} \not\subseteq i.o.\text{-}\mathrm{NSIZE}(2^{\varepsilon n}).$$

Then, for every fixed prime power $q \geq 2$ and constant $\gamma \geq 1$, γ-GapMDP_q is $\mathsf{W}[1]$-hard under deterministic FPT many-one reductions.

▶ **Theorem 5.** *Assume that there exists an $\varepsilon > 0$ such that*

$$\mathsf{E} \not\subseteq i.o.\text{-}\mathrm{NSIZE}(2^{\varepsilon n}).$$

For every fixed integer $p \geq 1$ and constant $\gamma \in [1, 2^{1/p})$, γ-GapSVP_p is $\mathsf{W}[1]$-hard under deterministic FPT many-one reductions.[1]

Finally, the conditional derandomization principle also applies to the classical, non-parameterized setting. Starting from Micciancio's randomized hardness result with one-sided error for γ-GapSVP_2 [33], we obtain a deterministic hardness result under the same circuit lower-bound assumption.

▶ **Theorem 6.** *Assume that there exists an $\varepsilon > 0$ such that*

$$\mathsf{E} \not\subseteq i.o.\text{-}\mathrm{NSIZE}(2^{\varepsilon n}).$$

Then, for every fixed constant $\gamma \geq 1$, γ-GapSVP_2 is NP-hard under deterministic polynomial-time many-one reductions.

[1] More generally, the result holds for every fixed $p \geq 1$ such that the language of pairs $(\mathbf{B}, d)$, where $\mathbf{B} \in \mathbb{Z}^{m \times n}$ is a lattice basis, $d \in \mathbb{Z}_{>0}$, and there exists $\boldsymbol{z} \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$ with $\|\mathbf{B}\boldsymbol{z}\|_p \leq d$, belongs to NP.

Compared with Wan's unconditional deterministic polynomial-time many-one hardness result for $1 \leq \gamma < \sqrt{2}$ [40], Theorem 6 extends the approximation range to every constant $\gamma \geq 1$, at the cost of the circuit lower-bound assumption above.

1.2 Technical Overview

The reductions follow Khot's approach [27] used by Bennett, Cheraghchi, Guruswami, and Ribeiro [7]. In that approach, a locally dense object is combined with an inhomogeneous instance, and a random sparsification step is used to make the output homogeneous. The random step has two roles: in YES instances, it should preserve at least one good vector; in NO instances, it should rule out annoying short vectors.

For MDP, we keep the random linear map used for the YES case, but add a deterministic checking block. The block is built from a BCH parity-check matrix $\mathbf{P}$ and a syndrome amplification map $\mathbf{E}$. Every nonzero vector of Hamming weight at most the relevant threshold has a nonzero syndrome under $\mathbf{P}$, and $\mathbf{E}$ expands any nonzero syndrome into more than the allowed number of nonzero coordinates. Thus every potential short vector in a NO instance is ruled out deterministically.

For SVP, the checking block is analogous. We choose a prime q, use a Reed–Solomon parity-check matrix modulo q, and lift it to the integers. A large scaling factor forces any nonzero syndrome in the checking block to have norm above the soundness threshold. The proof then separates possible short lattice vectors according to the coefficient of the target vector and shows that all cases are impossible in NO instances, independently of the remaining randomness.

For the conditional hardness of MDP and SVP, we assume that there exists an $\varepsilon > 0$ such that

$$\mathsf{E} \not\subseteq i.o.\text{-NSIZE}(2^{\varepsilon n}).$$

By the hardness-vs-randomness results of Impagliazzo and Wigderson [26], Klivans and van Melkebeek [29], and Shaltiel and Umans [38], this assumption gives logarithmic-seed pseudorandom generators against polynomial-size nonadaptive SAT-oracle circuits. For a fixed input, let $\phi(r)$ be the predicate that the random tape r makes the randomized reduction output a YES instance. On YES inputs, completeness gives $\Pr[\phi(r) = 1] \geq 2/3$. For the MDP and SVP instances used in our conditional applications, the YES language of the target problem belongs to NP. Thus the success predicate ϕ can be represented by the SAT oracle circuits considered above. The generator obtained from the circuit lower bound has logarithmic seed length and guarantees that, whenever such a predicate ϕ accepts at least a $2/3$ fraction of random tapes, there is a seed σ such that $\phi(G(\sigma)) = 1$. Hence it suffices to enumerate all seeds of G, run the reduction using the corresponding tapes $G(\sigma)$, and combine the outputs by an OR function. On NO inputs, every tape gives a NO instance since the reduction has a one-sided error. For promise problems, an OR function maps a tuple of instances to a single instance that is YES if at least one input is YES, and is NO if all inputs are NO.

1.3 Related Work

Fine-grained hardness of lattice problems and related problems has been studied under assumptions such as ETH, SETH, Gap-ETH, and Gap-SETH. Relevant results include hardness for SVP by Aggarwal and Stephens-Davidowitz [2], hardness for Bounded Distance Decoding (BDD) in ℓ_p norms by Bennett and Peikert [8], improved bounds for BDD and

SVP by Bennett, Peikert, and Tang [10], lower bounds for parameterized Nearest Codeword Problem (NCP) and related problems by Li, Lin, and Liu [30], consequences for parameterized MDP, Closest Vector Problem (CVP), and SVP via earlier gap-preserving reductions [11, 7], and recent ETH-based hardness results for CVP, SVP, and BDD by Aggarwal, Gupta, Morolia, and Zhang [1]. Several of the lattice hardness results cited above use locally dense lattice gadgets, sparsification, or both, but the specific gadgets and reductions in those works differ from ours.

Hittmeir [25] proved deterministic fine-grained hardness results for GapSVP_p in a different parameterized setting, where p is part of the input and also serves as the parameter. In contrast, in this paper p is fixed and the distance threshold is the parameter.

OR functions and related combining reductions have appeared in other contexts. Chang and Kadin [12] studied polynomial-time OR functions for languages, and Ball, Boyle, Degwekar, Deshpande, Rosen, Vaikuntanathan, and Vasudevan [6] studied lossy reductions that combine several input instances according to a Boolean function.

There is also an earlier conditional route to deterministic hardness for SVP: Micciancio [32] proved deterministic many-one NP-hardness of approximating SVP under a number-theoretic conjecture on the distribution of square-free smooth numbers.

1.4 Open Problems

Our results leave several natural open questions. Can the assumption $\mathsf{E} \not\subseteq i.o.\text{-NSIZE}(2^{\varepsilon n})$ for some $\varepsilon > 0$ be removed from Theorems 4 and 5? For SVP, Theorem 2 gives randomized $\mathsf{W}[1]$-hardness with one-sided error for $\gamma < 2^{1/p}$, whereas Bennett, Cheraghchi, Guruswami, and Ribeiro [7] obtained randomized hardness with two-sided error for every constant factor for fixed $p > 1$; can their entire approximation range be made one-sided error? For the Euclidean norm, Wan [40] proved deterministic polynomial-time NP-hardness of γ-GapSVP_2 for every constant $1 \le \gamma < \sqrt{2}$; can deterministic polynomial-time many-one hardness be extended to every constant $\gamma \ge \sqrt{2}$?

2 Preliminaries

2.1 Notations

All vectors are column vectors unless stated otherwise. For a positive integer N, we write $[N] := \{1, \dots, N\}$. We write $\mathbb{Z}_{>0}$ for the set of positive integers. For a finite set S, its cardinality is denoted by $|S|$; for a string x, its bit length is denoted by $|x|$. We use $\langle x_1, \dots, x_t \rangle$ for a standard polynomial-time computable encoding of a tuple. Unless explicitly indicated otherwise, logarithms are base 2; $\log_q$ denotes logarithm with base q. We use $\mathrm{poly}(\cdot)$ for an unspecified polynomial and allow constants hidden in $O(\cdot)$ to depend on fixed constants such as p and q, and on γ whenever γ is fixed throughout the statement. We write U_n for the uniform distribution over $\{0,1\}^n$.

For a map $f\colon X \to Y$ and subset $S \subseteq X$, we write $f(S) := \{f(x) : x \in S\} \subseteq Y$ for the image of S under f. For a set S in an abelian group and an element a, we write $S - a := \{s - a : s \in S\}$.

For $\boldsymbol{x} = (x_1, \dots, x_m)$, its support is $\mathrm{supp}(\boldsymbol{x}) := \{i \in [m] : x_i \neq 0\}$. For vectors over either $\mathbb{F}_q$ or $\mathbb{Z}$, we write $\|\boldsymbol{x}\|_0 := |\mathrm{supp}(\boldsymbol{x})|$. For $\boldsymbol{x} \in \mathbb{R}^m$ and $p \in [1, \infty)$, we write $\|\boldsymbol{x}\|_p := (\sum_{i=1}^m |x_i|^p)^{1/p}$, and $\|\boldsymbol{x}\|_\infty := \max_i |x_i|$. The Hamming distance between two vectors over $\mathbb{F}_q$ is $\|\boldsymbol{x} - \boldsymbol{y}\|_0$. For $r \ge 0$, define the Hamming ball over $\mathbb{F}_q^m$ by $B_{q,m}(r) := \{\boldsymbol{x} \in \mathbb{F}_q^m : \|\boldsymbol{x}\|_0 \le r\}$ and the ℓ_p ball in $\mathbb{R}^m$ by $\mathcal{B}_p^m(r) := \{\boldsymbol{x} \in \mathbb{R}^m : \|\boldsymbol{x}\|_p \le r\}$. When integer vectors are intended, we use $\mathcal{B}_p^m(r) \cap \mathbb{Z}^m$ implicitly.

2.2 Probability Theory

We use a standard consequence of Chebyshev's inequality.

▶ **Lemma 7.** *Let $X_1, \ldots, X_N$ be pairwise independent random variables over $\{0,1\}$ such that $\Pr[X_i = 1] = p > 0$ for $i = 1, \ldots, N$. Then, it holds that*

$$\Pr[\forall i \in [N], X_i = 0] \leq \frac{1}{pN}.$$

2.3 Promise Problems and Reductions

A promise problem is a pair $\Pi = (\Pi_{\text{YES}}, \Pi_{\text{NO}})$ of disjoint languages. A parameterized promise problem is such a pair whose instances are pairs (x, k), where $k \in \mathbb{N}$ is the parameter. For details on promise problems and parameterized complexity, see the survey by Goldreich [19] and the textbooks by Downey and Fellows [17, 16, 15].

Some reductions used are randomized. They are required to preserve NO instances for every choice of randomness, while YES instances need only be mapped correctly with constant probability.

▶ **Definition 8** (Randomized many-one reductions with one-sided error)**.** *Let $\Pi = (\Pi_{\text{YES}}, \Pi_{\text{NO}})$ and $\Pi' = (\Pi'_{\text{YES}}, \Pi'_{\text{NO}})$ be promise problems. A randomized polynomial-time algorithm R is called a randomized many-one reduction with one-sided error from Π to Π' if, on every input x, it outputs a single instance $R(x; r)$ in the input format of Π', and the following hold:*
1. *if $x \in \Pi_{\text{YES}}$, then $\Pr_r[R(x; r) \in \Pi'_{\text{YES}}] \geq 2/3$;*
2. *if $x \in \Pi_{\text{NO}}$, then $\Pr_r[R(x; r) \in \Pi'_{\text{NO}}] = 1$.*

In particular, for YES inputs we allow unsuccessful random strings to produce outputs outside the promise of Π'.

