

Integer programming on polytopes of Chvátal rank one is as hard as lattice problems

Alberto Del Pia*

October 7, 2026

Abstract

A rational polyhedron has Chvátal rank at most one if a single round of Chvátal–Gomory cuts yields its integer hull. For such polyhedra, integer feasibility is in $\text{NP} \cap \text{coNP}$ by a result of Boyd and Pulleyblank from the early 1980s, so it is unlikely to be NP-hard. Whether it is polynomial has remained open since then. We answer this question negatively, under either of two standard assumptions from lattice-based cryptography. First, a polynomial-time algorithm for this problem would solve bounded distance decoding with polynomial factors in deterministic polynomial time, contradicting a widely believed conjecture. Second, assuming the hardness of learning with errors, an average-case analogue of bounded distance decoding, the problem is also hard on average, for an efficiently samplable distribution of polytopes. Both results rest on an elementary sufficient condition: a polyhedron has Chvátal rank at most one if its width is less than one along every row of some unimodular matrix. For our polytopes, such a matrix exists but is hard to find.

Keywords: Chvátal–Gomory cuts · Chvátal rank · integer programming · promise problems · lattice problems · learning with errors

Mathematics Subject Classification (2020): 90C10 · 90C57 · 90C60 · 68Q17 · 11H06 · 52C07

1 Introduction

Let $P \subseteq \mathbb{R}^n$ be a rational polyhedron and let $P_I = \text{conv}(P \cap \mathbb{Z}^n)$ be its *integer hull*. A *Chvátal–Gomory cut* (CG cut) for P is an inequality $c^\top x \leq \lfloor \delta \rfloor$, where $c \in \mathbb{Z}^n$ and $c^\top x \leq \delta$ is valid for P . The *Chvátal closure* P' of P is the set of points satisfying all CG cuts for P [21, 8]. We have $P_I \subseteq P' \subseteq P$, and P' is again a rational polyhedron [35]. Iterating the closure operation yields P_I after finitely many steps, as shown by Chvátal [8] for polytopes and by Schrijver [35] for rational polyhedra. The *Chvátal rank* of P is the number of steps needed. Polyhedra of Chvátal rank zero are the *integral* polyhedra. Recognizing them is coNP-complete [30], and recognizing polyhedra of Chvátal rank at most one is NP-hard [14, 12].

Deciding whether $P \cap \mathbb{Z}^n \neq \emptyset$, which we call *integer feasibility*, is NP-complete [36, Theorem 18.1]. If P is integral, it is easy: P contains an integer point if and only if $P \neq \emptyset$, which can be decided in polynomial time by linear programming [36, Theorem 13.4]. The next case is Chvátal rank at most one, that is, $P' = P_I$: a single round of CG cuts yields the integer hull. Polyhedra of Chvátal rank at most one include the fractional matching polytope [17], the fractional stable set

*Department of Industrial and Systems Engineering & Wisconsin Institute for Discovery, University of Wisconsin–Madison, Madison, WI, USA. E-mail: delpia@wisc.edu.

polytope of a t -perfect graph [9], the polyhedra defined by matrices with the Edmonds–Johnson property [19, 16], and the standard linearization of binary polynomial optimization problems over kite-free β -acyclic hypergraphs [15].

For polyhedra with $P' = P_I$, integer feasibility is in $\text{NP} \cap \text{coNP}$. An integer point certifies feasibility. If $P \cap \mathbb{Z}^n = \emptyset$, then $P' = \emptyset$, and this is certified by a *refutation*, that is, a set of CG cuts for P of polynomial encoding size with empty intersection. By Helly’s theorem, $n + 1$ cuts suffice. Membership in $\text{NP} \cap \text{coNP}$ is a result of Boyd and Pulleyblank from the early 1980s, which appears in Schrijver’s 1986 book [36, Theorem 23.5 and Corollary 23.5a] and was formally published only in 2009 [7, Theorem 5.4] (see also [14] and [12, Theorem 1]). Whether integer feasibility is in fact polynomial for these polyhedra has remained open since the result of Boyd and Pulleyblank.

Question 1. *Let $P = \{x \in \mathbb{R}^n : Cx \leq d\}$ with C and d rational, and suppose $P' = P_I$. Can we decide whether P contains an integer point in time polynomial in the encoding size of (C, d) ?*

This question was later stated explicitly by Cornuéjols and Li [13, 14], and it is the main motivation of the systematic study of this class by Cornuéjols, Lee, and Li [12], where it is stated for polyhedra of Chvátal rank exactly one. The two versions are equivalent (Section 2).

We regard Question 1 as a *promise problem*, with the promise $P' = P_I$, as in [14, 12]. An algorithm solves it in polynomial time if it runs in polynomial time on all inputs and answers correctly on those that satisfy the promise, while its answers on other inputs may be arbitrary. The promise matters. Under the promise, $P \cap \mathbb{Z}^n = \emptyset$ if and only if $P' = \emptyset$. Without it, deciding whether $P' = \emptyset$ is NP-complete, even for polyhedra containing no integer point [13, 12], and separating over P' is NP-hard [18]. With the promise, NP-hardness is unlikely: since the promise problem is in $\text{NP} \cap \text{coNP}$, a polynomial-time reduction from an NP-hard problem all of whose queries satisfy the promise would imply $\text{NP} = \text{coNP}$ [23] (see also [20, Theorem 7]).

Several problems in $\text{NP} \cap \text{coNP}$ were eventually shown to be polynomial, such as linear programming [36, Theorem 13.4] and primality testing [3]. Yet no algorithm is known to benefit from the promise $P' = P_I$. For instance, Cornuéjols, Lee, and Li prove a flatness theorem for compact convex sets with empty Chvátal closure, with an essentially tight bound [12, Theorem 14 and Proposition 15], and observe that it yields a Lenstra-type algorithm [25] with running time $2^{O(n)} n^n$ times a polynomial in the encoding size. This is slower than the randomized algorithm of Reis and Rothvoss for general integer programs, with running time $(\log n)^{O(n)}$ times a polynomial in the encoding size [34]. Similarly, branch-and-bound does not benefit from the promise: it can require exponentially many nodes even on polytopes with empty Chvátal closure [24].

Our results. We answer Question 1 negatively, under two standard assumptions from lattice-based cryptography: that lattice problems such as the shortest vector problem are hard to approximate within polynomial factors, and that learning with errors, an average-case lattice problem, is hard. Lattice problems are a natural source of hardness here: like integer feasibility under the promise $P' = P_I$, they are not expected to be NP-hard, since the decision versions of approximating the length of a shortest nonzero vector, or the distance of a target vector from the lattice, within a factor $c\sqrt{n}$ for a suitable constant c , are in $\text{NP} \cap \text{coNP}$ [4].

Let $L \subseteq \mathbb{R}^n$ be a full-rank lattice and let $\lambda_1(L)$ be the Euclidean length of a shortest nonzero vector of L . In the *bounded distance decoding problem* with factor α (BDD_α) we are given a basis B of L and a target vector t whose distance from L is at most $\alpha\lambda_1(L)$, and we want to find a vector v of L closest to t , or equivalently the *error* $t - v$. In integer programming terms, we want to solve the integer least squares problem $\min\{\|Bx - t\| : x \in \mathbb{Z}^n\}$ under the promise that its optimal value is at most $\alpha\lambda_1(L)$.

