Low-dimensional lattice basis reduction revisited

Phong Q. Nguyen, Damien Stehlé

Low-Dimensional Lattice Basis Reduction Revisited

PHONG Q. NGUYEN
INRIA/École Normale Supérieure
and
DAMIEN STEHLÉ
CNRS/Universities of Macquarie, Sydney and Lyon/ÉNS Lyon/INRIA

Lattice reduction is a geometric generalization of the problem of computing greatest common divisors. Most of the interesting algorithmic problems related to lattice reduction are NP-hard as the lattice dimension increases. This article deals with the low-dimensional case. We study a greedy lattice basis reduction algorithm for the Euclidean norm, which is arguably the most natural lattice basis reduction algorithm, because it is a straightforward generalization of an old two-dimensional algorithm of Lagrange, usually known as Gauss' algorithm, and which is very similar to Euclid's gcd algorithm. Our results are two-fold. From a mathematical point of view, we show that up to dimension four, the output of the greedy algorithm is optimal: the output basis reaches all the successive minima of the lattice. However, as soon as the lattice dimension is strictly higher than four, the output basis may be arbitrarily bad as it may not even reach the first minimum. More importantly, from a computational point of view, we show that up to dimension four, the bit-complexity of the greedy algorithm is quadratic without fast integer arithmetic, just like Euclid's gcd algorithm. This was already proved by Semaev up to dimension three using rather technical means, but it was previously unknown whether or not the algorithm was still polynomial in dimension four. We propose two different analyzes: a global approach based on the geometry of the current basis when the length decrease stalls, and a local approach showing directly that a significant length decrease must occur every $O(1)$ consecutive steps. Our analyzes simplify Semaev's analysis in dimensions two and three, and unify the cases of dimensions two to four. Although the global approach is much simpler, we also present the local approach because it gives further information on the behavior of the algorithm.

Categories and Subject Descriptors: F.2.1 [**Theory of Computation**]: Numerical Algorithms and Problems

General Terms: Algorithms

Additional Key Words and Phrases: Gauss' algorithm, lattice reduction

First author's address: Phong Q. Nguyen, École Normale Supérieure, Département d'informatique, 45 rue d'Ulm, 75230 Paris Cedex 05, France. `http://www.di.ens.fr/~pnguyen/`
Second author's address: Damien Stehlé, Department of Mathematics and Statistics (F07), University of Sydney, NSW 2006, Australia. `http://perso.ens-lyon.fr/damien.stehle`

1. INTRODUCTION

A *lattice* is a discrete subgroup of $\mathbb{R}^n$. Any lattice L has a *lattice basis*, i.e., a set $\{\mathbf{b}_1, \ldots, \mathbf{b}_d\}$ of linearly independent vectors such that the lattice is the set of all integer linear combinations of the $\mathbf{b}_i$'s: $L[\mathbf{b}_1, \ldots, \mathbf{b}_d] = \left\{\sum_{i=1}^{d} x_i \mathbf{b}_i, x_i \in \mathbb{Z}\right\}$. A lattice basis is usually not unique, but all the bases have the same number of elements, called the *dimension* or *rank* of the lattice. In dimension higher than one, there are infinitely many bases, but some are more interesting than others: they are called *reduced*. Roughly speaking, a reduced basis is a basis made of reasonably short vectors that are almost orthogonal. Finding good reduced bases has proved invaluable in many fields of computer science and mathematics, particularly in cryptology (see for instance the survey [Nguyen and Stern 2001]); and the computational complexity of lattice problems has attracted considerable attention in the past few years (see for instance the book [Micciancio and Goldwasser 2002]), following Ajtai's discovery [1996] of a connection between the worst-case and average-case complexities of certain lattice problems. Lattice reduction can be viewed as a geometric generalization of gcd computations.

There exist many different notions of reduction, such as those of Hermite [1850], Minkowski [1896], Hermite-Korkine-Zolotarev (HKZ) [Hermite 1905; Korkine and Zolotarev 1873], Venkov [Ryskov 1972], Lenstra-Lenstra-Lovász (LLL) [Lenstra et al. 1982], etc. Among these, the most intuitive one is perhaps Minkowski's, and up to dimension four it is arguably optimal compared to all other known reductions, because it reaches all the so-called successive minima of a lattice. However, finding a Minkowski-reduced basis or a HKZ-reduced basis is NP-hard under randomized reductions as the dimension increases, because such bases contain a shortest lattice vector and the shortest vector problem is NP-hard under randomized reductions [Ajtai 1998]. In order to better understand lattice reduction, it is tempting to study the low-dimensional case. Improvements in low-dimensional lattice reduction may lead to significant running-time improvements in high-dimensional lattice reduction, as the best lattice reduction algorithms known in theory [Gama and Nguyen 2008; Schnorr 1987] and in practice [Schnorr and Euchner 1994; Schnorr and Hörner 1995] for high-dimensional lattices are based on a repeated use of low-dimensional HKZ-reduction.