For parameterized problems, we also require that the running time be fixed-parameter tractable and that the output parameter depend only on the input parameter. This gives the parameterized analogue of the preceding randomized reduction.

▶ **Definition 9** (Randomized FPT many-one reductions with one-sided error)**.** *Let $\Pi = (\Pi_{\text{YES}}, \Pi_{\text{NO}})$ and $\Pi' = (\Pi'_{\text{YES}}, \Pi'_{\text{NO}})$ be parameterized promise problems. A randomized algorithm R is called a randomized* FPT *many-one reduction with one-sided error from Π to Π' if there exist a computable function T, a computable function g, and a constant $c > 0$ such that, on input (x, k), the algorithm runs in time at most $T(k) \cdot |x|^c$, outputs a pair (x', k'), and satisfies*
1. *$k' \leq g(k)$;*
2. *if $(x, k) \in \Pi_{\text{YES}}$, then $\Pr[(x', k') \in \Pi'_{\text{YES}}] \geq 2/3$;*
3. *if $(x, k) \in \Pi_{\text{NO}}$, then $\Pr[(x', k') \in \Pi'_{\text{NO}}] = 1$.*

▶ Remark 10. With respect to the fixed encoding of tuples, the running-time bounds

$$T(k) \cdot |x|^c \qquad \text{and} \qquad T'(k) \cdot |\langle x, k \rangle|^c$$

are equivalent up to replacing T by another computable function of k. Therefore, in Definition 9 (and deterministic FPT many-one reduction), one may measure the polynomial factor using either $|x|$ or $|\langle x, k \rangle|$.

We assume that all random choices are implemented using a fixed-length random tape whose length is computable within the stated running-time bound. Standard bounded rejection sampling is used when necessary, and its arbitrarily small loss is absorbed into the completeness probability.

2.4 Coding Problems

For a matrix $\mathbf{G} \in \mathbb{F}_q^{m \times n}$, the linear code generated by the columns of $\mathbf{G}$ is $\mathcal{C} = \mathcal{C}(\mathbf{G}) := \{\mathbf{G}\boldsymbol{x} : \boldsymbol{x} \in \mathbb{F}_q^n\} \subseteq \mathbb{F}_q^m$. The minimum distance of a nonzero linear code $\mathcal{C} \subseteq \mathbb{F}_q^m$ is $\lambda(\mathcal{C}) := \min_{\boldsymbol{c} \in \mathcal{C} \setminus \{\mathbf{0}\}} \|\boldsymbol{c}\|_0$. We use the convention $\lambda(\{\mathbf{0}\}) := +\infty$. For a target vector $\boldsymbol{t} \in \mathbb{F}_q^m$, we write $\mathrm{dist}(\mathcal{C}, \boldsymbol{t}) := \min_{\boldsymbol{c} \in \mathcal{C}} \|\boldsymbol{c} - \boldsymbol{t}\|_0$.

The Minimum Distance Problem (MDP) asks for the Hamming weight of the shortest nonzero codeword in a given linear code. In this paper we use its gap version, where one distinguishes codes of minimum distance at most k from those of minimum distance greater than γk.

▶ **Definition 11** (γ-GapMDP$_q$, [18]). *For $\gamma \geq 1$ and a prime power $q \geq 2$, the (parameterized) promise problem γ-approximate Minimum Distance Problem over $\mathbb{F}_q$ (γ-GapMDP$_q$) is defined as follows. Instances are pairs $(\mathbf{G}, k)$, where $\mathbf{G} \in \mathbb{F}_q^{m \times n}$ is a generator matrix of $\mathcal{C}(\mathbf{G})$, and $k \in \mathbb{Z}_{>0}$ is a distance parameter such that*

1. *$(\mathbf{G}, k)$ is a YES instance if $\lambda(\mathcal{C}(\mathbf{G})) \leq k$;*
2. *$(\mathbf{G}, k)$ is a NO instance if $\lambda(\mathcal{C}(\mathbf{G})) > \gamma k$.*

The parameter of interest is k.

The Nearest Codeword Problem (NCP) is the inhomogeneous analogue of MDP: given a target vector, it asks whether some codeword is close to the target. We will use NCP as the starting point for reductions to MDP.

▶ **Definition 12** (γ-GapNCP$_q$, [18]). *For $\gamma \geq 1$ and a prime power $q \geq 2$, the (parameterized) promise problem γ-approximate Nearest Codeword Problem over $\mathbb{F}_q$ (γ-GapNCP$_q$) is defined as follows. Instances are tuples $(\mathbf{G}, \boldsymbol{t}, k)$, where $\mathbf{G} \in \mathbb{F}_q^{m \times n}$ is a generator matrix of $\mathcal{C}(\mathbf{G})$, $\boldsymbol{t} \in \mathbb{F}_q^m$ is a target vector, and $k \in \mathbb{Z}_{>0}$ is a distance parameter such that*

1. *$(\mathbf{G}, \boldsymbol{t}, k)$ is a YES instance if $\mathrm{dist}(\mathcal{C}(\mathbf{G}), \boldsymbol{t}) \leq k$;*
2. *$(\mathbf{G}, \boldsymbol{t}, k)$ is a NO instance if $\mathrm{dist}(\mathcal{C}(\mathbf{G}), \boldsymbol{t}) > \gamma k$.*

The parameter of interest is k.

The next theorem states the W[1]-hardness of γ-GapNCP$_q$. We will use this result later in the reduction to γ-GapMDP$_q$.

▶ **Theorem 13** ([11, Theorem 5.1, adapted] and [7, Theorem 2.7]). *For any real number $\gamma \geq 1$ and any prime power $q \geq 2$, γ-GapNCP$_q$ is W[1]-hard.*

2.5 Lattice Problems

We now turn to the lattice problems considered in the paper. The lattice analogues of the above coding problems are measured with respect to ℓ_p norms.

For a matrix $\mathbf{B} \in \mathbb{Z}^{m \times n}$, the lattice generated by the columns of $\mathbf{B}$ is $\mathcal{L} = \mathcal{L}(\mathbf{B}) := \{\mathbf{B}\boldsymbol{z} : \boldsymbol{z} \in \mathbb{Z}^n\} \subseteq \mathbb{Z}^m$; that is, $\mathcal{L}(\mathbf{B})$ consists of all integer linear combinations of the columns of $\mathbf{B}$. If the columns of $\mathbf{B}$ are linearly independent, then $\mathbf{B}$ is called a lattice basis of $\mathcal{L}(\mathbf{B})$. For $p \in [1, \infty]$, the ℓ_p length of a shortest nonzero lattice vector is $\lambda_1^{(p)}(\mathcal{L}) := \min_{\boldsymbol{v} \in \mathcal{L} \setminus \{\mathbf{0}\}} \|\boldsymbol{v}\|_p$. For a target vector $\boldsymbol{t} \in \mathbb{R}^m$, we write $\mathrm{dist}_p(\mathcal{L}, \boldsymbol{t}) := \min_{\boldsymbol{v} \in \mathcal{L}} \|\boldsymbol{v} - \boldsymbol{t}\|_p$.

One of the central problems on lattices is the Shortest Vector Problem (SVP), which is to find a shortest non-zero vector in a given lattice. In this paper, we study the promise problem version of the Shortest Vector Problem, which is defined as follows:

▶ **Definition 14** (γ-GapSVP$_p$, [20]). *For $p \geq 1$ and $\gamma \geq 1$, the (parameterized) promise problem γ-approximate Shortest Vector Problem (γ-GapSVP$_p$) is defined as follows. Instances are pairs $(\mathbf{B}, d)$, where $\mathbf{B} \in \mathbb{Z}^{m \times n}$ is a lattice basis of $\mathcal{L}(\mathbf{B})$, and $d \in \mathbb{Z}_{>0}$ is a distance parameter such that*

1. $(\mathbf{B}, d)$ *is a YES instance if* $\lambda_1^{(p)}(\mathcal{L}(\mathbf{B})) \le d$;
2. $(\mathbf{B}, d)$ *is a NO instance if* $\lambda_1^{(p)}(\mathcal{L}(\mathbf{B})) > \gamma d$.

The parameter of interest is d.

We will also use the following classical NP-hardness result for approximate SVP for ℓ_2 norm. This theorem is the non-parameterized hardness input for the deterministic hardness result later in the paper.

▶ **Theorem 15** ([33, Corollary 6.3]). *For any constant* $\gamma \ge 1$, γ-GapSVP$_2$ *is* NP*-hard under randomized many-one reductions with one-sided error.*

The Closest Vector Problem (CVP) is the inhomogeneous analogue of SVP: given a lattice and a target vector, it asks whether the target is close to some lattice vector. For the reduction to GapSVP, we use the following gap variant, whose NO instances require all lattice vectors to be far from every nonzero integer multiple of the target vector.

▶ **Definition 16** (γ-GapCVP$_p$, [7]). *For* $p \ge 1$ *and* $\gamma \ge 1$, *the (parameterized) promise problem* γ*-approximate Closest Vector Problem (*γ-GapCVP$_p$*) is defined as follows. Instances are tuples* $(\mathbf{B}, \boldsymbol{t}, d)$, *where* $\mathbf{B} \in \mathbb{Z}^{m \times n}$ *is a lattice basis of* $\mathcal{L}(\mathbf{B})$, $\boldsymbol{t} \in \mathbb{Z}^m$ *is a target vector, and* $d \in \mathbb{Z}_{>0}$ *is a distance parameter such that*

1. $(\mathbf{B}, \boldsymbol{t}, d)$ *is a YES instance if* $\mathrm{dist}_p(\mathcal{L}(\mathbf{B}), \boldsymbol{t}) \le d$;
2. $(\mathbf{B}, \boldsymbol{t}, d)$ *is a NO instance if* $\mathrm{dist}_p(\mathcal{L}(\mathbf{B}), w\boldsymbol{t}) > \gamma d$ *for all* $w \in \mathbb{Z} \setminus \{0\}$.

The parameter of interest is d.

The following theorem provides the parameterized hardness of this CVP variant. It will be combined with our randomized reduction from CVP to SVP.

▶ **Theorem 17** ([11, Theorem 7.2] and [7, Theorem 2.11]). *For any real numbers* $\gamma \ge 1$ *and* $p \ge 1$, γ-GapCVP$_p$ *is* W[1]*-hard under deterministic* FPT *many-one reductions.*

▶ Remark 18. In [11], the NO instance condition for γ-GapCVP$_p$ is stated as $\mathrm{dist}_p(\mathcal{L}(\mathbf{B}), \boldsymbol{t}) > \gamma d$, but their proof in fact shows that $\mathrm{dist}_p(\mathcal{L}(\mathbf{B}), w\boldsymbol{t}) > \gamma d$ for every nonzero integer $w \in \mathbb{Z} \setminus \{0\}$.