Theorem A (see Proposition 6, Theorem 7, and Corollary 9). *There is a deterministic polynomial-time reduction from $BDD_{1/(4n^2)}$ in dimension n to integer feasibility on rational polytopes in $\mathbb{R}^n$ with $P' = P_I$. In particular, a polynomial-time algorithm for the latter gives a polynomial-time algorithm for $BDD_{1/(4n^2)}$.*

Combined with reductions of Lyubashevsky and Micciancio [26], Theorem A has two further consequences (Corollary 9). First, a polynomial-time algorithm for integer feasibility under the promise $P' = P_I$ would give a polynomial-time algorithm for $uSVP_{4n^2}$, that is, for finding a shortest nonzero vector of L when every vector of L of length at most $4n^2\lambda_1(L)$ is an integer multiple of a shortest one. Second, it would give a randomized polynomial-time algorithm for $GapSVP_\gamma$ with $\gamma = 4n^{5/2}/\sqrt{\log n}$, that is, for approximating $\lambda_1(L)$ within a factor γ .

The best known algorithms for BDD, $uSVP$, and $GapSVP$ with polynomial factors run in time $2^{O(n)}$ [29, 2]. It is conjectured that no polynomial-time algorithm, even a randomized or quantum one, approximates lattice problems such as the shortest vector problem within polynomial factors [28, Conjectures 1 and 2]. This conjecture underlies lattice-based cryptography [33, 32]. Since $GapSVP$ is the decision version of the shortest vector problem, Corollary 9 shows that a polynomial-time algorithm for integer feasibility under the promise $P' = P_I$, even a randomized one, would contradict this conjecture.

The reduction of Theorem A preserves the dimension (Theorem 7), and so do those of Lyubashevsky and Micciancio. Hence, even an algorithm for integer feasibility under the promise $P' = P_I$ running in time $2^{o(n)}$ times a polynomial in the encoding size would give algorithms with the same running time for BDD and $uSVP$, and a randomized one for $GapSVP$ (Corollary 9).

Theorem A is a worst-case result: it does not give a distribution of hard instances that can be sampled efficiently. We obtain such a distribution from learning with errors (LWE) [33], the average-case problem on which much of lattice-based cryptography is built. In LWE with modulus q , we are given a uniformly random matrix $A \in \mathbb{Z}_q^{n \times m}$ and $t \equiv A^T s + e \pmod{q}$, where $s \in \mathbb{Z}_q^n$ is uniformly random and $e \in \mathbb{Z}^m$ is a short random error vector, and we want to find s , or to distinguish t from a uniformly random vector (decision-LWE). Thus t is a target vector close to the lattice of vectors $y \in \mathbb{Z}^m$ with $y \equiv A^T s \pmod{q}$ for some s , and LWE can be viewed as an average-case version of BDD.

Theorem B (see Propositions 6 and 12 and Theorem 13). *There is an efficiently samplable distribution of polytopes in $\mathbb{R}^m$ that are given by integral constraints with coefficients bounded by a polynomial in m and satisfy $P' = P_I$ with high probability. A randomized polynomial-time algorithm that decides integer feasibility correctly with probability at least $2/3$ on this distribution gives one for decision-LWE with a polynomial modulus and Gaussian errors. The same holds for a randomized polynomial-time algorithm that does so for every rational polytope with $P' = P_I$.*

A randomized polynomial-time algorithm for decision-LWE with these parameters would give a polynomial-time quantum algorithm for $GapSVP_\gamma$ with a polynomial γ , by a result of Regev [33] (Corollary 15). This contradicts the conjecture that no such quantum algorithm exists [28]. The two results are incomparable. The negative answer from Theorem A relies on the conjecture only for classical algorithms, and its reduction preserves the dimension. The negative answer from Theorem B relies on the conjecture for quantum algorithms, and its reduction increases the dimension from n to $O(n \log n)$. However, Theorem B gives hard instances on average, with integer coefficients bounded by a polynomial in the dimension, so it also rules out pseudo-polynomial algorithms.

The idea. The proof rests on an elementary sufficient condition for Chvátal rank at most one (Lemma 2): if P has width less than one along the rows of a unimodular matrix U , then

$P' = P_I$, and P_I is obtained by adding at most $2n$ CG cuts. We apply it to the parallelepipeds $\{x \in \mathbb{R}^n : \|Bx - t\|_\infty \leq r\}$ with $r > 0$, where B is a basis of a lattice L and t is a target vector (Figure 1). Their integer points x correspond, via $x \mapsto Bx$, to the vectors of L within ℓ_∞ -distance r from t . The unimodular matrices are exactly the matrices with rows $B^\top w_1, \dots, B^\top w_n$, where $w_1, \dots, w_n$ is a basis of the dual lattice L^* , and the width along $B^\top w_i$ is $2r\|w_i\|_1$. The dual lattice L^* has a basis with ℓ_1 -norms at most $n^2/\lambda_1(L)$, by a transference theorem of Banaszczyk [6, Theorem 2.1] (Lemma 5). Hence, for every t , these parallelepipeds and all their rational subpolyhedra have Chvátal rank at most one whenever $r < \lambda_1(L)/(2n^2)$, since widths can only decrease on subpolyhedra.

For Theorem A, if the distance of t from L is at most $\lambda_1(L)/(4n^2)$, we try radii r that are powers of two, and one of them gives a parallelepiped that satisfies the promise and contains the integer point corresponding to the closest vector. We then find this point coordinate by coordinate by binary search, whose queries are rational subpolyhedra of this parallelepiped and thus still satisfy the promise.

For Theorem B, the lattice of the vectors $y \in \mathbb{Z}^m$ with $y \equiv A^\top s \pmod{q}$ for some s depends only on A , which is uniformly random, so with high probability it has no short nonzero vectors (Lemma 11). Hence, by Proposition 6, each instance (A, t) yields a single parallelepiped in $\mathbb{R}^m$ that satisfies the promise with high probability. If t comes from LWE, then with high probability the error is short, and so this parallelepiped contains an integer point. If t is uniformly random, it contains none with high probability, by a counting argument. Thus a single query to an algorithm for integer feasibility distinguishes the two cases.

Easy with a short dual basis, hard without. For the parallelepipeds with $r < \lambda_1(L)/(2n^2)$, the promise holds because the dual lattice has a basis with small ℓ_1 -norms, and knowing such a basis makes the problem easy. With such a basis, Babai’s round-off algorithm [5] finds the integer point if there is one, and otherwise the basis gives a refutation with at most $2n + 1$ CG cuts (Remark 10). In the variables Ux , where U has rows $B^\top w_1, \dots, B^\top w_n$, the parallelepiped has width less than one along every coordinate direction, so each variable takes at most one integer value and branch-and-bound solves it with $O(n)$ nodes. This parallels the integer programs of Aardal, Hurkens, and Lenstra [1] and of Pataki, Tural, and Wong [31], which are hard for branch-and-bound in the original variables but easy after a reformulation computed by basis reduction. Here, however, finding such a basis is as hard as $\text{BDD}_{1/(4n^2)}$, and, for the parallelepipeds of Theorem B, as hard as decision-LWE (Remark 10). In proof complexity terms, CG cuts form the Cutting Planes proof system [11], and finding short refutations is NP-hard in general [22]. For our parallelepipeds, refutations with at most $2n + 1$ CG cuts always exist, but finding them is as hard as $\text{BDD}_{1/(4n^2)}$ and decision-LWE (Remark 10).

The paper is organized as follows. Section 2 contains preliminaries. Section 3 proves our sufficient condition for Chvátal rank at most one (Lemma 2), and Section 4 applies it to parallelepipeds defined by lattices (Proposition 6). Section 5 proves our results from worst-case lattice problems, including Theorem A (Theorem 7 and Corollary 9). Section 6 proves our results from LWE, including Theorem B (Proposition 12 and Theorem 13).

2 Preliminaries

Notation. We write e_i for the i th unit vector, and $\mathbf{0}$ and $\mathbf{1}$ for the all-zeros and all-ones vectors. All norms without subscript are Euclidean, and $\lfloor \cdot \rfloor$ denotes rounding to a nearest integer.