Lagrange's algorithm [1773] computes in quadratic time (without fast integer arithmetic [Schönhage and Strassen 1971]) a Minkowski-reduced basis of any two-dimensional lattice. This algorithm, which is a natural generalization of Euclid's gcd algorithm, was also described later by Gauss [1801], and is often erroneously called Gauss' algorithm. It was extended to dimension three by Vallée [1986] and Semaev [2001]: Semaev's algorithm is quadratic without fast integer arithmetic, whereas Vallée's has cubic complexity. More generally, Helfrich [1985] showed by means of the LLL algorithm [Lenstra et al. 1982] how to compute in cubic time a Minkowski-reduced basis of any lattice of fixed (arbitrary) dimension, but the hidden complexity constant grows very fast with the dimension. Finally, Eisenbrand and Rote described in [2001] a lattice basis reduction algorithm with a quasi-linear time complexity in any fixed dimension, but it is based on exhaustive enumerations and the complexity seems to blow up very quickly when the dimension increases. Moreover, they use fast integer arithmetic [Schönhage and Strassen 1971].

In this paper, we generalize Lagrange's algorithm to arbitrary dimension. Although the obtained greedy algorithm is arguably the simplest lattice basis reduction algorithm known, its analysis becomes remarkably more and more complex as the dimension increases. Semaev [2001] was the first to prove that the algorithm was still polynomial time in dimension three, but the polynomial-time complexity and the output quality remained open for higher dimension (see [Semaev 2001, Remark 5]). We show that up to dimension four, the greedy algorithm computes a Minkowski-reduced basis in quadratic time without fast arithmetic (which gives hope for a quasi-linear lime algorithm using fast arithmetic). This immediately implies that a shortest vector and a HKZ-reduced basis can be computed in quadratic time up to dimension four. Independently of the running time improvement, we hope our analysis may help to design new lattice reduction algorithms.

We propose two different approaches, both based on geometric properties of low-dimensional lattices, which generalize two different analyzes of Lagrange's algorithm. The global approach generalizes up to dimension four the two-dimensional analysis of Vallée [1991], and that of Akhavi [2000] where it was used to bound the number of loop iterations of the so-called optimal LLL algorithm in any dimension. Our generalization is different from this one. Roughly speaking, the global approach considers the following question: what does happen when the algorithm stops working well, that is, when it no longer shortens much the longest basis vector? The local approach considers a dual question: can we bound directly the number of consecutive steps necessary to significantly shorten the basis vectors? In dimension two, this method is very close to the argument given by Semaev in [2001], which is itself very different from previous analyzes of Lagrange's algorithm [Kaib and Schnorr 1996; Lagarias 1980; Vallée 1991]. In dimension three, Semaev's analysis [2001] is based on a rather exhaustive analysis of all the possible behaviors of the algorithm, which involves quite a few computations and makes it difficult to extend to higher dimension. We replace the main technical arguments by geometrical considerations on two-dimensional lattices. This makes it possible to extend the analysis to dimension four, by carefully studying geometrical properties of three-dimensional lattices, although a few additional technical difficulties appear.

The global approach provides a quicker proof of the main result, but less insight on the local behavior of the algorithm, i.e., how the algorithm makes progress in successive loop iterations. The local approach relies on more subtle geometrical properties of low-dimensional lattices, including the shapes of their Voronoï cells.

Road-map of the paper: In Section 2, we recall useful facts about lattices. In Section 3, we recall Lagrange's algorithm and give two different complexity analyzes. In Section 4 we describe its natural greedy generalization. Section 5 provides an efficient low-dimensional closest vector algorithm, which is the core of the greedy algorithm. In Section 6, we give our global approach to bound the number of loop iterations of the algorithm, and in Section 7 we prove the claimed quadratic complexity bound. In Section 8 we give an alternative proof for the bound of the number of loop iterations, the so-called local approach. In dimension below four, the quadratic complexity bound can also be derived from Sections 8 and 7 independently of Section 6. In Section 9, we prove geometrical results on low-