2.6 OR functions

An OR function is a deterministic map that, given a finite tuple of strings, outputs one instance of the same promise problem, with the guarantee that it outputs YES if at least one input is a YES instance and outputs NO if all inputs are NO instances.

▶ **Definition 19** (OR functions of a promise problem). *A promise problem* Π *has a polynomial-time OR function if there is a deterministic polynomial-time algorithm* C *such that, for every tuple* $(x_1, \ldots, x_t)$, *if some* $x_i \in \Pi_{\mathrm{YES}}$, *then* $C(x_1, \ldots, x_t) \in \Pi_{\mathrm{YES}}$, *and if all* $x_i \in \Pi_{\mathrm{NO}}$, *then* $C(x_1, \ldots, x_t) \in \Pi_{\mathrm{NO}}$.

▶ **Definition 20** (FPT OR functions of a parameterized promise problem). *A parameterized promise problem* Π *has an* FPT *OR function if there is a deterministic algorithm* C *and computable functions* T, g *such that, on input* $((x_1, k_1), \ldots, (x_t, k_t))$, *the algorithm runs in time* $T(\kappa)N^{O(1)}$, *where* $\kappa = \max_i k_i$ *and* $N = \sum_i |\langle x_i, k_i \rangle|$, *outputs* (y, ℓ) *with* $\ell \le g(\kappa)$, *and satisfies the same YES/NO OR guarantee as above.*

2.7 Circuits and Pseudorandom Generators

Finally, we recall the circuit classes and pseudorandom generators used in the derandomization argument. A nondeterministic circuit is a Boolean circuit with additional nondeterministic input wires; it accepts an input if some assignment to these wires makes the circuit output 1. For a function $s\colon \mathbb{N} \to \mathbb{N}$, $\mathrm{NSIZE}(s(n))$ denotes the class of languages decided by families of nondeterministic circuits of size $O(s(n))$. We write $L \in i.o.\text{-}\mathrm{NSIZE}(s(n))$ if, for infinitely many input lengths n, there is a nondeterministic circuit C_n of size $O(s(n))$ such that for every $x \in \{0,1\}^n$, C_n accepts x if and only if $x \in L$.

We also use nonadaptive SAT-oracle circuits. We write $\mathrm{SIZE}_{\|}^{\mathsf{SAT}}(s(n))$ for languages decided by families of nonadaptive SAT-oracle circuits of size $O(s(n))$. Nonadaptive means that on every path from an input gate to the output gate there is at most one oracle gate.

▶ **Definition 21** (SAT-circuitizable success predicates). *Let R be a randomized FPT many-one reduction from a parameterized promise problem Π to Π'. We say that R has SAT-circuitizable success predicates if there is a polynomial P such that, for every promised input (x,k), if μ is the number of random bits used by R, $m = |\langle x,k\rangle| + \mu$, and*

$$\phi_{x,k}(r) = 1 \iff R((x,k);r) \in \Pi'_{\mathrm{YES}},$$

then $\phi_{x,k}$ is computable by a circuit in $\mathrm{SIZE}_{\|}^{\mathsf{SAT}}(P(m))$. Extra bits of $r \in \{0,1\}^m$ are ignored.

A pseudorandom generator stretches a short seed into a longer string that is indistinguishable from a uniform random string for a specified class of Boolean circuits.

▶ **Definition 22** (Pseudorandom generators against circuit classes). *Let $\mathcal{C} = \{\mathcal{C}_n\}_{n\geq 1}$ be a family of Boolean circuit classes. A family of functions $G_n : \{0,1\}^{m(n)} \to \{0,1\}^n$ is an $\varepsilon(n)$-PRG for $\mathcal{C}$ if, for every sufficiently large n and every Boolean function $D \in \mathcal{C}_n$,*

$$\left| \Pr_{y \leftarrow U_n}[D(y) = 1] - \Pr_{\sigma \leftarrow U_{m(n)}}[D(G_n(\sigma)) = 1] \right| \leq \varepsilon(n).$$

The next theorem is the derandomization tool used in the paper. Under an exponential circuit lower bound for $\mathsf{E} := \mathsf{DTIME}(2^{O(n)})$ against nondeterministic circuits, it gives logarithmic-seed PRGs that fool polynomial-size nonadaptive SAT-oracle circuits.[2]

▶ **Theorem 23** ([26, 29, 38], see also Theorem 2.8 in [37]). *Assume that there exists an $\varepsilon > 0$ such that $\mathsf{E} \not\subseteq i.o.\text{-}\mathrm{NSIZE}(2^{\varepsilon n})$. Then, for every constant $c > 1$, there exists a constant $a > 1$ such that, for all sufficiently large n, there is a $1/n^c$-PRG*

$$G_n : \{0,1\}^{a \log n} \to \{0,1\}^n$$

for $\mathrm{SIZE}_{\|}^{\mathsf{SAT}}(n^c)$, and G_n is computable in time $\mathrm{poly}(n^c)$.

3 W[1]-hardness with One-Sided Error

In this section, we will show that γ-GapMDP_q and γ-GapSVP_p are $\mathsf{W}[1]$-hard under randomized FPT reductions with one-sided error. As in the prior work [7], this reduction is based on locally dense codes/lattices constructed from BCH and Reed–Solomon codes, together with sparsification; however, by additionally incorporating a gadget based on the minimum distance of the locally dense codes/lattices, it achieves one-sided error.

Locally dense codes and locally dense lattices are defined as follows.

[2] In the proof of Theorem 35, the PRG is used only through the following consequence: if $\phi \in \mathrm{SIZE}_{\|}^{\mathsf{SAT}}(m^c)$ satisfies $\Pr_{r \leftarrow U_m}[\phi(r) = 1] \geq 2/3$, then some pseudorandom output $G_m(\sigma)$ satisfies $\phi(G_m(\sigma)) = 1$. Thus an efficiently enumerable polynomial-size hitting set for the same predicates would suffice.

▶ **Definition 24** (Locally dense codes, [7]). *Fix a real number $\alpha \in (0,1)$, positive integers d, N, m, n, and a prime power q. A (q, α, d, N, m, n)-*locally dense code *is specified by a generator matrix $\mathbf{A} \in \mathbb{F}_q^{m \times n}$ and a target vector $\boldsymbol{s} \in \mathbb{F}_q^m$ with the following properties:*

- $\lambda(\mathcal{C}(\mathbf{A})) > d$.
- $|(\mathcal{C}(\mathbf{A}) - \boldsymbol{s}) \cap B_{q,m}(\alpha d)| \geq N$.

▶ **Definition 25** (Locally dense lattices, [7]). *Fix real numbers $\alpha \in (0,1)$ and $p \geq 1$ and positive integers d, N, m, n. A (p, α, d, N, m, n)-*locally dense lattice *is specified by a basis $\mathbf{A} \in \mathbb{Z}^{m \times n}$ and a target vector $\boldsymbol{s} \in \mathbb{Z}^m$ with the following properties:*

- $\lambda_1^{(p)}(\mathcal{L}(\mathbf{A})) > d$.
- $\left|(\mathcal{L}(\mathbf{A}) - \boldsymbol{s}) \cap \mathcal{B}_p^m(\alpha d)\right| \geq N$.

▶ **Lemma 26.** *Let $T \subseteq \mathbb{F}_q^M \setminus \{0\}$ be a set of pairwise linearly independent vectors, and let $\mathbf{R} \in \mathbb{F}_q^{h \times M}$ be uniformly random. For every $\boldsymbol{a} \in \mathbb{F}_q^h$,*

$$\Pr_{\mathbf{R}}[\exists \boldsymbol{w} \in T : \mathbf{R}\boldsymbol{w} = \boldsymbol{a}] \geq 1 - \frac{q^h}{|T|}.$$

Proof. For each $\boldsymbol{w} \in T$, the indicator of the event $\mathbf{R}\boldsymbol{w} = \boldsymbol{a}$ has expectation q^{-h}. Pairwise linear independence of the vectors in T implies pairwise independence of these indicators. The claim follows from Lemma 7. ◀

3.1 W[1]-hardness of γ-GapMDP$_q$ with One-Sided Error

We will show the W[1]-hardness of GapMDP by giving a randomized FPT reduction with one-sided error from GapNCP to GapMDP.

For this, we use properties of BCH codes.

▶ **Theorem 27** (q-ary BCH codes, [7]). *Fix a prime power q. Then, given integers $m' = q^r - 1$ and $1 \leq d \leq m'$ for some integer r, it is possible to construct in time* poly(m′) *a generator matrix $\mathbf{G}_{\mathrm{BCH}} \in \mathbb{F}_q^{m' \times n'}$ such that $\mathcal{C}_{\mathrm{BCH}} = \mathcal{C}(\mathbf{G}_{\mathrm{BCH}}) \subseteq \mathbb{F}_q^{m'}$ has minimum distance at least d and co-dimension*

$$m' - n' \leq \lceil (d-1)(1 - 1/q) \rceil \log_q(m' + 1).$$

Bennett, Cheraghchi, Guruswami, and Ribeiro [7] constructed the following locally dense code using the BCH code from Theorem 27.

▶ **Theorem 28** ([7, Theorem 3.3]). *Fix a prime power $q \geq 2$ and set $\gamma = 4q$. There exists a randomized algorithm which, given positive integers m and $k \leq m$, runs in time* poly(m) *and outputs with probability at least 0.99 a $(q, \alpha, d, N, m', n')$-locally dense code $(\mathbf{A}, \boldsymbol{s})$, where*

$$m', n' \leq \mathrm{poly}(m),$$
$$d = \gamma k = 4qk,$$
$$\alpha = 1 - \frac{1}{2q},$$
$$N = \frac{(qm)^{2d}}{100},$$

provided that m is sufficiently large compared to q. Moreover, $\lambda(\mathcal{C}(\mathbf{A})) > d$ with probability 1.

In addition to these locally dense codes, by using a random matrix and the parity-check matrix of a BCH code, we obtain a randomized FPT reduction with one-sided error.

▶ **Theorem 29.** *For a fixed prime power $q \geq 2$ and real numbers $\gamma := 4q$ and $\gamma' := \gamma/(\gamma-1) = 4q/(4q-1)$, there exists a randomized* FPT *many-one reduction with one-sided error from γ-GapNCP$_q$ to γ'-GapMDP$_q$.*

Proof. We use the following equivalent formulation of $4q$-GapNCP$_q$. An instance $(\mathbf{G}, \boldsymbol{t}, k)$ consists of a matrix $\mathbf{G} \in \mathbb{F}_q^{m \times n}$, a target $\boldsymbol{t} \in \mathbb{F}_q^m$, and an integer $k \geq 1$. In the NO case we are promised that

$$\operatorname{dist}(\mathcal{C}(\mathbf{G}), \beta \boldsymbol{t}) > 4qk \qquad \text{for every } \beta \in \mathbb{F}_q \setminus \{0\}.$$

This is equivalent to the usual definition because, for every $\beta \in \mathbb{F}_q \setminus \{0\}$,

$$\operatorname{dist}(\mathcal{C}(\mathbf{G}), \beta \boldsymbol{t}) = \min_{\boldsymbol{c} \in \mathcal{C}(\mathbf{G})} \|\boldsymbol{c} - \beta \boldsymbol{t}\|_0 = \min_{\boldsymbol{c}' \in \mathcal{C}(\mathbf{G})} \|\beta \boldsymbol{c}' - \beta \boldsymbol{t}\|_0 = \min_{\boldsymbol{c}' \in \mathcal{C}(\mathbf{G})} \|\boldsymbol{c}' - \boldsymbol{t}\|_0 = \operatorname{dist}(\mathcal{C}(\mathbf{G}), \boldsymbol{t}),$$

since $\mathcal{C}(\mathbf{G})$ is closed under multiplication by nonzero field elements and $\|\beta \boldsymbol{v}\|_0 = \|\boldsymbol{v}\|_0$ for all $\boldsymbol{v} \in \mathbb{F}_q^m$.