Polyhedra. For a polyhedron $P \subseteq \mathbb{R}^n$ and $c \in \mathbb{R}^n$, let $\delta_P(c) = \sup\{c^\top x : x \in P\}$, and let $\text{width}_P(c) = \delta_P(c) + \delta_P(-c)$ be the *width* of P along c . A *rational subpolyhedron* of P is a rational polyhedron contained in P .

Lattices. A *lattice* is a set $L = B\mathbb{Z}^n$, where $B \in \mathbb{R}^{n \times n}$ is nonsingular, and B is a *basis* of L . For $i = 1, \dots, n$, the i th successive minimum $\lambda_i(L)$ is the smallest λ such that L contains i linearly independent vectors of norm at most λ . For $t \in \mathbb{R}^n$, let $\text{dist}(t, L) = \min\{\|v - t\| : v \in L\}$. The *dual lattice* is $L^* = \{w \in \mathbb{R}^n : w^\top y \in \mathbb{Z} \text{ for all } y \in L\}$. We have $L^* = B^{-\top}\mathbb{Z}^n$ and $L^{**} = L$.

Promise problems. An algorithm solves a promise problem if it runs within its time bound on every input and answers correctly on every input that satisfies the promise [20, Section 1.2]. Its output on other inputs is arbitrary. A randomized or quantum algorithm solves a promise problem if it runs within its time bound on every input and answers correctly with probability at least $2/3$ on every input that satisfies the promise. Similarly, an oracle for a promise problem answers every query, and answers correctly the queries that satisfy the promise. A *reduction* from one promise problem to another is an algorithm that solves the first with every oracle for the second, where each oracle call counts as one step. The reduction is deterministic or randomized, and polynomial-time, if this algorithm is. It *preserves the dimension* if, on inputs of dimension n , all its queries have dimension n .

Lattice problems. In the following problems, the input is a rational basis B of a lattice $L \subseteq \mathbb{R}^n$, together with a rational vector t for BDD and a rational number η for GapSVP. The parameters $\alpha \in (0, 1)$ and $\gamma \geq 1$ are functions of n .

- BDD $_\alpha$: under the promise $\text{dist}(t, L) \leq \alpha\lambda_1(L)$, find $v \in L$ with $\|v - t\| = \text{dist}(t, L)$.
- uSVP $_\gamma$: under the promise $\lambda_2(L) > \gamma\lambda_1(L)$, find $v \in L$ with $\|v\| = \lambda_1(L)$.
- GapSVP $_\gamma$: under the promise that $\lambda_1(L) \leq \eta$ or $\lambda_1(L) > \gamma\eta$, decide which of the two holds.
- SIVP $_\gamma$: find n linearly independent vectors of L of norm at most $\gamma\lambda_n(L)$.

Learning with errors. Let $q \geq 2$, and let $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$, whose elements we represent by integers in $\{0, \dots, q-1\}$. In the following problem, the input is a pair (A, t) with $A \in \mathbb{Z}_q^{n \times m}$ and $t \in \mathbb{Z}_q^m$. The modulus q , the number of samples m , and a probability distribution χ on $\mathbb{Z}$ are functions of n . An *LWE instance* is a pair (A, t) with A uniformly random and $t \equiv A^\top s + e \pmod{q}$, where $s \in \mathbb{Z}_q^n$ is uniformly random and $e \in \mathbb{Z}^m$ has independent entries distributed according to χ . A *uniform instance* is a pair (A, t) with A and t uniformly random.

- decision-LWE $_{n,q,\chi}$ with m samples: given an LWE instance or a uniform instance, decide which of the two it is, by outputting 1 or 0, respectively.

An algorithm *solves* this problem if the probabilities that it outputs 1 on an LWE instance and on a uniform instance differ by at least n^{-c} for some constant $c > 0$ and all sufficiently large n .

Chvátal rank exactly one. We now show that the version of Question 1 for polyhedra of Chvátal rank exactly one [12] is equivalent to ours, which also allows rank zero. A rational polyhedron is integral if and only if each of its minimal faces contains an integer point [36, Section 16.3]. Given a rational polyhedron P with $P' = P_I$, we decide in polynomial time whether $P = \emptyset$, and if not,

we compute a minimal face F of P and decide whether F contains an integer point [36, proof of Theorem 16.2 and Corollary 5.3b]. If $P = \emptyset$ or F contains an integer point, we know the answer. Otherwise $P \neq P_I$, so P has Chvátal rank exactly one. Hence, in all our results, it suffices to consider polytopes of Chvátal rank exactly one, since every query can first be processed in this way.

3 A sufficient condition for Chvátal rank at most one

In this section we prove Lemma 2, the sufficient condition for Chvátal rank at most one on which all our reductions rest.

Lemma 2. *Let $U \in \mathbb{Z}^{n \times n}$ be unimodular with rows $u_1^\top, \dots, u_n^\top$, and let $P \subseteq \mathbb{R}^n$ be a rational polyhedron with $\text{width}_P(u_i) < 1$ for $i = 1, \dots, n$. Then $P' = P_I$, P_I is the intersection of P with at most $2n$ CG cuts, and P contains at most one integer point. Moreover, every rational subpolyhedron of P has Chvátal rank at most one.*

Proof. We may assume $P \neq \emptyset$. Then $\delta_P(\pm u_i)$ is finite, since $\text{width}_P(u_i) < 1$. Let P_0 be the intersection of P with the $2n$ CG cuts $u_i^\top x \leq \lfloor \delta_P(u_i) \rfloor$ and $-u_i^\top x \leq \lfloor \delta_P(-u_i) \rfloor$. For every i , every $x \in P_0$ satisfies $\lceil -\delta_P(-u_i) \rceil \leq u_i^\top x \leq \lfloor \delta_P(u_i) \rfloor$. Since these bounds are integers and $\text{width}_P(u_i) < 1$, either $P_0 = \emptyset$, or for every i there is an integer γ_i with $u_i^\top x = \gamma_i$ for all $x \in P_0$. In the second case, $P_0 \subseteq \{U^{-1}\gamma\}$, and $U^{-1}\gamma$ is an integer point since U is unimodular. In both cases $P_0 \subseteq P_I$, and so $P_I \subseteq P' \subseteq P_0 \subseteq P_I$, that is, $P' = P_I = P_0$. If $x, y \in P \cap \mathbb{Z}^n$, then $u_i^\top(x - y)$ is an integer of absolute value less than one for every i , so $Ux = Uy$ and $x = y$. Let S be a rational subpolyhedron of P . Then $\text{width}_S \leq \text{width}_P$, so the width assumption holds for S , and the first statement applies to S . $\square$

Remark 3. We note two features of Lemma 2, both illustrated, for $n \geq 2$, by the *cropped cube*

$$\left\{ x \in [0, 1]^n : \sum_{j \in J} x_j + \sum_{j \notin J} (1 - x_j) \geq \frac{1}{2} \text{ for all } J \subseteq \{1, \dots, n\} \right\},$$

which has Chvátal rank at least n [10, Lemma 7.2]. First, the strict inequality in Lemma 2 cannot be relaxed: the cropped cube has width one along every e_i . Second, the statement of Lemma 2 on rational subpolyhedra does not hold for general polyhedra of Chvátal rank at most one: the cube $[0, 1]^n$ is integral, but its rational subpolyhedron, the cropped cube, has Chvátal rank at least n .