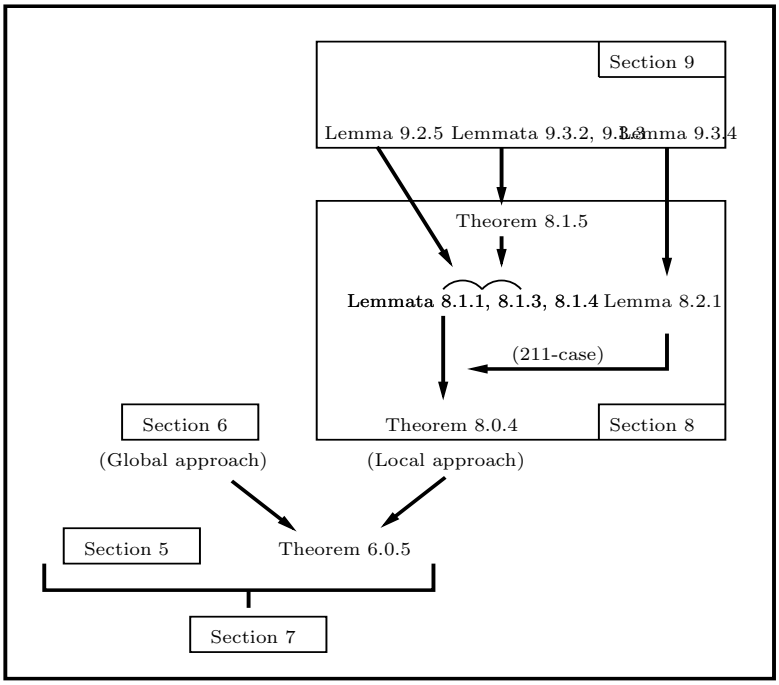

Fig. 1. The graph of the proof of the complexity bound.

dimensional lattices that are useful to prove the so-called Gap Lemma, an essential ingredient of the local approach of Section 8. Finally, in Section 10, we explain the difficulties arising in dimension 5. The structure of the proof of the complexity bound is given in Figure 1.

Preliminary remark: The present article is an extended and improved version of the conference paper [Nguyen and Stehlé 2004]. Interestingly, the cancellation technique of Section 7 has been slightly modified to give a precise analysis of a provable floating-point LLL algorithm, in [Nguyen and Stehlé 2005], leading to the first LLL algorithm with quadratic complexity. In the conference version [Nguyen and Stehlé 2004], we claimed that all variants of the LLL algorithm were at least cubic in any fixed dimension: this is no longer true since [Nguyen and Stehlé 2005], which was motivated by the present low-dimensional work.

Notation: Let $\|\cdot\|$ and $\langle\cdot,\cdot\rangle$ denote respectively the Euclidean norm and inner product of $\mathbb{R}^n$; variables in bold are vectors; whenever the notation $[\mathbf{b}_1,\ldots,\mathbf{b}_d]_{\leq}$ is used, we have $\|\mathbf{b}_1\| \leq \ldots \leq \|\mathbf{b}_d\|$ and in such a case, we say that the $\mathbf{b}_i$'s are *ordered*. Besides, the complexity model we use is the RAM model and the computational cost is measured in elementary operations on bits. In any complexity statement, we assume that the underlying lattice L is integral ($L \subseteq \mathbb{Z}^n$). If $x \in \mathbb{R}$, then $\lfloor x \rceil$ denotes a nearest integer to x. For any $n \in \mathbb{N}$, $\mathcal{S}_n$ denotes the group of the permutations of $[\![1,n]\!]$.

2. PRELIMINARIES

We assume the reader is familiar with geometry of numbers (see [Cassels 1971; Martinet 2002; Siegel 1989]).

2.1 Some Basic Definitions

We first recall some basic definitions related to Gram-Schmidt orthogonalization and the first minima.

Gram matrix and orthogonality-defect. Let $\mathbf{b}_1, \ldots, \mathbf{b}_d$ be vectors. The *Gram matrix* $G(\mathbf{b}_1, \ldots, \mathbf{b}_d)$ of $\mathbf{b}_1, \ldots, \mathbf{b}_d$ is the $d \times d$ symmetric matrix $(\langle \mathbf{b}_i, \mathbf{b}_j \rangle)_{1 \leq i,j \leq d}$ formed by all the inner products. The vectors $\mathbf{b}_1, \ldots, \mathbf{b}_d$ are linearly independent if and only if the determinant of $G(\mathbf{b}_1, \ldots, \mathbf{b}_d)$ is not zero. The volume vol L of a lattice L is the square root of the determinant of the Gram matrix of any basis of L. The *orthogonality-defect* of a basis $(\mathbf{b}_1, \ldots, \mathbf{b}_d)$ of L is defined as $\delta_\perp(\mathbf{b}_1, \ldots, \mathbf{b}_d) = (\prod_{i=1}^{d} \|\mathbf{b}_i\|)/\text{vol } L$: it is always greater than 1, with equality if and only if the basis is orthogonal.

Gram-Schmidt orthogonalization and size-reduction. Let $(\mathbf{b}_1, \ldots, \mathbf{b}_d)$ be linearly independent vectors. The *Gram-Schmidt orthogonalization* $(\mathbf{b}_1^*, \ldots, \mathbf{b}_d^*)$ is defined as follows: $\mathbf{b}_i^*$ is the component of $\mathbf{b}_i$ that is orthogonal to the subspace spanned by the vectors $\mathbf{b}_1, \ldots, \mathbf{b}_{i-1}$. Any basis vector $\mathbf{b}_i$ can be expressed as a (real) linear combination of the previous $\mathbf{b}_j^*$'s. We define the *Gram-Schmidt coefficients* $\mu_{i,j}$'s as the coefficients of these linear combinations, namely, for any $i \in [\![1, d]\!]$:

$$\mathbf{b}_i = \mathbf{b}_i^* + \sum_{j<i} \mu_{i,j} \mathbf{b}_j^*.$$

We have the equality $\mu_{i,j} = \frac{\langle \mathbf{b}_i, \mathbf{b}_j^* \rangle}{\|\mathbf{b}_j^*\|^2}$, for any $j < i$.