By a standard preprocessing, we may assume $1 \leq k \leq m$ and that m is sufficiently large compared with the fixed field size q. Indeed, if $k > m$, the input is automatically a YES instance, and if m is bounded by a constant depending only on q, the instance can be solved exactly by brute-force search. In these exceptional cases we output a fixed YES or NO instance of γ'-GapMDP$_q$ accordingly.

We first describe the reduction. Set $d := \gamma k$, $\alpha := 1 - 1/(2q)$, and $k' := k + \alpha d = (4q-1)k$. By Theorem 28, in randomized polynomial time on input (m, k) we obtain, with probability at least 0.99, a $(q, \alpha, d, N, m', n')$-locally dense code $(\mathbf{A}, \boldsymbol{s})$, where $m', n' \leq \operatorname{poly}(m)$ and $N = (qm)^{2d}/100$. Moreover, Theorem 28 guarantees that $\lambda(\mathcal{C}(\mathbf{A})) > d$ with probability 1. Define

$$\mathcal{S} := (\mathcal{C}(\mathbf{A}) - \boldsymbol{s}) \cap B_{q,m'}(\alpha d).$$

Then, with probability at least 0.99, we have $|\mathcal{S}| \geq (qm)^{2d}/100$. Next define

$$\widehat{m} := \min \left\{ q^r - 1 : q^r - 1 \geq \max\{m, d+1\} \right\}.$$

By Theorem 27 applied with block length $\widehat{m}$ and distance parameter $d+1$, there is a q-ary BCH code of length $\widehat{m}$ and minimum distance at least $d+1$ whose co-dimension h satisfies

$$h \leq \lceil d(1-1/q) \rceil \log_q(\widehat{m}+1) = d(1-1/q) \log_q(\widehat{m}+1).$$

The equality holds because $d(1-1/q) = 4(q-1)k$ is an integer. Let $\mathbf{H}_P \in \mathbb{F}_q^{h \times \widehat{m}}$ be a parity-check matrix of this BCH code. Let $\mathbf{P} \in \mathbb{F}_q^{h \times m}$ be the matrix consisting of the first m columns of $\mathbf{H}_P$. Then every nonzero vector $\boldsymbol{u} \in \mathbb{F}_q^m$ with $\|\boldsymbol{u}\|_0 \leq d$ satisfies $\mathbf{P}\boldsymbol{u} \neq 0$. Indeed, if $\mathbf{P}\boldsymbol{u} = 0$, then the vector obtained from $\boldsymbol{u}$ by padding $\widehat{m} - m$ zeros would be a nonzero codeword of the BCH code checked by $\mathbf{H}_P$ of ℓ_0-norm at most d, contradicting its minimum distance at least $d+1$. Define the linear map

$$\mathbf{E} : \mathbb{F}_q^h \to \mathbb{F}_q^{(d+1)h}$$

by

$$\mathbf{E}(a_1, \ldots, a_h) := (a_1 \mathbf{1}_{d+1}, \ldots, a_h \mathbf{1}_{d+1}),$$

where $\mathbf{1}_{d+1}$ is the all-ones vector of length $d+1$. Then every nonzero $\boldsymbol{a} \in \mathbb{F}_q^h$ satisfies $\|\mathbf{E}\boldsymbol{a}\|_0 \geq d+1$. Finally, sample $\mathbf{R} \in \mathbb{F}_q^{h \times m'}$ uniformly at random, and output the code generated by

$$\mathbf{G}' := \begin{pmatrix} \mathbf{G} & \mathbf{0} & -\boldsymbol{t} \\ \mathbf{0} & \mathbf{A} & -\boldsymbol{s} \\ \mathbf{EPG} & \mathbf{ERA} & -\mathbf{E}(\mathbf{P}\boldsymbol{t} + \mathbf{R}\boldsymbol{s}) \end{pmatrix}$$

together with the parameter k'. Equivalently, for every $(\boldsymbol{x}, \boldsymbol{y}, \beta) \in \mathbb{F}_q^{n+n'+1}$, the corresponding codeword is $\boldsymbol{c}(\boldsymbol{x}, \boldsymbol{y}, \beta) = \big(\boldsymbol{u}, \boldsymbol{w}, \mathbf{E}(\mathbf{P}\boldsymbol{u} + \mathbf{R}\boldsymbol{w})\big)$, where $\boldsymbol{u} := \mathbf{G}\boldsymbol{x} - \beta\boldsymbol{t}$ and $\boldsymbol{w} := \mathbf{A}\boldsymbol{y} - \beta\boldsymbol{s}$.

We now verify that this is an FPT reduction. By Theorem 28, we have $m', n' \leq \mathrm{poly}(m)$. Also $\widehat{m} \leq q(\max\{m, d+1\} + 1) = O_q(m)$ because $k \leq m$ and hence $d = 4qk \leq 4qm$. Therefore $h = O_q(k \log m)$, the output length is polynomial in the input size, and the output parameter is $k' = (4q-1)k$. Hence the reduction runs in time $f(k) \cdot \mathrm{poly}(|\mathbf{G}| + |\boldsymbol{t}|)$ and maps k to $O(k)$.

It remains to prove completeness and soundness.

Completeness. Assume that $(\mathbf{G}, \boldsymbol{t}, k)$ is a YES instance of $4q$-GapNCP$_q$. Then there exists $\boldsymbol{x}' \in \mathbb{F}_q^n$ such that $\|\mathbf{G}\boldsymbol{x}' - \boldsymbol{t}\|_0 \leq k$. Let $\boldsymbol{u}' := \mathbf{G}\boldsymbol{x}' - \boldsymbol{t}$ and $\boldsymbol{a} := -\mathbf{P}\boldsymbol{u}' \in \mathbb{F}_q^h$. Condition on the event that $(\mathbf{A}, \boldsymbol{s})$ is locally dense, equivalently that $|\mathcal{S}| \geq (qm)^{2d}/100$. This event has probability at least 0.99.

Choose a subset $\mathcal{T} \subseteq \mathcal{S} \setminus \{\mathbf{0}\}$ containing exactly one representative from each one-dimensional subspace that intersects $\mathcal{S} \setminus \{\mathbf{0}\}$ nontrivially. Then distinct elements of $\mathcal{T}$ are pairwise linearly independent. Moreover, on the event under consideration, $|\mathcal{S}| \geq (qm)^{2d}/100 \geq 2$, where the last inequality follows from the preprocessing. Hence

$$|\mathcal{T}| \geq \frac{|\mathcal{S}| - 1}{q - 1} \geq \frac{|\mathcal{S}|}{2q} \geq \frac{(qm)^{2d}}{200q}.$$

By Lemma 26, the probability that no $\boldsymbol{w} \in \mathcal{T}$ satisfies $\mathbf{R}\boldsymbol{w} = \boldsymbol{a}$ is at most $q^h/|\mathcal{T}|$. The BCH codimension bound gives

$$q^h \leq (\widehat{m} + 1)^{d(1-1/q)} \leq \big(q(4q+3)m\big)^d,$$

and our preprocessing ensures

$$\frac{q^h}{|\mathcal{T}|} \leq 200q \left(\frac{4q+3}{qm}\right)^d \leq 0.01.$$

Hence, conditioned on the event that $(\mathbf{A}, \boldsymbol{s})$ is locally dense, with probability at least 0.99 over $\mathbf{R}$ there exists $\boldsymbol{w} \in \mathcal{T} \subseteq \mathcal{S} \setminus \{\mathbf{0}\}$ such that $\mathbf{R}\boldsymbol{w} = -\mathbf{P}\boldsymbol{u}'$.

Fix such a $\boldsymbol{w}$. Since $\boldsymbol{w} \in \mathcal{S} \subseteq \mathcal{C}(\mathbf{A}) - \boldsymbol{s}$, there exists $\boldsymbol{y} \in \mathbb{F}_q^{n'}$ such that $\boldsymbol{w} = \mathbf{A}\boldsymbol{y} - \boldsymbol{s}$ and $\|\boldsymbol{w}\|_0 \leq \alpha d$. Then $\mathbf{P}\boldsymbol{u}' + \mathbf{R}\boldsymbol{w} = 0$, and therefore $\boldsymbol{c}(\boldsymbol{x}', \boldsymbol{y}, 1) = (\boldsymbol{u}', \boldsymbol{w}, 0)$. It follows that

$$\|\boldsymbol{c}(\boldsymbol{x}', \boldsymbol{y}, 1)\|_0 \leq \|\boldsymbol{u}'\|_0 + \|\boldsymbol{w}\|_0 \leq k + \alpha d = k'.$$

Thus the output instance is a YES instance of γ'-GapMDP$_q$.

Since the event that $(\mathbf{A}, \boldsymbol{s})$ is locally dense has probability at least 0.99 and, conditioned on that event, the probability over $\mathbf{R}$ that some $\boldsymbol{w} \in \mathcal{T}$ satisfies $\mathbf{R}\boldsymbol{w} = -\mathbf{P}\boldsymbol{u}'$ is at least 0.99, we conclude that

$$\Pr[\text{output is a YES instance of } \gamma'\text{-GapMDP}_q] \geq 0.99 \cdot 0.99 > 2/3.$$

Soundness. Assume that $(\mathbf{G}, \boldsymbol{t}, k)$ is a NO instance of $4q$-GapNCP$_q$. We show that for every realization of $(\mathbf{A}, \boldsymbol{s})$ produced above and every choice of $\mathbf{R}$, the output is a NO instance of γ'-GapMDP$_q$.

Let $\boldsymbol{c} = \boldsymbol{c}(\boldsymbol{x}, \boldsymbol{y}, \beta) \in \mathcal{C}(\mathbf{G}') \setminus \{0\}$ be an arbitrary nonzero codeword. Suppose toward a contradiction that $\|\boldsymbol{c}\|_0 \le d$. Writing $\boldsymbol{c} = \big(\boldsymbol{u}, \boldsymbol{w}, \mathbf{E}(\mathbf{P}\boldsymbol{u} + \mathbf{R}\boldsymbol{w})\big)$, where $\boldsymbol{u} = \mathbf{G}\boldsymbol{x} - \beta\boldsymbol{t}$ and $\boldsymbol{w} = \mathbf{A}\boldsymbol{y} - \beta\boldsymbol{s}$, we get $\|\boldsymbol{u}\|_0 + \|\boldsymbol{w}\|_0 \le d$.