4 Parallelepipeds defined by lattices

In this section we apply Lemma 2 to parallelepipeds defined by lattices: we compute their widths along the directions given by dual bases, and we show that these parallelepipeds satisfy the promise when they are thin enough (Proposition 6). For a basis $B \in \mathbb{Q}^{n \times n}$ of a lattice L , $t \in \mathbb{Q}^n$, and $r > 0$, let

$$Q(B, t, r) = \{x \in \mathbb{R}^n : \|Bx - t\|_\infty \leq r\} = \{x \in \mathbb{R}^n : t - r\mathbf{1} \leq Bx \leq t + r\mathbf{1}\},$$

which is a parallelepiped (Figure 1). The map $x \mapsto Bx$ is a bijection between $Q(B, t, r) \cap \mathbb{Z}^n$ and the set of vectors of L within ℓ_∞ -distance r from t . To apply Lemma 2 to $Q(B, t, r)$, we need a unimodular matrix along whose rows $Q(B, t, r)$ has width less than one. The next lemma shows that every basis $w_1, \dots, w_n$ of the dual lattice L^* gives a candidate, with rows $B^\top w_1, \dots, B^\top w_n$, and computes the widths along these rows.

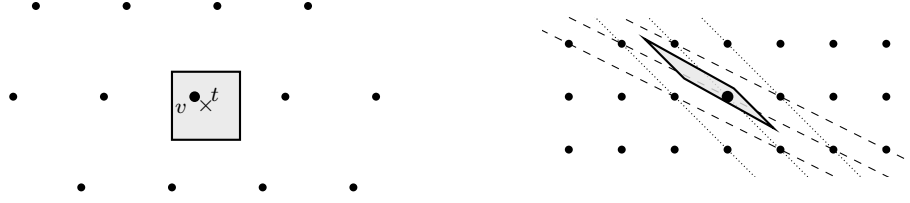


Figure 1: The parallelepiped $Q(B, t, r)$ for $B = \begin{pmatrix} 5 & 9 \\ 4 & 4 \end{pmatrix}$, $t = (4.5, -0.4)$, and $r = 1.5$. Left: the lattice $L = B\mathbb{Z}^2$ and the square $t + r[-1, 1]^2$, which contains only the vector $v = (4, 0)$ of L . Right: $Q(B, t, r)$, whose only integer point is $B^{-1}v = (-1, 1)$, and some of the lines $u_1^T x \in \mathbb{Z}$ (dashed) and $u_2^T x \in \mathbb{Z}$ (dotted), where $u_1 = B^T w_1 = (1, 2)$ and $u_2 = B^T w_2 = (1, 1)$ for the basis $w_1 = (\frac{1}{4}, -\frac{1}{16})$, $w_2 = (0, \frac{1}{4})$ of L^* . By Lemma 4, the widths of $Q(B, t, r)$ along u_1 and u_2 are $\frac{15}{16}$ and $\frac{3}{4}$, so Lemma 2 applies, whereas its widths along e_1 and e_2 are $\frac{39}{16}$ and $\frac{27}{16}$.

Lemma 4. *Let $B \in \mathbb{Q}^{n \times n}$ be a basis of a lattice L , let $t \in \mathbb{Q}^n$, let $r > 0$, and let $w_1, \dots, w_n$ be a basis of L^* . Then $B^T w_1, \dots, B^T w_n$ are the rows of a unimodular matrix, every unimodular matrix arises in this way from a basis of L^* , and $\text{width}_{Q(B, t, r)}(B^T w) = 2r\|w\|_1$ for every $w \in \mathbb{R}^n$.*

Proof. The map $w \mapsto B^T w$ is a linear bijection from L^* to $\mathbb{Z}^n$, hence it maps the bases of L^* bijectively to the bases of $\mathbb{Z}^n$, that is, to the rows of unimodular matrices. Moreover, $(B^T w)^T x = w^T Bx$ and $\{Bx : x \in Q(B, t, r)\} = t + r[-1, 1]^n$. Hence $\delta_{Q(B, t, r)}(B^T w) = w^T t + r\|w\|_1$ for every $w \in \mathbb{R}^n$, and adding this identity for w and $-w$ gives the claim. $\square$

To make these widths less than one, we need a basis of L^* with small ℓ_1 -norms. The next lemma shows that such a basis always exists.

Lemma 5. *For every lattice $L \subseteq \mathbb{R}^n$, the dual lattice L^* has a basis $w_1, \dots, w_n$ with $\|w_i\|_1 \leq n^2/\lambda_1(L)$ for $i = 1, \dots, n$.*

Proof. We have $\lambda_n(L^*) \leq n/\lambda_1(L)$, by a transference theorem of Banaszczyk [6, Theorem 2.1]. Moreover, by [27, Corollary 7.2], L^* has a basis $w_1, \dots, w_n$ such that, for $i = 1, \dots, n$,

$$\|w_i\| \leq \max\{1, \sqrt{i}/2\} \lambda_i(L^*).$$

Hence, since $\lambda_i(L^*) \leq \lambda_n(L^*)$, we have $\|w_i\| \leq \max\{1, \sqrt{n}/2\} n/\lambda_1(L) \leq n^{3/2}/\lambda_1(L)$, and $\|w_i\|_1 \leq \sqrt{n} \|w_i\| \leq n^2/\lambda_1(L)$. $\square$

Combining Lemmas 2, 4, and 5, we obtain the following.

Proposition 6. *Let $B \in \mathbb{Q}^{n \times n}$ be a basis of a lattice $L \subseteq \mathbb{R}^n$ and let $t \in \mathbb{Q}^n$. If $r \in \mathbb{Q}$ and $0 < r < \lambda_1(L)/(2n^2)$, then every rational subpolyhedron of $Q(B, t, r)$ has Chvátal rank at most one, and $Q(B, t, r)$ contains at most one integer point.*

Proof. Let $w_1, \dots, w_n$ be the basis of L^* given by Lemma 5. By Lemma 4, the matrix with rows $B^T w_1, \dots, B^T w_n$ is unimodular, and, for each i , the width of $Q(B, t, r)$ along $B^T w_i$ is $2r\|w_i\|_1 \leq 2rn^2/\lambda_1(L) < 1$. Since B , t , and r are rational, $Q(B, t, r)$ is a rational polyhedron, and the statement follows from Lemma 2. $\square$

5 Hardness from worst-case lattice problems

In this section we reduce worst-case lattice problems to integer feasibility under the promise $P' = P_I$. We use the parallelepipeds of Proposition 6 to solve BDD: we guess r and find the closest vector coordinate by coordinate (Theorem 7). Combined with reductions of Lyubashevsky and Micciancio, this gives consequences for uSVP and GapSVP (Corollary 9).

Theorem 7. *BDD $_{1/(4n^2)}$ can be solved in deterministic polynomial time with an oracle for integer feasibility under the promise that the query is a rational subpolyhedron of some parallelepiped $Q(B, t, r)$ in $\mathbb{R}^n$ with $r \in \mathbb{Q}$ and $r < \lambda_1(L)/(2n^2)$, where L is the lattice with basis B . Every query is a polytope in $\mathbb{R}^n$ given by at most $2n + 1$ rational inequalities.*

Proof. Let $B \in \mathbb{Q}^{n \times n}$ be a basis of a lattice L and let $t \in \mathbb{Q}^n$, with total encoding size σ . Let $\rho = \text{dist}(t, L)$, and let v^* be a vector of L closest to t . For an integer j , let $Q_j = Q(B, t, 2^j)$. The idea is to guess ρ up to a factor of two by trying the radii 2^j . If the input satisfies the promise of BDD, some j satisfies $\rho \leq 2^j < \lambda_1(L)/(2n^2)$. For such j , $B^{-1}v^*$ is the only integer point of Q_j , and we find it coordinate by coordinate by binary search.