A lattice basis $(\mathbf{b}_1, \ldots, \mathbf{b}_d)$ is said to be *size-reduced* if its Gram-Schmidt coefficients $\mu_{i,j}$'s all satisfy: $|\mu_{i,j}| \leq 1/2$. Size-reduction was introduced by Lagrange [1773], and can be easily achieved by subtracting to each $\mathbf{b}_i$ a suitable linear combination $\sum_{j=1}^{i-1} x_j \mathbf{b}_j$ of the previous $\mathbf{b}_j$'s, for each $i = 2, \ldots, d$.

Successive minima and the Shortest Vector Problem. Let L be a d-dimensional lattice in $\mathbb{R}^n$. For $1 \leq i \leq d$, the *i-th minimum* $\lambda_i(L)$ is the radius of the smallest closed ball centered at the origin containing at least i linearly independent lattice vectors. The most famous lattice problem is the *shortest vector problem* (SVP): given a basis of a lattice L, find a lattice vector whose norm is exactly $\lambda_1(L)$. There always exist linearly independent lattice vectors $\mathbf{v}_i$'s such that $\|\mathbf{v}_i\| = \lambda_i(L)$ for all i. Amazingly, as soon as $d \geq 4$ such vectors do not necessarily form a lattice basis, and when $d \geq 5$ there may not even exist a lattice basis reaching all the minima.

2.2 Different Types of Strong Reduction

Several types of strong lattice basis reductions are often considered in the literature. The following list is not exhaustive but includes the most frequent ones: Minkowski's and Hermite-Korkine-Zolotarev's. Notice that though mathematically different, these two reductions are computationally very close in low dimension: one can derive a reduced basis of one type from a reduced basis of the other type very efficiently.

Minkowski reduction. A basis $[\mathbf{b}_1, \ldots, \mathbf{b}_d]_{\leq}$ of a lattice L is *Minkowski-reduced* if for all $1 \leq i \leq d$, the vector $\mathbf{b}_i$ has minimal norm among all lattice vectors $\mathbf{b}_i$ such that $[\mathbf{b}_1, \ldots, \mathbf{b}_i]_{\leq}$ can be extended to a basis of L. Equivalently:

LEMMA 2.2.1. *A basis $[\mathbf{b}_1, \ldots, \mathbf{b}_d]_{\leq}$ of a lattice L is Minkowski-reduced if and only if for any $i \in [\![1, d]\!]$ and for any integers $x_1, \ldots, x_d$ such that $x_i, \ldots, x_d$ are altogether coprime, we have:*

$$\|x_1\mathbf{b}_1 + \ldots + x_d\mathbf{b}_d\| \geq \|\mathbf{b}_i\|.$$

With the above statement, one might think that to ensure that a given basis is Minkowski reduced, there are infinitely many conditions to be checked. Fortunately, a classical result states that in any fixed dimension, it is sufficient to check a finite subset of them. This result is described as the second finiteness theorem in [Siegel 1989]. Several sufficient sets of conditions are possible. We call *Minkowski conditions* such a subset with minimal cardinality. Minkowski conditions have been obtained by Tammela [1973] up to dimension 6. As a consequence, in low dimension, one can check very quickly if a basis is Minkowski-reduced by checking these conditions.

THEOREM 2.2.2 [MINKOWSKI CONDITIONS]. *Let $d \leq 6$. A basis $[\mathbf{b}_1, \ldots, \mathbf{b}_d]_{\leq}$ of L is Minkowski-reduced if and only if for any $i \leq d$ and for any integers $x_1, \ldots, x_d$ that satisfy both conditions below, we have the inequality:*

$$\|x_1\mathbf{b}_1 + \ldots + x_d\mathbf{b}_d\| \geq \|\mathbf{b}_i\|.$$

(1) The integers $x_i, \ldots, x_d$ are altogether coprime,

(2) For some permutation σ of $[\![1, d]\!]$, $(|x_{\sigma(1)}|, \ldots, |x_{\sigma(d)}|)$ appears in the list below (where blanks eventually count as zeros).

1	1				
1	1	1			
1	1	1	1		
1	1	1	1	1	
1	1	1	1	2	
1	1	1	1	1	1
1	1	1	1	1	2
1	1	1	1	2	2
1	1	1	1	2	3

Moreover this list is minimal, which means that if any condition is disregarded, then a basis can satisfy all the others without being Minkowski-reduced.