We first show that $\beta = 0$. If $\beta \neq 0$, then by the NO promise for $4q$-GapNCP$_q$, $\|\boldsymbol{u}\|_0 = \|\mathbf{G}\boldsymbol{x} - \beta\boldsymbol{t}\|_0 > 4qk = d$, contradicting $\|\boldsymbol{u}\|_0 + \|\boldsymbol{w}\|_0 \le d$.

Thus $\beta = 0$. We next show that $\boldsymbol{w} = 0$. If $\boldsymbol{w} \neq 0$, then $\boldsymbol{w} = \mathbf{A}\boldsymbol{y}$ is a nonzero codeword of $\mathcal{C}(\mathbf{A})$, and hence $\|\boldsymbol{w}\|_0 \ge \lambda(\mathcal{C}(\mathbf{A})) > d$, again contradicting $\|\boldsymbol{u}\|_0 + \|\boldsymbol{w}\|_0 \le d$.

Therefore $\beta = 0$ and $\boldsymbol{w} = 0$, so $\boldsymbol{c} = \big(\boldsymbol{u}, 0, \mathbf{E}(\mathbf{P}\boldsymbol{u})\big)$ with $\boldsymbol{u} = \mathbf{G}\boldsymbol{x}$. Since $\boldsymbol{c} \neq 0$, we must have $\boldsymbol{u} \neq 0$. Also $\|\boldsymbol{u}\|_0 \le d$, so by the defining property of $\mathbf{P}$, $\mathbf{P}\boldsymbol{u} \neq 0$. Hence $\|\mathbf{E}(\mathbf{P}\boldsymbol{u})\|_0 \ge d + 1$, which implies $\|\boldsymbol{c}\|_0 \ge d + 1$, contradicting $\|\boldsymbol{c}\|_0 \le d$. This contradiction proves that every nonzero codeword of $\mathcal{C}(\mathbf{G}')$ has ℓ_0-norm strictly larger than d. Therefore $\lambda(\mathcal{C}(\mathbf{G}')) > d$.

Finally, since $d = \gamma' k'$, we obtain $\lambda(\mathcal{C}(\mathbf{G}')) > \gamma' k'$, so the output is a NO instance of γ'-GapMDP$_q$. This holds for every realization of $(\mathbf{A}, \boldsymbol{s})$ and every choice of $\mathbf{R}$, and thus the reduction has one-sided error. ◀

To amplify to an arbitrary approximation constant factor, we use the following well-known fact.

▶ **Fact 30.** *For any two linear codes $\mathcal{C}(\mathbf{G}_1)$ and $\mathcal{C}(\mathbf{G}_2)$ with $\mathbf{G}_1 \in \mathbb{F}_q^{m_1 \times n_1}$, $\mathbf{G}_2 \in \mathbb{F}_q^{m_2 \times n_2}$, and minimum distances $\lambda(\mathcal{C}(\mathbf{G}_1)) = d_1$, $\lambda(\mathcal{C}(\mathbf{G}_2)) = d_2$, we have*

$$\lambda(\mathcal{C}(\mathbf{G}_1 \otimes \mathbf{G}_2)) = d_1 \cdot d_2,$$

where $\mathbf{G}_1 \otimes \mathbf{G}_2 \in \mathbb{F}_q^{m_1 m_2 \times n_1 n_2}$ is the Kronecker product of $\mathbf{G}_1$ and $\mathbf{G}_2$.

By combining the above claims, we obtain the desired proof.

Proof of Theorem 1. By Theorems 13 and 29, the problem

$$\gamma_0\text{-GapMDP}_q \qquad \text{with} \qquad \gamma_0 := \frac{4q}{4q-1} > 1$$

is W[1]-hard under randomized FPT many-one reductions with one-sided error.

Fix an integer $c \ge 1$. Given an instance $(\mathbf{G}, k)$ of γ_0-GapMDP$_q$, map it to $(\mathbf{G}^{\otimes c}, k^c)$, where $\mathbf{G}^{\otimes c}$ denotes the c-fold Kronecker product of $\mathbf{G}$ with itself. By Fact 30, $\lambda(\mathcal{C}(\mathbf{G}^{\otimes c})) = \lambda(\mathcal{C}(\mathbf{G}))^c$. Hence, if $(\mathbf{G}, k)$ is a YES instance, then

$$\lambda(\mathcal{C}(\mathbf{G}^{\otimes c})) \le k^c,$$

so $(\mathbf{G}^{\otimes c}, k^c)$ is a YES instance of γ_0^c-GapMDP$_q$. If $(\mathbf{G}, k)$ is a NO instance, then

$$\lambda(\mathcal{C}(\mathbf{G}^{\otimes c})) > (\gamma_0 k)^c = \gamma_0^c k^c,$$

so $(\mathbf{G}^{\otimes c}, k^c)$ is a NO instance of γ_0^c-GapMDP$_q$. Because c is a constant, this is a deterministic FPT many-one reduction. Therefore, for every integer $c \ge 1$, the problem γ_0^c-GapMDP$_q$ is W[1]-hard under randomized FPT many-one reductions with one-sided error.

Now let $\gamma \ge 1$ be arbitrary. Choose c so that $\gamma_0^c \ge \gamma$. Every YES instance of γ_0^c-GapMDP$_q$ is also a YES instance of γ-GapMDP$_q$, and every NO instance of γ_0^c-GapMDP$_q$ is also a NO instance of γ-GapMDP$_q$. Hence the identity map is a deterministic FPT many-one reduction from γ_0^c-GapMDP$_q$ to γ-GapMDP$_q$. Therefore γ-GapMDP$_q$ is W[1]-hard under randomized FPT many-one reductions with one-sided error. ◀

3.2 W[1]-hardness of γ-GapSVP$_p$ with One-Sided Error

In this section, we prove a randomized FPT reduction with one-sided error from CVP to SVP using ideas similar to those for the hardness of MDP.

▶ **Lemma 31** (Reed–Solomon codes, [36]). *Let q be a prime and let m, r be integers with $1 \le r \le m < q$. Then one can construct in time* $\mathrm{poly(m, \log q)}$ *a matrix $\mathbf{P} \in \mathbb{F}_q^{r\times m}$ such that every nonzero vector $\boldsymbol{u} \in \mathbb{F}_q^m$ with $\|\boldsymbol{u}\|_0 \le r$ satisfies $\mathbf{P}\boldsymbol{u} \neq 0$.*

Proof. Take the standard $r \times m$ Vandermonde parity-check matrix of a Reed–Solomon code over $\mathbb{F}_q$. Any set of at most r columns is linearly independent, so no nonzero vector of Hamming weight at most r lies in its kernel. This construction is deterministic and polynomial time. ◀

The following theorem gives a randomized algorithm for constructing locally dense lattices based on Reed–Solomon codes.

▶ **Theorem 32** ([7, Theorem 4.3]). *Fix real numbers $p \ge 1$ and $\gamma' \in [1, 2^{1/p})$. Let*

$$\varepsilon = (\gamma')^{-p} - \frac{1}{2} > 0,\ \gamma = \left\lceil \max\left(\frac{12}{\varepsilon}, \frac{1}{(1+\varepsilon/2)^{1/p}-1}\right)\right\rceil,\ \alpha = \left(\frac{1}{(\gamma')^p} - \frac{2}{\gamma^p}\right)^{1/p}.$$

Then there exists a randomized algorithm which, on input positive integers m and d, runs in time poly(m, d) and outputs with probability at least 0.99 a $(p, \alpha, \gamma d, N, m', n')$-locally dense lattice $(\mathbf{A}, \boldsymbol{s})$, where

$$m', n' \le \mathit{poly}(m, d),\ N = (2m(1+\gamma d))^{3(\gamma d)^p},$$

provided that m is sufficiently large compared to p. Moreover, $\lambda_1^{(p)}(\mathcal{L}(\mathbf{A})) > \gamma d$ with probability 1.

As in the case of MDP, by using a random matrix and the parity-check matrix of a Reed–Solomon code, we obtain a randomized FPT reduction with one-sided error.

▶ **Theorem 33.** *Fix a real number $p \ge 1$ and a rational constant $\gamma' \in [1, 2^{1/p})$. Define*

$$\varepsilon = (\gamma')^{-p} - \frac{1}{2} > 0 \ \text{ and } \ \gamma = \left\lceil \max\left(\frac{12}{\varepsilon}, \frac{1}{(1+\varepsilon/2)^{1/p}-1}\right)\right\rceil.$$

Then there exists a randomized FPT *many-one reduction with one-sided error from γ-*GapCVP$_p$ *to γ'-*GapSVP$_p$.

Proof. Let $(\mathbf{B}, \boldsymbol{t}, d)$ be an instance of γ-GapCVP$_p$ with $\mathbf{B} \in \mathbb{Z}^{m\times n}$, $\boldsymbol{t} \in \mathbb{Z}^m$, and $d \in \mathbb{Z}_{>0}$.

By padding $\mathbf{B}$ and $\boldsymbol{t}$ with zero rows, if necessary, we may assume that m is sufficiently large compared with p, so that Theorem 32 applies. This padding preserves $\mathrm{dist}_p(\mathcal{L}(\mathbf{B}), a\boldsymbol{t})$ for every $a \in \mathbb{Z}$ and leaves the parameter d unchanged.

Write $\gamma' = s_0/t_0$ in lowest terms with $s_0, t_0 \in \mathbb{Z}_{>0}$. Set

$$\alpha := \left(\frac{1}{(\gamma')^p} - \frac{2}{\gamma^p}\right)^{1/p},\ r := \min\{m, \lceil(\gamma d)^p\rceil\},\ L := s_0,\ d' := \gamma t_0 d = L\frac{\gamma}{\gamma'}d \in \mathbb{Z}_{>0}.$$

By Theorem 32, in randomized time $\mathrm{poly}(m, d)$ on input (m, d) we obtain, with probability at least 0.99, a $(p, \alpha, \gamma d, N, m', n')$-locally dense lattice $(\mathbf{A}, \boldsymbol{s})$, where

$$N = (2m(1+\gamma d))^{3(\gamma d)^p},\ m', n' \le \mathrm{poly}(m, d), \ \text{ and } \ \lambda_1^{(p)}(\mathcal{L}(\mathbf{A})) > \gamma d.$$

Next, choose a prime q satisfying

$$2\max\{m, \gamma d\} < q \leq 4\max\{m, \gamma d\}.$$

By Bertrand's postulate and primality testing, such a prime can be found deterministically in time $\mathrm{poly}(m, d)$. If $\lceil (\gamma d)^p \rceil \geq m$, let $\mathbf{P} := I_m \in \mathbb{F}_q^{m \times m}$. Otherwise, apply Lemma 31 with parameters (q, m, r) to obtain $\mathbf{P} \in \mathbb{F}_q^{r \times m}$ such that every nonzero vector $\boldsymbol{u} \in \mathbb{F}_q^m$ with $\|\boldsymbol{u}\|_0 \leq r$ satisfies $\mathbf{P}\boldsymbol{u} \neq 0$. Let $\widehat{\mathbf{P}} \in \mathbb{Z}^{r \times m}$ be the canonical integer lift of $\mathbf{P}$ whose entries lie in $\{0, 1, \ldots, q-1\}$. Define the reduction modulo q maps

$$\pi_m : \mathbb{Z}^m \to \mathbb{F}_q^m, \qquad \pi_m(\boldsymbol{u}) = \boldsymbol{u} \bmod q,$$
$$\pi_{m'} : \mathbb{Z}^{m'} \to \mathbb{F}_q^{m'}, \qquad \pi_{m'}(\boldsymbol{w}) = \boldsymbol{w} \bmod q.$$