We first construct integers $j_0 \leq j_1$ such that, under the promise, some j^* between them satisfies $\rho \leq 2^{j^*} < \lambda_1(L)/(2n^2)$. To do so, it suffices that $2^{j_0} \leq \lambda_1(L)/(4n^2)$ and $2^{j_1} \geq \rho$. Indeed, let j^* be the smallest integer $j \geq j_0$ with $2^j \geq \rho$, so that $j^* \leq j_1$. If $j^* = j_0$, then $2^{j^*} \leq \lambda_1(L)/(4n^2)$. Otherwise $2^{j^*-1} < \rho$ by the choice of j^* , and so $2^{j^*} < 2\rho$, which is at most $\lambda_1(L)/(2n^2)$ under the promise $\rho \leq \lambda_1(L)/(4n^2)$. We now construct such j_0 and j_1 . Since $\mathbf{0} \in L$, we have $\rho \leq \|t\| \leq 2^\sigma$, so $j_1 = \sigma$ satisfies $2^{j_1} \geq \rho$. The least common denominator D of the entries of B satisfies $D \leq 2^\sigma$ and $DL \subseteq \mathbb{Z}^n$. Since every nonzero vector of DL has norm at least one, $\lambda_1(L) \geq 1/D \geq 2^{-\sigma}$. Hence $j_0 = -\sigma - \lceil \log_2(4n^2) \rceil$ satisfies $2^{j_0} \leq \lambda_1(L)/(4n^2)$.

We consider $j = j_0, j_0 + 1, \dots, j_1$ and do the following for each j . We ask the oracle whether Q_j contains an integer point, and if it reports none, we proceed to the next j . If the oracle reports an integer point, then for $i = 1, \dots, n$, we compute $I_i = \{x_i : x \in Q_j\}$ by linear programming, and we let z_i be the result of binary search for the smallest integer $c \in I_i$ for which the oracle reports an integer point in $Q_j \cap \{x : x_i \leq c\}$ (or $z_i = 0$ if the search finds none). Each query is Q_j or $Q_j \cap \{x : x_i \leq c\}$, described by the $2n$ inequalities of $\|Bx - t\|_\infty \leq 2^j$ and possibly $x_i \leq c$. We then output Bz and stop. If no output is produced for $j \leq j_1$, we output $\mathbf{0}$. There are $j_1 - j_0 + 1 = O(\sigma)$ values of j , and 2^j has encoding size $O(\sigma)$ for each of them. The endpoints of I_i are optimal values of linear programs over Q_j , so they have encoding size polynomial in σ [36, Corollary 10.2a], and each binary search makes a number of queries polynomial in σ . Hence, on every input, the oracle is called a number of times polynomial in σ , on queries of encoding size polynomial in σ , and all other computations take time polynomial in σ .

We now show that the output is v^* if the input satisfies the promise $\rho \leq \lambda_1(L)/(4n^2)$. The point $z^* = B^{-1}v^*$ is integral, since $v^* \in B\mathbb{Z}^n$, and it lies in Q_{j^*} , since $\|Bz^* - t\|_\infty = \|v^* - t\|_\infty \leq \|v^* - t\| = \rho \leq 2^{j^*}$. By Proposition 6 with $r = 2^{j^*}$, z^* is the unique integer point of Q_{j^*} . For $j \leq j^*$, we have $Q_j \subseteq Q_{j^*}$, so Q_j and all queries made for it are rational subpolyhedra of Q_{j^*} , and the oracle answers them correctly, since $2^{j^*} < \lambda_1(L)/(2n^2)$. Hence, if Q_j contains no integer point, we proceed to the next j . Otherwise $Q_j \cap \mathbb{Z}^n = \{z^*\}$, so $Q_j \cap \{x : x_i \leq c\}$ contains an integer point if and only if $z_i^* \leq c$. These answers are monotone in c , and $z_i^* \in I_i$, so the binary search returns $z_i = z_i^*$, and $z = z^*$. Since Q_{j^*} contains z^* , the procedure stops at some $j \leq j^*$ and outputs $Bz^* = v^*$. This is why we try the values of j in increasing order: the oracle is guaranteed to answer correctly only for $j \leq j^*$. $\square$

To derive consequences for uSVP and GapSVP, we use the following reductions of Lyubashevsky and Micciancio.

Theorem 8 ([26, Theorems 2 and 4 and their proofs]). *Let $\gamma = \gamma(n)$ be bounded by a polynomial in n . There is a deterministic polynomial-time reduction from uSVP_γ to $\text{BDD}_{1/\gamma}$ that preserves the dimension. If $n \geq 2$ and $\gamma > 2\sqrt{n/\log n}$, there is a randomized polynomial-time reduction from GapSVP_γ to $\text{BDD}_{\sqrt{n/\log n}/\gamma}$ that preserves the dimension.*

The proofs in [26] show that both reductions are correct with every oracle for BDD that returns a vector of the lattice on every query. Every oracle can be turned into such an oracle by replacing each answer v to a query with basis B such that $B^{-1}v \notin \mathbb{Z}^n$ by $\mathbf{0}$, so these are reductions in the sense of Section 2. Theorem 7 and Proposition 6 give Theorem A. Replacing the oracle by an algorithm and combining Theorem 7 with Theorem 8, we obtain the further consequences stated in the introduction.

Corollary 9. *Suppose that an algorithm solves integer feasibility for rational polytopes under the promise $P' = P_I$ in time $T(n, s)$, where n is the dimension, s is the encoding size of the input, and T is nondecreasing. If T is bounded by a polynomial, then $\text{BDD}_{1/(4n^2)}$ and uSVP_{4n^2} can be solved in deterministic polynomial time, and, for $n \geq 2$, GapSVP_γ with $\gamma = 4n^{5/2}/\sqrt{\log n}$ can be solved in randomized polynomial time. If $T(n, s) = 2^{o(n)} \text{poly}(s)$, then these problems can be solved in time $2^{o(n)}$ times a polynomial in the encoding size, deterministically for BDD and uSVP and with randomization for GapSVP. If the algorithm is randomized, then all these statements hold with randomized algorithms for the three problems.*

Proof. By Proposition 6, every rational subpolyhedron of a parallelepiped $Q(B, t, r)$ with $r \in \mathbb{Q}$ and $r < \lambda_1(L)/(2n^2)$ satisfies $P' = P_I$, so the algorithm is an oracle as in Theorem 7. Since the queries are in dimension n and have encoding size polynomial in the encoding size σ of (B, t) , and T is nondecreasing, we obtain a deterministic algorithm for $\text{BDD}_{1/(4n^2)}$ that runs in time $T(n, \text{poly}(\sigma)) \text{poly}(\sigma)$ on every input. The statements about uSVP and GapSVP follow from Theorem 8 with $\gamma = 4n^2$ and $\gamma = 4n^{5/2}/\sqrt{\log n}$, respectively, since in both cases the BDD factor is $1/(4n^2)$. The statements about running times $2^{o(n)}$ hold since all the reductions preserve the dimension and make a polynomial number of queries of polynomial encoding size.

Suppose now that the algorithm is randomized and answers correctly with probability at least $2/3$. The algorithms above make a number K of queries polynomial in the encoding size of their input. We answer each new query by the majority answer of $O(\log K)$ independent runs of the algorithm, and give the same answer if the query is repeated, so that, by Hoeffding's inequality, each query that satisfies the promise is answered correctly with probability at least $1 - 1/(12K)$. By the union bound, all such queries are answered correctly with probability at least $11/12$. Hence BDD and uSVP are solved correctly with probability at least $11/12$, and GapSVP with probability at least $2/3 - 1/12 = 7/12$. Taking the majority answer of a constant number of independent runs of this algorithm for GapSVP raises this probability to $2/3$, again by Hoeffding's inequality. $\square$

We conclude this section with a remark on refutations.