A basis of a d-dimensional lattice that reaches the d minima must be Minkowski-reduced, but a Minkowski-reduced basis may not reach all the minima, except the first four ones (see [van der Waerden 1956]): if $[\mathbf{b}_1, \ldots, \mathbf{b}_d]_\leq$ is a Minkowski-reduced basis of L, then for all $1 \leq i \leq \min(d, 4)$ we have $\|\mathbf{b}_i\| = \lambda_i(L)$, but the best theoretical upper bound known for $\|\mathbf{b}_d\|/\lambda_d(L)$ grows exponentially in d. Therefore, a Minkowski-reduced basis is optimal in a natural sense up to dimension four. A related classical result (see [van der Waerden 1956]) states that the orthogonality-defect of a Minkowski-reduced basis can be upper-bounded by a constant that only depends on the lattice dimension.

Hermite reduction. Hermite [1905] defined different types of reduction, which sometimes creates confusions. In particular, Hermite reduction differs from what we call below Hermite-Korkine-Zolotarev reduction. An ordered basis $[\mathbf{b}_1, \ldots, \mathbf{b}_d]_\leq$ is *Hermite-reduced* if it is the smallest basis of L for the lexicographic order: for any other basis $[\mathbf{b}'_1, \ldots, \mathbf{b}'_d]_\leq$ of L, we must have $\|\mathbf{b}_1\| = \|\mathbf{b}'_1\|, \ldots, \|\mathbf{b}_{i-1}\| = \|\mathbf{b}'_{i-1}\|$ and $\|\mathbf{b}'_i\| > \|\mathbf{b}_i\|$ for some $i \in [\![1, d]\!]$. In particular a Hermite-reduced basis is always Minkowski-reduced. The converse is true as long as $d \leq 6$ (see [Ryskov 1972]).

Hermite-Korkine-Zolotarev reduction. This reduction is often called more simply Korkine-Zolotarev reduction. A basis $(\mathbf{b}_1, \ldots, \mathbf{b}_d)$ of a lattice L is *Hermite-Korkine-Zolotarev-reduced* (HKZ-reduced for short) if $\|\mathbf{b}_1\| = \lambda_1(L)$ and for any $i \geq 2$, the vector $\mathbf{b}_i$ is a lattice vector having minimal nonzero distance to the linear span of $\mathbf{b}_1, \ldots, \mathbf{b}_{i-1}$, and the basis is size-reduced, that is, its Gram-Schmidt coefficients $\mu_{i,j}$ have absolute values $\leq 1/2$. In high dimension, the reduction of Hermite-Korkine-Zolotarev [Hermite 1905; Korkine and Zolotarev 1873] seems to be stronger than Minkowski's: all the elements of a HKZ-reduced basis are known to be very close to the successive minima (see [Lagarias et al. 1990]), while in the case of Minkowski reduction the best upper bound known for for the approximation to the successive minima grows exponentially with the dimension [van der Waerden 1956], as mentioned previously. In dimension two, HKZ reduction is equivalent to Minkowski's. But in dimension three, there are lattices such that no Minkowski-reduced basis is HKZ-reduced:

LEMMA 2.2.3. *Let* $\mathbf{b}_1 = [100, 0, 0], \mathbf{b}_2 = [49, 100, 0]$ *and* $\mathbf{b}_3 = [0, 62, 100]$. *Then* $L[\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3]_\leq$ *has no basis that is simultaneously Minkowski-reduced and HKZ-reduced.*

PROOF. First, the basis $[\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3]_\leq$ is not HKZ-reduced because $|\mu_{3,2}| = \frac{62}{100} > 1/2$. But it is Minkowski-reduced (it suffices to check the Minkowski conditions to prove it). Therefore $[\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3]_\leq$ reaches the first three minima. More precisely, the vectors $\pm\mathbf{b}_1$ are the only two vectors reaching the first minimum, the vectors $\pm\mathbf{b}_2$ are the only two vectors reaching the second minimum and the vectors $\pm\mathbf{b}_3$ are the only two vectors reaching the third minimum. If the lattice $L[\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3]_\leq$ had a basis which was both Minkowski-reduced and HKZ-reduced, this basis would reach the first three minima and would be of the kind $[\pm\mathbf{b}_1, \pm\mathbf{b}_2, \pm\mathbf{b}_3]_\leq$, which contradicts the fact that $[\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3]_\leq$ is not HKZ-reduced. □

2.3 Voronoï Cell and Voronoï Vectors

This subsection is useful for the local approach of Sections 8 and 9 and can be disregarded by the reader interested only in the global approach.