Observe that every nonzero $\boldsymbol{u} \in \mathbb{Z}^m$ with $\|\boldsymbol{u}\|_p \leq \gamma d$ satisfies $\mathbf{P}\pi_m(\boldsymbol{u}) \neq 0$. Indeed, $|u_i| \leq \|\boldsymbol{u}\|_p \leq \gamma d < q/2$ for every coordinate, so $\pi_m(\boldsymbol{u}) \neq 0$. Moreover,

$$\|\pi_m(\boldsymbol{u})\|_0 \leq \|\boldsymbol{u}\|_0 \leq \|\boldsymbol{u}\|_p^p \leq (\gamma d)^p \leq r$$

if $r < m$, while if $r = m$ then $\mathbf{P} = I_m$ and the claim is immediate. Now sample $\mathbf{R} \in \mathbb{F}_q^{r \times m'}$ uniformly at random, let $\widehat{\mathbf{R}} \in \mathbb{Z}^{r \times m'}$ be its canonical integer lift. More precisely, $\mathbf{R}$ is obtained by sampling the entries independently and uniformly at random from $\mathbb{F}_q$. Define the lattice basis

$$\mathbf{B}' := \begin{pmatrix} \mathbf{B} & \mathbf{0}_{m \times n'} & -\boldsymbol{t} & \mathbf{0}_{m \times r} \\ \mathbf{0}_{m' \times n} & \mathbf{A} & -\boldsymbol{s} & \mathbf{0}_{m' \times r} \\ \mathbf{0}_{1 \times n} & \mathbf{0}_{1 \times n'} & 1 & \mathbf{0}_{1 \times r} \\ \beta\widehat{\mathbf{P}}\mathbf{B} & \beta\widehat{\mathbf{R}}\mathbf{A} & -\beta(\widehat{\mathbf{P}}\boldsymbol{t} + \widehat{\mathbf{R}}\boldsymbol{s}) & \beta q \mathbf{I}_r \end{pmatrix}, \qquad \beta := \gamma d + 1.$$

And set $\widehat{\mathbf{B}} := L\mathbf{B}'$. Output the lattice basis $\widehat{\mathbf{B}}$ together with the threshold d'. Equivalently, for every $(\boldsymbol{x}, \boldsymbol{y}, a, \boldsymbol{z}) \in \mathbb{Z}^{n+n'+1+r}$, the corresponding lattice vector is

$$\boldsymbol{c}(\boldsymbol{x}, \boldsymbol{y}, a, \boldsymbol{z}) = \big(\boldsymbol{u}, \boldsymbol{w}, a, \beta(\widehat{\mathbf{P}}\boldsymbol{u} + \widehat{\mathbf{R}}\boldsymbol{w} + q\boldsymbol{z})\big),$$

where $\boldsymbol{u} := \mathbf{B}\boldsymbol{x} - a\boldsymbol{t}$ and $\boldsymbol{w} := \mathbf{A}\boldsymbol{y} - a\boldsymbol{s}$. This is the output instance of γ'-GapSVP$_p$.

We now verify that this is an FPT reduction. Since $m', n' \leq \mathrm{poly}(m, d)$ and $r \leq \lceil (\gamma d)^p \rceil$, the output basis has size polynomial in the input size, and the output parameter is $d' = \gamma t_0 d = O(d)$, because γ and t_0 are constants depending only on the fixed target factor γ'. Hence the reduction runs in time $f(d) \cdot \mathrm{poly}(|\mathbf{B}| + |\boldsymbol{t}|)$ and maps d to $O(d)$.

It remains to prove completeness and soundness.

Completeness. Assume that $(\mathbf{B}, \boldsymbol{t}, d)$ is a YES instance of γ-GapCVP$_p$. Then there exists $\boldsymbol{x}' \in \mathbb{Z}^n$ such that $\|\mathbf{B}\boldsymbol{x}' - \boldsymbol{t}\|_p \leq d$. Let

$$\boldsymbol{u}' := \mathbf{B}\boldsymbol{x}' - \boldsymbol{t}, \qquad \boldsymbol{a} := -\mathbf{P}\pi_m(\boldsymbol{u}') \in \mathbb{F}_q^r.$$

Define

$$\mathcal{W}_s := (\mathcal{L}(\mathbf{A}) - \boldsymbol{s}) \cap \mathcal{B}_p^{m'}(\alpha\gamma d).$$

Then, with probability at least 0.99, we have $|\mathcal{W}_s| \geq N$. Because every $\boldsymbol{w} \in \mathcal{W}_s$ has $\|\boldsymbol{w}\|_p \leq \alpha\gamma d < q/2$, the map $\pi_{m'}$ is injective on $\mathcal{W}_s$, and $\pi_{m'}(\boldsymbol{w}) \neq 0$ whenever $\boldsymbol{w} \neq 0$.

Choose $\mathcal{T} \subseteq \mathcal{W}_s \setminus \{\mathbf{0}\}$ so that $\pi_{m'}(\mathcal{T})$ contains exactly one representative from each one-dimensional subspace of $\mathbb{F}_q^{m'}$ that intersects $\pi_{m'}(\mathcal{W}_s \setminus \{\mathbf{0}\})$. Then $\pi_{m'}(\mathcal{T})$ is pairwise linearly independent and, since $|\mathcal{W}_s| \geq N$ and $N \geq q$,

$$|\mathcal{T}| \geq \frac{|\mathcal{W}_s| - 1}{q - 1} \geq \frac{N}{q}.$$

By Lemma 26, the probability that no $\boldsymbol{w} \in \mathcal{T}$ satisfies

$$\mathbf{R}\pi_{m'}(\boldsymbol{w}) = -\mathbf{P}\pi_m(\boldsymbol{u}') \tag{1}$$

is at most $q^r/|\mathcal{T}| \leq q^{r+1}/N$. With $M := 2m(1 + \gamma d)$, the choices of q, r, N give

$$\frac{q^{r+1}}{N} \leq \frac{(2M)^{(\gamma d)^p + 2}}{M^{3(\gamma d)^p}} < 0.01.$$

Thus, conditioned on the locally dense lattice event, with probability at least 0.99 over $\mathbf{R}$ there exists $\boldsymbol{w} \in \mathcal{T} \subseteq \mathcal{W}_s$ satisfying Equation (1).

Fix such a vector $\boldsymbol{w}$. Since $\boldsymbol{w} \in \mathcal{W}_s \subseteq \mathcal{L}(\mathbf{A}) - \boldsymbol{s}$, there exists $\boldsymbol{y} \in \mathbb{Z}^{n'}$ such that $\boldsymbol{w} = \mathbf{A}\boldsymbol{y} - \boldsymbol{s}$ and $\|\boldsymbol{w}\|_p \leq \alpha\gamma d$. Since $\widehat{\mathbf{P}}\boldsymbol{u}' + \widehat{\mathbf{R}}\boldsymbol{w} = 0 \pmod q$, this implies that there exists $\boldsymbol{z} \in \mathbb{Z}^r$ such that

$$\widehat{\mathbf{P}}\boldsymbol{u}' + \widehat{\mathbf{R}}\boldsymbol{w} + q\boldsymbol{z} = 0.$$

Hence $\boldsymbol{c}(\boldsymbol{x}', \boldsymbol{y}, 1, \boldsymbol{z}) = (\boldsymbol{u}', \boldsymbol{w}, 1, \mathbf{0}_r)$. Its ℓ_p norm satisfies

$$\begin{aligned}
\|\boldsymbol{c}(\boldsymbol{x}', \boldsymbol{y}, 1, \boldsymbol{z})\|_p^p &= \|\boldsymbol{u}'\|_p^p + \|\boldsymbol{w}\|_p^p + 1 \\
&\leq d^p + (\alpha\gamma d)^p + 1 \\
&\leq 2d^p + \alpha^p\gamma^p d^p \\
&= (2 + \alpha^p\gamma^p)\, d^p \\
&= \left(\frac{\gamma}{\gamma'}\right)^p d^p,
\end{aligned}$$

where the last equality uses the definition of α. Hence

$$\|\boldsymbol{c}(\boldsymbol{x}', \boldsymbol{y}, 1, \boldsymbol{z})\|_p \leq \frac{\gamma}{\gamma'} d.$$

Therefore the nonzero vector $L\boldsymbol{c}(\boldsymbol{x}', \boldsymbol{y}, 1, \boldsymbol{z}) \in \mathcal{L}(\widehat{\mathbf{B}})$ satisfies

$$\|L\boldsymbol{c}(\boldsymbol{x}', \boldsymbol{y}, 1, \boldsymbol{z})\|_p \leq L\frac{\gamma}{\gamma'} d = d'.$$

Thus the output instance is a YES instance of γ'-GapSVP$_p$. Since the event that $(\mathbf{A}, \boldsymbol{s})$ is $(p, \alpha, \gamma d, N, m', n')$-locally dense lattice has probability at least 0.99 and, conditioned on that event, the probability over $\mathbf{R}$ that some $\boldsymbol{w} \in \mathcal{W}_s$ satisfies the congruence in Equation (1) is at least 0.99, we conclude that

$$\Pr[\text{output is a YES instance of } \gamma'\text{-GapSVP}_p] \geq 0.99 \cdot 0.99 > \frac{2}{3}.$$

Soundness. Assume that $(\mathbf{B}, \boldsymbol{t}, d)$ is a NO instance of γ-GapCVP$_p$. We first show that, regardless of the choice of $\mathbf{R}$, every nonzero vector of $\mathcal{L}(\mathbf{B}')$ has ℓ_p norm strictly larger than γd. Let $\boldsymbol{c} = \boldsymbol{c}(\boldsymbol{x}, \boldsymbol{y}, a, \boldsymbol{z}) \in \mathcal{L}(\mathbf{B}') \setminus \{0\}$ be an arbitrary nonzero lattice vector. Suppose toward a contradiction that $\|\boldsymbol{c}\|_p \le \gamma d$. Writing

$$\boldsymbol{c} = \big(\boldsymbol{u}, \boldsymbol{w}, a, \beta(\widehat{\mathbf{P}}\boldsymbol{u} + \widehat{\mathbf{R}}\boldsymbol{w} + q\boldsymbol{z})\big),$$

where $\boldsymbol{u} = \mathbf{B}\boldsymbol{x} - a\boldsymbol{t}$ and $\boldsymbol{w} = \mathbf{A}\boldsymbol{y} - a\boldsymbol{s}$, we get

$$\|\boldsymbol{u}\|_p^p + \|\boldsymbol{w}\|_p^p + |a|^p \le (\gamma d)^p.$$

In particular, if $a \neq 0$, then by the NO promise for γ-GapCVP$_p$,

$$\|\boldsymbol{u}\|_p = \|\mathbf{B}\boldsymbol{x} - a\boldsymbol{t}\|_p > \gamma d,$$

a contradiction. Hence $a = 0$. If now $\boldsymbol{w} \neq 0$, then because $\lambda_1^{(p)}(\mathcal{L}(\mathbf{A})) > \gamma d$, we get $\|\boldsymbol{w}\|_p > \gamma d$, again a contradiction. Therefore $a = 0$ and $\boldsymbol{w} = 0$. So every short vector must be of the form

$$\boldsymbol{c}(\boldsymbol{x}, \boldsymbol{y}, a, \boldsymbol{z}) = (\boldsymbol{u}, 0, 0, \beta(\widehat{\mathbf{P}}\boldsymbol{u} + q\boldsymbol{z})).$$