Remark 10. If they contain no integer point, the parallelepipeds $Q(B, t, r)$ with $r < \lambda_1(L)/(2n^2)$ and their rational subpolyhedra have short refutations, but these refutations are hard to find. Let $B \in \mathbb{Q}^{n \times n}$ be a basis of a lattice L , let $t \in \mathbb{Q}^n$, and let $r \in \mathbb{Q}$ with $0 < r < \lambda_1(L)/(2n^2)$. Let $P \subseteq Q(B, t, r)$ be a rational polyhedron without integer points, and let $w_1, \dots, w_n$ be the basis of L^* given by Lemma 5. If $P = \emptyset$, then $n + 1$ of its defining inequalities, scaled to have integral coefficients and with their right-hand sides rounded down, form a refutation, by Helly's theorem. So we may assume $P \neq \emptyset$. As in the proof of Proposition 6, P has width less than one along each $u_i = B^\top w_i$, so the CG cuts for P along u_i and $-u_i$ either have empty intersection or together

give an equation $u_i^\top x = \gamma_i$ with $\gamma_i \in \mathbb{Z}$. If this happens for every i , the equations define a single integer point $\bar{z}$, since $u_1, \dots, u_n$ are the rows of a unimodular matrix, and $\bar{z} \notin P$. An inequality defining P that $\bar{z}$ violates, scaled to have integral coefficients and with its right-hand side rounded down, is a CG cut violated by $\bar{z}$, and together with the n equations it gives a contradiction. Hence P has a refutation with at most $2n + 1$ CG cuts. Given $w_1, \dots, w_n$, these cuts are easy to compute. For $P = Q(B, t, r)$, their right-hand sides are $\lfloor w_i^\top t + r \|w_i\|_1 \rfloor$ and $\lfloor -w_i^\top t + r \|w_i\|_1 \rfloor$, as in Babai's round-off algorithm [5]. Without such a basis, however, finding a refutation is as hard as $\text{BDD}_{1/(4n^2)}$. Indeed, given an algorithm that finds a refutation whenever one exists, we decide integer feasibility for these polytopes by running it and checking by linear programming whether its output is a refutation, and Theorem 7 applies. The same holds for finding $w_1, \dots, w_n$, or any unimodular matrix along whose rows $Q(B, t, r)$ has width less than one. Indeed, such a matrix gives, by linear programming, the CG cuts of the proof of Lemma 2, and thus decides integer feasibility for every rational subpolyhedron of $Q(B, t, r)$. Similarly, by Theorem 13 and the discussion after it, finding a refutation, or such a matrix, for these polytopes is as hard as decision-LWE. Thus, for these polytopes, the difficulty lies not in the size of the refutations but in finding them.

6 Hardness from learning with errors

In this section we reduce learning with errors to integer feasibility under the promise $P' = P_I$. We show that the parallelepipeds defined by random q -ary lattices, that is, lattices L with $q\mathbb{Z}^m \subseteq L \subseteq \mathbb{Z}^m$ [28, Section 2], satisfy the promise with high probability (Proposition 12), and we reduce decision-LWE to integer feasibility for a single such parallelepiped (Theorem 13). Combined with a result of Regev, this gives consequences for GapSVP and SIVP for quantum algorithms (Corollary 15).

For $A \in \mathbb{Z}_q^{n \times m}$ we consider the q -ary lattice

$$\Lambda_q(A^\top) = \{y \in \mathbb{Z}^m : y \equiv A^\top s \pmod{q} \text{ for some } s \in \mathbb{Z}_q^n\},$$

which contains $q\mathbb{Z}^m$ and hence has full rank. For an LWE instance (Section 2), $t - e \in \Lambda_q(A^\top)$, so t is close to $\Lambda_q(A^\top)$ when e is short. In this section, n is the dimension of s , and also of the lattice problems in Theorem 14, while the lattices $\Lambda_q(A^\top)$ and the parallelepipeds $Q(B, t, r)$ have dimension m .

By Proposition 6, the parallelepipeds $Q(B, t, r)$ defined by $\Lambda_q(A^\top)$ satisfy the promise whenever $r < \lambda_1(\Lambda_q(A^\top))/(2m^2)$. We first show that $\lambda_1(\Lambda_q(A^\top))$ is large with high probability over the choice of A .

Lemma 11. *Let q be prime, and let $A \in \mathbb{Z}_q^{n \times m}$ be uniformly random. Then $\lambda_1(\Lambda_q(A^\top)) > q/8$ with probability at least $1 - q^n 2^{-m}$.*

Proof. Let $L = \Lambda_q(A^\top)$. A nonzero vector of $q\mathbb{Z}^m$ has ℓ_∞ -norm at least q , and every other vector of L is congruent modulo q to $A^\top s$ for some nonzero $s \in \mathbb{Z}_q^n$. For fixed nonzero s , the vector $A^\top s$ is uniformly random in $\mathbb{Z}_q^m$, since q is prime. At most $2\lfloor q/8 \rfloor + 1 \leq q/2$ residues modulo q have a representative c with $|c| \leq q/8$. Hence, for fixed nonzero s , every entry of $A^\top s$ is such a residue with probability at most 2^{-m} . By the union bound over the fewer than q^n nonzero s , the probability that L has a nonzero vector of ℓ_∞ -norm at most $q/8$ is at most $q^n 2^{-m}$. Otherwise every nonzero $y \in L$ satisfies $\|y\| \geq \|y\|_\infty > q/8$, and so $\lambda_1(L) > q/8$. $\square$

We now show that the parallelepiped defined by an instance (A, t) satisfies the promise with high probability, and that it separates LWE instances from uniform instances.

Proposition 12. *Let q be prime, let $k = \lceil \log_2 q \rceil$ and $m = 3nk$, and assume $q > 16m^2$. Let $r = \lfloor (q-1)/(16m^2) \rfloor$, let χ be a probability distribution on $\mathbb{Z}$, and let ε_χ be the probability that a vector $e \in \mathbb{Z}^m$ with independent entries distributed according to χ satisfies $\|e\|_\infty > r$. Given A , a basis $B \in \{0, \dots, q\}^{m \times m}$ of $\Lambda_q(A^\top)$ can be computed in time polynomial in n and $\log q$. For $t \in \mathbb{Z}_q^m$, let $Q = Q(B, t, r)$. If $r < \lambda_1(\Lambda_q(A^\top))/(2m^2)$, then every rational subpolyhedron of Q has Chvátal rank at most one. If (A, t) is an LWE instance or a uniform instance, then $r < \lambda_1(\Lambda_q(A^\top))/(2m^2)$ with probability at least $1 - 2^{-2nk}$, and Q contains an integer point with probability at least $1 - \varepsilon_\chi$ in the first case and at most 2^{-m} in the second.*

Proof. We let B be the Hermite normal form basis of the lattice generated by the columns of $[A^\top \mid qI_m]$, that is, of $\Lambda_q(A^\top)$, which can be computed in time $\text{poly}(n, \log q)$ [36, Theorem 5.3]. Since B is lower triangular and $qe_i \in \Lambda_q(A^\top)$ for every i , each diagonal entry of B divides q , and the other entries in its row are nonnegative and smaller, so $B \in \{0, \dots, q\}^{m \times m}$. Then $Q = \{x : Bx \leq t + r\mathbf{1}, -Bx \leq -t + r\mathbf{1}\}$ has integral data, $2m$ inequalities, and encoding size polynomial in n and $\log q$.