The *Voronoï cell* [Voronoï 1908] of a lattice $L = L[\mathbf{b}_1, \ldots, \mathbf{b}_d]_{\leq}$, denoted by $\mathrm{Vor}(\mathbf{b}_1, \ldots, \mathbf{b}_d)$, is the set of vectors $\mathbf{x}$ in the linear span of L that are closer to $\mathbf{0}$ than to any other lattice vector: for all $\mathbf{v} \in L$, we have $\|\mathbf{x} - \mathbf{v}\| \geq \|\mathbf{x}\|$, that is $\|\mathbf{v}\|^2 \geq 2\langle \mathbf{v}, \mathbf{x} \rangle$. The Voronoï cell is a finite polytope that tiles the linear span of L by translations by lattice vectors. We extend the notation $\mathrm{Vor}(\mathbf{b}_1, \ldots, \mathbf{b}_d)$ to the case where the first vectors may be zero (the remaining vectors being linearly independent): $\mathrm{Vor}(\mathbf{b}_1, \ldots, \mathbf{b}_d)$ denotes the Voronoï cell of the lattice spanned by the non-zero $\mathbf{b}_i$'s. A vector $\mathbf{v} \in L$ is called a *Voronoï vector* if the vector $\mathbf{v}/2$ belongs to the Voronoï cell (in which case the vector $\mathbf{v}/2$ will be on the boundary of the Voronoï cell). A vector $\mathbf{v} \in L$ is a *strict Voronoï vector* if $\mathbf{v}/2$ is contained in the interior of a $(d-1)$-dimensional facet of the Voronoï cell. A classical result states that Voronoï vectors correspond to the minima of the cosets of $L/2L$. We say that $(x_1, \ldots, x_d) \in \mathbb{Z}^d$ is a *possible Voronoï coord* (respectively *possible strict Voronoï coord*) if there exists a Minkowski-reduced basis $[\mathbf{b}_1, \ldots, \mathbf{b}_d]_{\leq}$ such that $x_1\mathbf{b}_1 + \ldots + x_d\mathbf{b}_d$ is a Voronoï vector (respectively strict Voronoï vector). In his PhD thesis, Tammela [1973] listed the possible strict Voronoï coords up to dimension 6. We will notice later that the set of possible Voronoï coords is strictly larger than the set of possible strict Voronoï coords.

THEOREM 2.3.1 [TAMMELA 1973; STOGRIN 1977]. *Let $d \leq 6$. The possible strict Voronoï coords in dimension d are the possible Voronoï coordinates in dimension $d-1$ and the d-tuples $(x_1, \ldots, x_d)$ such that there exists a permutation σ of $[\![1, d]\!]$ such that $(|x_{\sigma(1)}|, \ldots, |x_{\sigma(d)}|)$ appears in the d-th block of the table below:*

1				
1	*1*			
1	*1*	*1*		
1	*1*	*1*	*1*	
1	*1*	*1*	*2*	
1	*1*	*1*	*1*	*1*
1	*1*	*1*	*1*	*2*
1	*1*	*1*	*2*	*2*
1	*1*	*1*	*2*	*3*

1	*1*	*1*	*1*	*1*	*1*
1	*1*	*1*	*1*	*1*	*2*
1	*1*	*1*	*1*	*1*	*3*
1	*1*	*1*	*1*	*2*	*2*
1	*1*	*1*	*1*	*2*	*3*
1	*1*	*1*	*2*	*2*	*2*
1	*1*	*1*	*2*	*2*	*3*
1	*1*	*1*	*2*	*2*	*4*
1	*1*	*2*	*2*	*2*	*3*
1	*1*	*1*	*2*	*3*	*3*
1	*1*	*1*	*2*	*3*	*4*
1	*1*	*2*	*2*	*3*	*4*
1	*2*	*2*	*2*	*3*	*3*

In some parts of the article, we will deal with Voronoï coordinates with respect to other types of reduced bases: the kind of reduction considered will be clear from the context. The *covering radius* $\rho(L)$ of a lattice L is half of the diameter of the Voronoï cell. The *closest vector problem* (CVP) is a non-homogeneous version of the SVP: given a basis of a lattice and an arbitrary vector $\mathbf{x}$ of $\mathbb{R}^n$, find a

Input: A basis $[\mathbf{u}, \mathbf{v}]_{\leq}$ with its Gram matrix $G = (g_{i,j})_{1 \leq i,j \leq 2}$.
Output: A reduced basis of $L[\mathbf{u}, \mathbf{v}]$ with its Gram matrix.