If $\boldsymbol{u} = 0$, then since $\boldsymbol{c} \neq 0$, $\boldsymbol{z} \neq 0$. Hence

$$\|\boldsymbol{c}(\boldsymbol{x}, \boldsymbol{y}, a, \boldsymbol{z})\|_p \ge \beta q > \gamma d,$$

a contradiction. So we may assume $\boldsymbol{u} \neq 0$. Since $\|\boldsymbol{u}\|_p \le \gamma d$, property of $\mathbf{P}$ implies $\mathbf{P}\pi_m(\boldsymbol{u}) \neq 0$. Equivalently,

$$\widehat{\mathbf{P}}\boldsymbol{u} + q\boldsymbol{z} \neq 0 \qquad \text{for every } \boldsymbol{z} \in \mathbb{Z}^r.$$

Therefore the last block of $\boldsymbol{c}(\boldsymbol{x}, \boldsymbol{y}, a, \boldsymbol{z})$ is nonzero, so

$$\|\boldsymbol{c}(\boldsymbol{x}, \boldsymbol{y}, a, \boldsymbol{z})\|_p \ge \beta > \gamma d,$$

a contradiction. We conclude that every nonzero vector of $\mathcal{L}(\mathbf{B}')$ has ℓ_p norm strictly larger than γd. Since $\mathcal{L}(\widehat{\mathbf{B}}) = L\mathcal{L}(\mathbf{B}')$, every nonzero vector of $\mathcal{L}(\widehat{\mathbf{B}})$ has ℓ_p norm strictly larger than $L\gamma d = \gamma' d'$. Therefore the output is a NO instance of γ'-GapSVP$_p$. This holds for every pair $(\mathbf{A}, \boldsymbol{s})$ from Theorem 32 and every choice of $\mathbf{R}$, and thus the reduction has one-sided error. ◀

From the above, we immediately obtain Theorem 2.

Proof of Theorem 2. Let $\gamma \in [1, 2^{1/p})$ be the target approximation factor. Choose any rational number η such that $\gamma < \eta < 2^{1/p}$. By Theorems 17 and 33, the problem η-GapSVP$_p$ is W[1]-hard under randomized FPT many-one reductions with one-sided error.

Now observe that every YES instance of η-GapSVP$_p$ is also a YES instance of γ-GapSVP$_p$, and every NO instance of η-GapSVP$_p$ is also a NO instance of γ-GapSVP$_p$, because $\eta > \gamma$. Hence any algorithm for γ-GapSVP$_p$ would also solve η-GapSVP$_p$ on the same input.

Therefore γ-GapSVP$_p$ is W[1]-hard under randomized FPT many-one reductions with one-sided error. ◀

4 Deterministic Hardness under the Circuit Lower Bound

In this section, we describe the derandomization principle used later. The proof is the same in the ordinary and parameterized settings: enumerate a small hitting set of random tapes, run the randomized reduction with one-sided error on all of them, and combine the outputs by an OR function.

▶ **Theorem 34.** *Assume that there exists an $\varepsilon > 0$ such that*

$$\mathsf{E} \not\subseteq i.o.\text{-NSIZE}(2^{\varepsilon n}).$$

Let Π and Π' be promise problems. Suppose that
1. *Π is NP-hard under deterministic polynomial-time many-one reductions;*
2. *$\Pi'_{\mathrm{YES}} \in \mathsf{NP}$;*
3. *Π' has a polynomial-time OR function;*
4. *there exists a randomized many-one reduction with one-sided error from Π to Π'.*

Then Π' is NP-hard under deterministic polynomial-time many-one reductions.

Proof sketch. Let R be the randomized reduction. For a fixed input x, let $\phi_x(r) = 1$ iff $R(x; r) \in \Pi'_{\mathrm{YES}}$. Since $\Pi'_{\mathrm{YES}} \in \mathsf{NP}$, after hardwiring x, the predicate ϕ_x is computable by a polynomial-size nonadaptive SAT-oracle circuit: compute $R(x; r)$, reduce membership in Π'_{YES} to SAT, and ask one oracle query.

On YES inputs, completeness gives $\Pr_r[\phi_x(r) = 1] \geq 2/3$. By Theorem 23, the corresponding hitting set contains a tape r with $\phi_x(r) = 1$, once the combined input-and-randomness length is large enough. For the finitely many smaller lengths, enumerate all random tapes. The deterministic reduction runs R on all tapes in the chosen list and combines the resulting instances by the polynomial-time OR function. Completeness follows because one output is YES. Soundness follows because, on NO inputs, one-sidedness ensures that every tape produces a NO instance. Composing with the deterministic hardness reduction to Π proves the theorem. ◀

▶ **Theorem 35.** *Assume that there exists an $\varepsilon > 0$ such that*

$$\mathsf{E} \not\subseteq i.o.\text{-NSIZE}(2^{\varepsilon n}).$$

Let Π and Π' be parameterized promise problems. Suppose that
1. *Π is $\mathsf{W}[1]$-hard under deterministic FPT many-one reductions;*
2. *Π' has an FPT OR function;*
3. *there exists a randomized FPT many-one reduction with one-sided error $R : \Pi \to \Pi'$;*
4. *R has SAT-circuitizable success predicates.*

Then Π' is $\mathsf{W}[1]$-hard under deterministic FPT many-one reductions.

Proof. Let R be the randomized reduction with one-sided error and let C be an FPT OR function for Π'. By the SAT-circuitizability assumption, there is a polynomial P such that every success predicate

$$\phi_{x,k}(r) = 1 \iff R((x, k); r) \in \Pi'_{\mathrm{YES}}$$

is in $\mathrm{SIZE}^{\mathsf{SAT}}_{\|}(P(m))$, where $m = |\langle x, k\rangle| + \mu$ and μ is the number of random bits used by R. Choose a constant c with $P(m) \leq m^c$ for all sufficiently large m, and take the hitting sets $H_m := \{G_m(\sigma) : \sigma \in \{0,1\}^{a \log m}\}$ from Theorem 23. Increase the threshold m_0 if necessary so that the theorem applies for all $m \geq m_0$.

The deterministic reduction is as follows. On input (x, k), compute $m = |\langle x, k\rangle| + \mu$. If $m < m_0$, list all 2^μ random tapes; this is only a constant-size list because m_0 is fixed. If $m \geq m_0$, enumerate H_m. Run R on (x, k) using each listed tape, and apply the FPT OR function C to all resulting outputs.

The running time is FPT: the hitting set has size $m^{O(1)}$, each call to R takes $T(k)|x|^{O(1)}$ time, and the OR function is called on a tuple whose maximum parameter is bounded by the parameter bound of R. Hence the output parameter is bounded by a computable function of k.

If $(x, k) \in \Pi_{\mathrm{YES}}$, then $\Pr_r[\phi_{x,k}(r) = 1] \geq 2/3$. In the small case, the list contains a successful tape; in the large case, the hitting set hits the accepting set of $\phi_{x,k}$. Thus at least one input to C is a YES instance, and the output is YES. If $(x, k) \in \Pi_{\mathrm{NO}}$, then soundness of R says that every tape gives a NO instance of Π', and the OR function outputs NO. Therefore we have a deterministic FPT many-one reduction from Π to Π', and the claimed hardness follows from item (1). ◀

5 Conditional Hardness of MDP and SVP

We now construct the OR functions needed in Theorems 34 and 35 and apply the derandomization theorem to MDP and SVP.

5.1 OR functions

▶ **Lemma 36.** *Let $q \geq 2$ be a prime power, and let $\gamma \geq 1$ be a constant. Then γ-GapMDP$_q$, parameterized by the distance threshold, has an FPT OR function.*

Proof. Given a tuple of strings, discard all syntactically invalid strings and keep the valid instances $(\mathbf{G}_i, k_i)$. If none remain, output any fixed NO instance. Let $\kappa = \max_i k_i$, $K = \mathrm{lcm}(1, \ldots, \kappa)$, and $c_i = K/k_i$. Let $\widetilde{\mathbf{G}}_i$ be obtained from $\mathbf{G}_i$ by repeating each row c_i times, and output the block-diagonal generator matrix

$$\mathbf{G}_{\mathrm{out}} = \mathrm{diag}(\widetilde{\mathbf{G}}_1, \ldots, \widetilde{\mathbf{G}}_s) \quad \text{with threshold } K.$$

Repeating rows multiplies the minimum distance by c_i, and the minimum distance of a block-diagonal code is the minimum of the block minimum distances. Hence

$$\lambda(\mathcal{C}(\mathbf{G}_{\mathrm{out}})) = \min_i c_i \lambda(\mathcal{C}(\mathbf{G}_i)).$$

Thus a YES input block gives distance at most K, while if all retained inputs are NO then every block has distance larger than γK. The output threshold K depends only on κ, and the construction runs in time $T(\kappa)N^{O(1)}$. This is an FPT OR function. ◀

▶ **Lemma 37.** *Let $p \in [1, \infty)$ and let $\gamma \geq 1$ be a constant. Then γ-GapSVP$_p$ has a polynomial-time OR function.*

Proof. Keep the valid instances $(\mathbf{B}_i, d_i)$ with $d_i \geq 1$, and output a fixed NO instance if none remain. Set $D = \prod_i d_i$, $c_i = D/d_i$, and $\widetilde{\mathbf{B}}_i = c_i \mathbf{B}_i$. Output

$$\mathbf{B}_{\mathrm{out}} = \mathrm{diag}(\widetilde{\mathbf{B}}_1, \ldots, \widetilde{\mathbf{B}}_s) \quad \text{with threshold } D.$$

Scaling a basis by c_i scales $\lambda_1^{(p)}$ by c_i, and a block-diagonal lattice has shortest-vector length equal to the minimum over blocks. Therefore

$$\lambda_1^{(p)}(\mathcal{L}(\mathbf{B}_{\mathrm{out}})) = \min_i c_i \lambda_1^{(p)}(\mathcal{L}(\mathbf{B}_i)).$$

The OR guarantee follows exactly as above. The bit length of D is at most the sum of the bit lengths of the input thresholds, so the construction is polynomial time. ◀

▶ **Lemma 38.** *Let $p \in [1, \infty)$ and let $\gamma \geq 1$ be a constant. Then γ-GapSVP$_p$, parameterized by the threshold, has an FPT OR function.*

Proof. Use the same block-diagonal construction as in Lemma 37, but replace $D = \prod_i d_i$ by $D = \mathrm{lcm}(1, \ldots, \kappa)$, where $\kappa = \max_i d_i$. Then D depends only on the largest input parameter, and the same distance calculation proves the OR guarantee. The construction runs in time $T(\kappa)N^{O(1)}$, and the output parameter is D. ◀

5.2 Applications

We will use the following lemma to verify item (4) in Theorem 35.