In LWE instances and in uniform instances alike, A is uniformly random, so $\lambda_1(\Lambda_q(A^\top)) > q/8$ with probability at least $1 - q^n 2^{-m}$ by Lemma 11. Moreover, $q^n \leq 2^{nk} = 2^{m/3}$, so this probability is at least $1 - 2^{-2nk}$. Since $q > 16m^2$, we have $r \geq 1$ and $r < q/(16m^2)$. Hence, if $\lambda_1(\Lambda_q(A^\top)) > q/8$, then $r < (q/8)/(2m^2) < \lambda_1(\Lambda_q(A^\top))/(2m^2)$, and every rational subpolyhedron of Q has Chvátal rank at most one by Proposition 6.

Consider an LWE instance with $\|e\|_\infty \leq r$, which occurs with probability at least $1 - \varepsilon_\chi$. Since $t \equiv A^\top s + e \pmod{q}$, the vector $t - e \in \Lambda_q(A^\top)$ lies within ℓ_∞ -distance r of t , and so Q contains an integer point.

Consider a uniform instance. If Q contains an integer point, then $t \equiv A^\top s + e' \pmod{q}$ for some $s \in \mathbb{Z}_q^n$ and $e' \in \{-r, \dots, r\}^m$. There are at most $q^n(2r+1)^m$ such residues, and so Q contains an integer point with probability at most $q^n(2r+1)^m/q^m$. Since $q > 16m^2 \geq 16$, we have $2r+1 \leq q/(8m^2)+1 \leq q/4$, and $q^n \leq 2^{nk} = 2^{m/3}$, so this probability is at most $2^{m/3}4^{-m} \leq 2^{-m}$. $\square$

For $\alpha \in (0, 1)$, let $\bar{\Psi}_\alpha$ be the distribution of $\lfloor X \rfloor$, where X is normal with mean zero and standard deviation $\alpha q/\sqrt{2\pi}$. This is the error distribution of Regev [33, Section 2], lifted from $\mathbb{Z}_q$ to $\mathbb{Z}$, and it can be sampled efficiently. For this error distribution and suitable parameters, Proposition 12 gives an explicit distribution of hard instances.

Theorem 13. *Let n be sufficiently large, let $q = q(n)$ be a prime in $[n^3, 2n^3]$, which exists by Bertrand's postulate and can be found in time polynomial in n , let $k = \lceil \log_2 q \rceil$, let $\alpha = 1/(200n^2k^2 \log n)$, and let $m = 3nk$. Let $\mathcal{D}$ be the distribution of the parallelepiped Q of Proposition 12 with $\chi = \bar{\Psi}_\alpha$ when (A, t) is an LWE instance or a uniform instance, each with probability $1/2$. The distribution $\mathcal{D}$ can be sampled in polynomial time, and a sample of $\mathcal{D}$ has Chvátal rank at most one with probability at least $1 - 2^{-2nk}$. Suppose that a randomized polynomial-time algorithm decides integer feasibility correctly with probability at least $1/2 + n^{-c}$ for some constant $c > 0$, over the choice of Q from $\mathcal{D}$ and its own randomness. Then there is a randomized polynomial-time algorithm that solves decision-LWE $_{n,q,\bar{\Psi}_\alpha}$ with m samples.*

Proof. We apply Proposition 12 with $\chi = \bar{\Psi}_\alpha$. Since n is sufficiently large, we have $q > 16m^2$, and $r = \lfloor (q-1)/(16m^2) \rfloor \geq \alpha q \log n$, since $\alpha q \log n = q/(200n^2k^2)$, $16m^2 = 144n^2k^2$, $q \geq n^3$, and $k = O(\log n)$. Each entry of e is distributed according to $\bar{\Psi}_\alpha$, that is, it equals $\lfloor X \rfloor$ with X normal with mean zero and standard deviation $\bar{\sigma} = \alpha q/\sqrt{2\pi}$. Then each entry has absolute value greater than r with probability at most $\Pr[|X| \geq r + \frac{1}{2}] \leq \Pr[|X| \geq \alpha q \log n] = \Pr[|X| \geq \sqrt{2\pi} \log n \cdot \bar{\sigma}] \leq 2 \exp(-\pi \log^2 n)$, by the Gaussian tail bound $\Pr[|X| \geq \tau \bar{\sigma}] \leq 2 \exp(-\tau^2/2)$ for $\tau \geq 0$. Hence, by

the union bound over the m entries, $\varepsilon_\chi \leq 2m \exp(-\pi \log^2 n)$, which is smaller than every inverse polynomial in n for sufficiently large n . The distribution $\mathcal{D}$ can be sampled in polynomial time, since $\bar{\Psi}_\alpha$ can be and Q can be computed in polynomial time. By Proposition 12, a sample of $\mathcal{D}$ has Chvátal rank at most one with probability at least $1 - 2^{-2nk}$.

Given (A, t) , our algorithm computes Q as in Proposition 12, runs the given algorithm on Q , and outputs 1 if and only if the given algorithm reports that Q contains an integer point. Since $q \leq 2n^3$, our algorithm runs in time polynomial in n . Let β_1 and β_0 be the probabilities that the given algorithm answers incorrectly on Q for LWE instances and for uniform instances, respectively. Then $\beta_1 + \beta_0 \leq 1 - 2n^{-c}$, since the given algorithm answers incorrectly with probability at most $1/2 - n^{-c}$ for Q drawn from $\mathcal{D}$. By Proposition 12, the output is 1 with probability at least $1 - \varepsilon_\chi - \beta_1$ on LWE instances and at most $2^{-m} + \beta_0$ on uniform instances. These probabilities differ by at least $2n^{-c} - \varepsilon_\chi - 2^{-m}$, which is at least n^{-c} for sufficiently large n . $\square$

Theorem 13 also covers the worst case. Its assumption holds for an algorithm that decides integer feasibility correctly with probability at least $2/3$ for every parallelepiped $Q(B, t, r)$ in $\mathbb{R}^m$ with $r \in \mathbb{Q}$ and $r < \lambda_1(L)/(2m^2)$, where L is the lattice with basis B , and thus, by Proposition 6, for one that does so for every rational polytope with $P' = P_I$. Indeed, by Proposition 12, a sample of $\mathcal{D}$ is such a parallelepiped with probability at least $1 - 2^{-2nk}$, since B , t , and r are integral. Hence such an algorithm is correct with probability at least $2/3 - 2^{-2nk} \geq 1/2 + 1/n$ over the choice of Q from $\mathcal{D}$ and its own randomness. Together with Proposition 12, which gives the properties of these polytopes, this proves Theorem B.

To derive consequences for GapSVP and SIVP, we use the following result of Regev.

Theorem 14 ([33, Theorem 3.1, Section 3.3, and Lemma 4.4]). *Let $q = q(n)$ be a prime and $m = m(n)$ an integer, both bounded by a polynomial in n , and let $\alpha = \alpha(n) \in (0, 1)$ with $\alpha q > 2\sqrt{n}$ for all sufficiently large n . If there is a randomized polynomial-time algorithm that solves decision-LWE $_{n,q,\bar{\Psi}_\alpha}$ with m samples, then there is a polynomial-time quantum algorithm that solves GapSVP $_\gamma$ and SIVP $_\gamma$ on n -dimensional lattices for some $\gamma = \tilde{O}(n/\alpha)$, where $\tilde{O}$ hides polylogarithmic factors.*

Theorem 14 is stated with our notion of solving decision-LWE. Regev's results apply to it since, by averaging over s , an algorithm that solves decision-LWE in our sense distinguishes, for a fraction at least $n^{-c}/2$ of all $s \in \mathbb{Z}_q^n$, the LWE instances with secret s from uniform instances, with output probabilities that differ by at least $n^{-c}/2$, as required in [33, Lemma 4.4]. Combining Theorem 13, and the discussion after it, with Theorem 14, we obtain the consequence for quantum algorithms stated in the introduction.