▶ **Lemma 39.** *Let R be a randomized* FPT *many-one reduction from Π to Π'. Suppose that, after padding the random tape with ignored bits, its length μ on input (x, k) is at least the running-time bound of R on that input, and set $m = |\langle x, k\rangle| + \mu$. If $\Pi'_{\mathrm{YES}} \in$ NP, then R has SAT-circuitizable success predicates.*

Proof. For fixed (x, k), view the success predicate as a function of $r \in \{0,1\}^m$, where only the first μ bits are used as the random tape. Since the running time, and hence the output length, is at most $\mu \leq m$, compute $R((x, k); r)$ by a polynomial-size circuit. Then compose with a polynomial-time reduction from Π'_{YES} to SAT, and finally make one SAT-oracle query. ◀

Therefore, the desired claims follow.

Proof of Theorem 4. Fix q and γ. We apply Theorem 35 to the randomized reduction with one-sided error underlying Theorem 1; equivalently, the source is the W[1]-hard problem $4q$-GapNCP$_q$ from Theorem 13, followed by the constant number of tensorings needed to reach the target approximation factor. The target γ-GapMDP$_q$ has an FPT OR function by Lemma 36.

The YES language of γ-GapMDP$_q$ is in NP. The concrete reduction can be padded with ignored random bits so that the random tape length is at least its FPT running-time bound. Hence Lemma 39 gives SAT-circuitizable success predicates. All hypotheses of Theorem 35 hold, so γ-GapMDP$_q$ is W[1]-hard under deterministic FPT many-one reductions. ◀

Proof of Theorem 6. Fix $\gamma \geq 1$. By Theorem 15, there is a randomized polynomial-time reduction with one-sided error from an NP-hard language to γ-GapSVP$_2$. The YES language of γ-GapSVP$_2$ is in NP. By Lemma 37, γ-GapSVP$_2$ has a polynomial-time OR function. Therefore Theorem 34 applies and yields deterministic polynomial-time NP-hardness. ◀

Proof of Theorem 5. Fix an integer $p \geq 1$ and $\gamma < 2^{1/p}$. Choose a rational η with $\gamma < \eta < 2^{1/p}$. It is enough to prove deterministic W[1]-hardness of η-GapSVP$_p$, since the identity map reduces η-GapSVP$_p$ to γ-GapSVP$_p$ on promised instances.

By Theorem 2, η-GapSVP$_p$ is W[1]-hard under randomized FPT many-one reductions with one-sided error; specifically, the source is the W[1]-hard Γ-GapCVP$_p$ from Theorem 17, where Γ is the source approximation factor in Theorem 33. The target has an FPT OR function by Lemma 38.

Since p is fixed, the YES language of η-GapSVP$_p$ is in NP. The reduction in Theorem 33 can be padded with ignored random bits so that the random tape length is at least its FPT running-time bound. By Lemma 39, it has SAT-circuitizable success predicates. Applying Theorem 35 gives deterministic FPT hardness of η-GapSVP$_p$, and hence of γ-GapSVP$_p$. ◀

References

1 Divesh Aggarwal, Rishav Gupta, Aditya Morolia, and Chuanqi Zhang. Mind the Gap? Not for SVP Hardness under ETH! In *ICALP*, 2026.

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

3 E. Agrell, T. Eriksson, A. Vardy, and K. Zeger. Closest point search in lattices. *IEEE Transactions on Information Theory*, 48(8):2201–2214, 2002. doi:10.1109/TIT.2002.800499.

4 Miklós Ajtai. The shortest vector problem in L2 is NP-hard for randomized reductions (extended abstract). In *STOC*, 1998.

5 Per Austrin and Subhash Khot. A Simple Deterministic Reduction for the Gap Minimum Distance of Code Problem. *IEEE Transactions on Information Theory*, 60(10):6636–6645, 2014. Preliminary version in ICALP 2011. doi:10.1109/TIT.2014.2340869.

6 Marshall Ball, Elette Boyle, Akshay Degwekar, Apoorvaa Deshpande, Alon Rosen, Vinod Vaikuntanathan, and Prashant Nalini Vasudevan. Cryptography from Information Loss. In *ITCS*, 2020.

7 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.

8 Huck Bennett and Chris Peikert. Hardness of Bounded Distance Decoding on Lattices in ℓ_p Norms. In *CCC*, 2020.

9 Huck Bennett and Chris Peikert. Hardness of the (Approximate) Shortest Vector Problem: A Simple Proof via Reed-Solomon Codes. In *RANDOM/APPROX*, 2023.

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

11 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. *Journal of the ACM*, 68(3), 2021. doi:10.1145/3444942.

12 Richard Chang and Jim Kadin. On Computing Boolean Connectives of Characteristic Functions. *Mathematical Systems Theory*, 28(3):173–198, 1995. doi:10.1007/BF01303054.

13 Qi Cheng and Daqing Wan. A Deterministic Reduction for the Gap Minimum Distance Problem. *IEEE Transactions on Information Theory*, 58(11):6935–6941, 2012. Preliminary version in STOC 2009. doi:10.1109/TIT.2012.2209198.

14 Marek Cygan, Fedor V. Fomin, Lukasz Kowalik, Daniel Lokshtanov, Dániel Marx, Marcin Pilipczuk, Michał Pilipczuk, and Saket Saurabh. *Parameterized Algorithms*. Springer, 2015. doi:10.1007/978-3-319-21275-3.

15 Rodney G. Downey and Michael R. Fellows. Fixed-Parameter Tractability and Completeness I: Basic Results. *SIAM Journal on Computing*, 24(4):873–921, 1995. doi:10.1137/S0097539792228228.

16 Rodney G. Downey and Michael R. Fellows. Fixed-Parameter Tractability and Completeness II: On Completeness for W[1]. *Theoretical Computer Science*, 141(1–2):109–131, 1995. doi:10.1016/0304-3975(94)00097-3.

17 Rodney G. Downey and Michael R. Fellows. *Parameterized Complexity*. Monographs in Computer Science. Springer, 1999. doi:10.1007/978-1-4612-0515-9.

18 Ilya Dumer, Daniele Micciancio, and Madhu Sudan. Hardness of approximating the minimum distance of a linear code. *IEEE Transactions on Information Theory*, 49(1):22–37, 2003. Preliminary version in FOCS 1999. doi:10.1109/TIT.2002.806118.

19 Oded Goldreich. *On promise problems: A survey*, volume 3895 of *Lecture Notes in Computer Science*, pages 254–290. Springer, 2006. doi:10.1007/11685654_12.

20 Oded Goldreich and Shafi Goldwasser. On the Limits of Nonapproximability of Lattice Problems. *Journal of Computer and System Sciences*, 60(3):540–563, 2000. Preliminary version in STOC 1998. doi:10.1006/JCSS.1999.1686.

21 Isaac M Hair and Amit Sahai. Deterministic Hardness of Approximation For SVP in all Finite ℓ_p Norms, 2026. doi:10.48550/arXiv.2604.01451.

22 Isaac M. Hair and Amit Sahai. SVP_p Is Deterministically NP-Hard for All $p > 2$, Even to Approximate within a Factor of $2^{\log^{1-\varepsilon} n}$. In *STOC*, 2026.

23 Ishay Haviv and Oded Regev. Tensor-based Hardness of the Shortest Vector Problem to within Almost Polynomial Factors. *Theory of Computing*, 8(23):513–531, 2012. Preliminary version in STOC 2007. doi:10.4086/TOC.2012.V008A023.

24 Yahli Hecht and Muli Safra. Deterministic Hardness of Approximation of Unique-SVP and GapSVP in ℓ_p Norms for $p > 2$. In *STOC*, 2026.

25 Markus Hittmeir. Fine-grained deterministic hardness of the shortest vector problem, 2026. arXiv:2511.01626.

26 Russell Impagliazzo and Avi Wigderson. P = BPP if E requires exponential circuits: derandomizing the XOR lemma. In *STOC*, 1997.

27 Subhash Khot. Hardness of approximating the shortest vector problem in lattices. *Journal of the ACM*, 52(5):789–808, 2005. Preliminary version in FOCS 2004. doi:10.1145/1089023.1089027.

28 Subhash Khot. Hardness of approximating the Shortest Vector Problem in high ℓ_p norms. *Journal of Computer and System Sciences*, 72(2):206–219, 2006. Preliminary version in FOCS 2003. doi:10.1016/J.JCSS.2005.07.002.

29 Adam R. Klivans and Dieter van Melkebeek. Graph Nonisomorphism Has Subexponential Size Proofs Unless the Polynomial-Time Hierarchy Collapses. *SIAM Journal on Computing*, 31(5):1501–1526, 2002. Preliminary version in STOC 1999. doi:10.1137/S0097539700389652.

30 Shuangle Li, Bingkai Lin, and Yuwei Liu. Improved Lower Bounds for Approximating Parameterized Nearest Codeword and Related Problems Under ETH. In *ICALP*, 2024.

31 Shu Lin and Juane Li. *Fundamentals of Classical and Modern Error-Correcting Codes*. Cambridge University Press, 2021.

32 Daniele Micciancio. The Shortest Vector in a Lattice is Hard to Approximate to within Some Constant. *SIAM Journal on Computing*, 30(6):2008–2035, 2001. Preliminary version in FOCS 1998. doi:10.1137/S0097539700373039.

33 Daniele Micciancio. Inapproximability of the Shortest Vector Problem: Toward a Deterministic Reduction. *Theory of Computing*, 8(22):487–512, 2012. doi:10.4086/TOC.2012.V008A022.

34 Daniele Micciancio. Locally Dense Codes. In *CCC*, 2014.

35 Chris Peikert. A Decade of Lattice Cryptography. *Foundations and Trends® in Theoretical Computer Science*, 10(4):283–424, 2016. doi:10.1561/0400000074.

36 I. S. Reed and G. Solomon. Polynomial Codes Over Certain Finite Fields. *Journal of the Society for Industrial and Applied Mathematics*, 8(2):300–304, 1960.

37 Ronen Shaltiel and Jad Silbak. Explicit Codes for Poly-Size Circuits and Functions that are Hard to Sample on Low Entropy Distributions, 2023. Electronic Colloquium onComputational Complexity (ECCC). URL: https://eccc.weizmann.ac.il/report/2023/149/.

38 Ronen Shaltiel and Christopher Umans. Pseudorandomness for Approximate Counting and Sampling. *Computational Complexity*, 15(4):298–341, 2006. doi:10.1007/S00037-007-0218-9.

39 Peter van Emde Boas. Another NP-complete partition problem and the complexity of computing short vectors in a lattice. *Technical Report, Department of Mathematics, University of Amsterdam*, 1981.

40 Daqing Wan. NP-hardness of SVP in Euclidean Space, 2026. doi:10.48550/arXiv.2603.27398.

41 Violetta Weger, Niklas Gassner, and Joachim Rosenthal. A Survey on Code-Based Cryptography, 2024. arXiv:2201.07119.