Corollary 15. *Suppose that there is a randomized polynomial-time algorithm as in Theorem 13. Then, for some $\gamma = \tilde{O}(n^3)$, there is a polynomial-time quantum algorithm that solves GapSVP $_\gamma$ and SIVP $_\gamma$ on n -dimensional lattices.*

Proof. Let q , α , and m be as in Theorem 13. By Theorem 13, there is a randomized polynomial-time algorithm that solves decision-LWE $_{n,q,\bar{\Psi}_\alpha}$ with m samples. Theorem 14 applies, since $q \leq 2n^3$ is prime, $m = 3nk$, and $\alpha q \geq n^3/(200n^2k^2 \log n) > 2\sqrt{n}$, and it gives $\gamma = \tilde{O}(n/\alpha) = \tilde{O}(n^3)$. $\square$

Funding. A. Del Pia is partially supported by AFOSR Grant FA9550-23-1-0433 and ONR Grant N00014-25-1-2490. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the Air Force Office of Scientific Research or the Office of Naval Research.

References

- [1] Karen Aardal, Cor A. J. Hurkens, and Arjen K. Lenstra. Solving a system of linear Diophantine equations with lower and upper bounds on the variables. *Mathematics of Operations Research*, 25(3):427–442, 2000.
- [2] Divesh Aggarwal, Daniel Dadush, Oded Regev, and Noah Stephens-Davidowitz. Solving the shortest vector problem in 2^n time via discrete Gaussian sampling. In *Proceedings of the 47th Annual ACM Symposium on Theory of Computing (STOC)*, pages 733–742, 2015.
- [3] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. PRIMES is in P. *Annals of Mathematics*, 160(2):781–793, 2004.
- [4] Dorit Aharonov and Oded Regev. Lattice problems in $\text{NP} \cap \text{coNP}$. *Journal of the ACM*, 52(5):749–765, 2005.
- [5] László Babai. On Lovász’ lattice reduction and the nearest lattice point problem. *Combinatorica*, 6(1):1–13, 1986.
- [6] Wojciech Banaszczyk. New bounds in some transference theorems in the geometry of numbers. *Mathematische Annalen*, 296:625–635, 1993.
- [7] Sylvia Boyd and William R. Pulleyblank. Facet generating techniques. In William Cook, László Lovász, and Jens Vygen, editors, *Research Trends in Combinatorial Optimization*, pages 33–55. Springer, 2009.
- [8] Vašek Chvátal. Edmonds polytopes and a hierarchy of combinatorial problems. *Discrete Mathematics*, 4(4):305–337, 1973.
- [9] Vašek Chvátal. On certain polytopes associated with graphs. *Journal of Combinatorial Theory, Series B*, 18(2):138–154, 1975.
- [10] Vašek Chvátal, William J. Cook, and Mark E. Hartmann. On cutting-plane proofs in combinatorial optimization. *Linear Algebra and its Applications*, 114–115:455–499, 1989.
- [11] William Cook, Collette R. Coullard, and György Turán. On the complexity of cutting-plane proofs. *Discrete Applied Mathematics*, 18(1):25–38, 1987.
- [12] Gérard Cornuéjols, Dabeen Lee, and Yanjun Li. On the rational polytopes with Chvátal rank 1. *Mathematical Programming*, 179(1–2):21–46, 2020.
- [13] Gérard Cornuéjols and Yanjun Li. Deciding emptiness of the Gomory–Chvátal closure is NP-complete, even for a rational polyhedron containing no integer point. In *Integer Programming and Combinatorial Optimization (IPCO 2016)*, volume 9682 of *Lecture Notes in Computer Science*, pages 387–397. Springer, 2016.
- [14] Gérard Cornuéjols and Yanjun Li. When the Gomory–Chvátal closure coincides with the integer hull. *Operations Research Letters*, 46(2):251–256, 2018.
- [15] Alberto Del Pia and Silvia Di Gregorio. Chvátal rank in binary polynomial optimization. *INFORMS Journal on Optimization*, 3(4):315–349, 2021.

- [16] Alberto Del Pia, Antoine Musitelli, and Giacomo Zambelli. On matrices with the Edmonds–Johnson property arising from bidirected graphs. *Journal of Combinatorial Theory, Series B*, 130:49–91, 2018.
- [17] Jack Edmonds. Maximum matching and a polyhedron with 0,1-vertices. *Journal of Research of the National Bureau of Standards, Section B*, 69B(1–2):125–130, 1965.
- [18] Friedrich Eisenbrand. On the membership problem for the elementary closure of a polyhedron. *Combinatorica*, 19(2):297–300, 1999.
- [19] A. M. H. Gerards and Alexander Schrijver. Matrices with the Edmonds–Johnson property. *Combinatorica*, 6(4):365–379, 1986.
- [20] Oded Goldreich. On promise problems: a survey. In Oded Goldreich, Arnold L. Rosenberg, and Alan L. Selman, editors, *Theoretical Computer Science: Essays in Memory of Shimon Even*, volume 3895 of *Lecture Notes in Computer Science*, pages 254–290. Springer, 2006.
- [21] Ralph E. Gomory. Outline of an algorithm for integer solutions to linear programs. *Bulletin of the American Mathematical Society*, 64(5):275–278, 1958.
- [22] Mika Göös, Sajin Korothe, Ian Mertz, and Toniann Pitassi. Automating cutting planes is NP-hard. In *Proceedings of the 52nd Annual ACM Symposium on Theory of Computing (STOC)*, pages 68–77, 2020.
- [23] Joachim Grollmann and Alan L. Selman. Complexity measures for public-key cryptosystems. *SIAM Journal on Computing*, 17(2):309–335, 1988.
- [24] Robert G. Jeroslow. Trivial integer programs unsolvable by branch-and-bound. *Mathematical Programming*, 6(1):105–109, 1974.
- [25] Hendrik W. Lenstra, Jr. Integer programming with a fixed number of variables. *Mathematics of Operations Research*, 8(4):538–548, 1983.
- [26] Vadim Lyubashevsky and Daniele Micciancio. On bounded distance decoding, unique shortest vectors, and the minimum distance problem. In *Advances in Cryptology – CRYPTO 2009*, volume 5677 of *Lecture Notes in Computer Science*, pages 577–594. Springer, 2009.
- [27] Daniele Micciancio and Shafi Goldwasser. *Complexity of Lattice Problems: A Cryptographic Perspective*, volume 671 of *The Kluwer International Series in Engineering and Computer Science*. Kluwer Academic Publishers, 2002.
- [28] Daniele Micciancio and Oded Regev. Lattice-based cryptography. In Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen, editors, *Post-Quantum Cryptography*, pages 147–191. Springer, 2009.
- [29] Daniele Micciancio and Panagiotis Voulgaris. A deterministic single exponential time algorithm for most lattice problems based on Voronoi cell computations. *SIAM Journal on Computing*, 42(3):1364–1391, 2013.
- [30] Christos H. Papadimitriou and Mihalis Yannakakis. On recognizing integer polyhedra. *Combinatorica*, 10(1):107–109, 1990.

- [31] Gábor Pataki, Mustafa Tural, and Erick B. Wong. Basis reduction and the complexity of branch-and-bound. In *Proceedings of the 21st Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 1254–1261, 2010.
- [32] Chris Peikert. A decade of lattice cryptography. *Foundations and Trends in Theoretical Computer Science*, 10(4):283–424, 2016.
- [33] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM*, 56(6):34:1–34:40, 2009.
- [34] Victor Reis and Thomas Rothvoss. The subspace flatness conjecture and faster integer programming. In *Proceedings of the 64th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 974–988, 2023.
- [35] Alexander Schrijver. On cutting planes. *Annals of Discrete Mathematics*, 9:291–296, 1980.
- [36] Alexander Schrijver. *Theory of Linear and Integer Programming*. Wiley, 1986.