1. Repeat
2. $\quad \mathbf{r} := \mathbf{v} - x\mathbf{u}$ where $x := \left\lfloor \frac{\langle \mathbf{u}, \mathbf{v} \rangle}{\|\mathbf{u}\|^2} \right\rceil$: when computing $x = \left\lfloor \frac{g_{1,2}}{g_{1,1}} \right\rceil$, also compute the remainder $y = g_{1,2} - x g_{1,1}$ of the centered Euclidean division.
3. $\quad \mathbf{v} := \mathbf{u}$,
4. $\quad \mathbf{u} := \mathbf{r}$,
5. $\quad$ Update the Gram matrix of $(\mathbf{u}, \mathbf{v})$ as follows: swap $g_{2,2}$ and $g_{1,1}$; then let $g_{1,2} := y$ and $g_{1,1} := g_{1,1} - x(y + g_{1,2})$.
6. Until $\|\mathbf{u}\| \geq \|\mathbf{v}\|$.
7. Return $[\mathbf{v}, \mathbf{u}]_{\leq}$ and its Gram matrix (setting $g_{2,1} = g_{1,2}$).

Fig. 2. Lagrange's algorithm.

lattice vector $\mathbf{v}$ minimizing the distance $\|\mathbf{v} - \mathbf{x}\|$. In other words, if $\mathbf{y}$ denotes the orthogonal projection of the vector $\mathbf{x}$ onto the linear span of L, the goal is to find $\mathbf{v} \in L$ such that $\mathbf{y} - \mathbf{v}$ belongs to the Voronoï cell of L.

We have seen that if $[\mathbf{b}_1, \ldots, \mathbf{b}_d]_{\leq}$ is Minkowski-reduced, then the Voronoï coordinates are confined. There is a result due to Delone and Sandakova (see [Delone and Sandakova 1961; Stogrin 1977]) claiming a stronger statement: if the basis is reduced, then the (real) coordinates towards the basis vectors of any point of the Voronoï cell are bounded. This result holds in any dimension and for different types of basis reductions, but the following is sufficient for our needs:

THEOREM 2.3.2. *The following statements hold:*

(1) *Let* $[\mathbf{b}_1, \mathbf{b}_2]_{\leq}$ *be a Minkowski-reduced basis and* $\mathbf{u} \in \mathrm{Vor}(\mathbf{b}_1, \mathbf{b}_2)$. *Write* $\mathbf{u} = x\mathbf{b}_1 + y\mathbf{b}_2$. *Then* $|x| < 3/4$ *and* $|y| \leq 2/3$.

(2) *Let* $[\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3]_{\leq}$ *be a Minkowski-reduced basis and* $\mathbf{u} \in \mathrm{Vor}(\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3)$. *Write* $\mathbf{u} = x\mathbf{b}_1 + y\mathbf{b}_2 + z\mathbf{b}_3$. *Then* $|x| < 3/2, |y| \leq 4/3$ *and* $|z| \leq 1$.

3. TWO CLASSICAL ANALYZES OF LAGRANGE'S ALGORITHM

Lagrange's algorithm – described in Figure 2 – can be seen as a two-dimensional generalization of the centered Euclidean algorithm.

At Step 2 of each loop iteration, the vector $\mathbf{u}$ is shorter than the vector $\mathbf{v}$, and one would like to shorten $\mathbf{v}$, while preserving the fact that $[\mathbf{u}, \mathbf{v}]$ is a lattice basis. This can be achieved by subtracting from $\mathbf{v}$ a multiple $x\mathbf{u}$ of $\mathbf{u}$, because such a transformation is unimodular. The optimal choice (to make the norm of the vector $\mathbf{v}$ decrease as much as possible for this loop iteration) is when $x\mathbf{u}$ is the closest vector to $\mathbf{v}$, in the one-dimensional lattice spanned by $\mathbf{u}$. This gives rise to $x := \left\lfloor \frac{\langle \mathbf{u}, \mathbf{v} \rangle}{\|\mathbf{u}\|^2} \right\rceil$. In other words, we size-reduce the basis $[\mathbf{u}, \mathbf{v}]$. The values $\langle \mathbf{u}, \mathbf{v} \rangle$ and $\|\mathbf{u}\|^2$ are extracted from $G(\mathbf{u}, \mathbf{v})$, which is updated efficiently at Step 5 of each loop iteration. Indeed, at the beginning of the loop iteration, the Gram matrix

is $\begin{pmatrix} \|\mathbf{u}\|^2 & \langle \mathbf{u}, \mathbf{v} \rangle \\ \langle \mathbf{u}, \mathbf{v} \rangle & \|\mathbf{v}\|^2 \end{pmatrix}$, whereas at the end of the iteration it becomes:

$$\begin{pmatrix} \|\mathbf{v}\|^2 - 2x\langle \mathbf{u}, \mathbf{v} \rangle + x^2\|\mathbf{u}\|^2 & \langle \mathbf{u}, \mathbf{v} \rangle - x\|\mathbf{u}\|^2 \\ \langle \mathbf{u}, \mathbf{v} \rangle - x\|\mathbf{u}\|^2 & \|\mathbf{u}\|^2 \end{pmatrix}.$$

The analysis of Lagrange's algorithm is summarized by the following classical result:

THEOREM 3.0.3. *Given as input any basis $[\mathbf{u}, \mathbf{v}]_{\leq}$ of a lattice L with its Gram matrix, Lagrange's algorithm described in Fig. 2 outputs a Minkowski-reduced basis of the lattice L in time $O(\log \|\mathbf{v}\| \cdot [1 + \log \|\mathbf{v}\| - \log \lambda_1(L)])$.*

Note that if the Gram matrix of $[\mathbf{u}, \mathbf{v}]_{\leq}$ is not given, then it can be computed in time $O(\log^2 \|\mathbf{v}\|)$, so the running time of Lagrange's algorithm becomes $O(\log \|\mathbf{v}\| \cdot [1 + \log \|\mathbf{v}\|])$, which is still quadratic. Since computing the Gram matrix is not cheap, Lagrange's algorithm must update the Gram matrix in an efficient way, as done in Step 5.

Theorem 3.0.3 is not trivial to prove. It is not even clear *a priori* why Lagrange's algorithm would output a Minkowski-reduced basis. The correctness statement of the theorem comes from Minkowski's conditions in dimension two, that is Theorem 2.2.2. Here, we give two different approaches showing that Lagrange's algorithm has a quadratic bit complexity, a global analysis and a local analysis. The main goal of this paper is to generalize both analyzes to higher dimensions.

In dimension two, the main difficulty is to prove that the total number of loop iterations is $O(1 + \log \|\mathbf{v}\| - \log \lambda_1(L))$, where $\mathbf{v}$ is the initial second basis vector. We will first show this with the global approach, then with the local approach. Finally, we will deduce the quadratic bit-complexity.

3.1 The Global Analysis of Lagrange's Algorithm

The global analysis of Lagrange's algorithm can be found in [Vallée 1991] and [Akhavi 2000], where a weaker version of Theorem 3.0.3 was proved with a cubic (and not quadratic) bit-complexity. In this approach, we split the loop iterations of the algorithm into two phases: a first phase with $O(1 + \log \|\mathbf{v}\| - \log \lambda_1(L))$ loop iterations, and a second phase with $O(1)$ loop iterations.

To do so, let η such that $0 < \eta < 1$. We define the first phase as all the first consecutive loop iterations such that $\mathbf{r}$ (defined at Step 2) is at least $1 + \eta$ shorter than the current $\mathbf{v}$. Thus, the product of the lengths of the basis vectors decreases at least by a factor $1 + \eta$ at each loop iteration. Since this product is always $\geq \lambda_1(L)^2$, it follows that the number of loop iterations of the first phase is $O(1 + \log \|\mathbf{v}\| - \log \lambda_1(L))$.

It remains to prove that the second phase has $O(1)$ loop iterations, independently of the lattice. After the first phase, either the algorithm terminates in which case we are done, or during the last loop iteration of the first phase, the triplet $(\mathbf{u}, \mathbf{v}, \mathbf{r})$ satisfies right after Step 2:

$$\|\mathbf{r}\| < \|\mathbf{u}\| \leq \|\mathbf{v}\| \leq (1 + \eta)\|\mathbf{r}\|.$$

We show that the basis $[\mathbf{u}, \mathbf{v}]_{\leq}$ has bounded orthogonality-defect. Let $\mathbf{v}^* = \mathbf{v} - \frac{\langle \mathbf{u}, \mathbf{v} \rangle}{\|\mathbf{u}\|^2}\mathbf{u}$ be the component of $\mathbf{v}$ orthogonal to $\mathbf{u}$. Then $\|\mathbf{r}\|^2 \leq \|\mathbf{v}^*\|^2 + \|\mathbf{u}\|^2/4$

because $[\mathbf{u}, \mathbf{r}]$ is size-reduced. Since $\|\mathbf{u}\| \leq \|\mathbf{v}\| \leq (1+\eta)\|\mathbf{r}\|$, this implies that:

$$\|\mathbf{v}^*\|^2 \geq \left(\frac{1}{(1+\eta)^2} - \frac{1}{4}\right) \cdot \|\mathbf{v}\|^2,$$

where $1/(1+\eta)^2 - 1/4 > 0$ since $0 < \eta < 1$. It follows that $[\mathbf{u}, \mathbf{v}]_{\leq}$ has bounded orthogonality-defect, namely:

$$\delta_{\perp}(\mathbf{u}, \mathbf{v}) = \frac{\|\mathbf{v}\|}{\|\mathbf{v}^*\|} \leq 1/\sqrt{\frac{1}{(1+\eta)^2} - \frac{1}{4}}.$$

This implies that the second phase has $O(1)$ loop iterations, where the constant is independent of the lattice. Indeed, because the algorithm is greedy, each new vector "$\mathbf{r}_i$" created during each Step 2 of the second phase cannot be longer than $\mathbf{u}$. But the number of lattice vectors $\mathbf{w} \in L$ such that $\|\mathbf{w}\| \leq \|\mathbf{u}\|$ is $O(1)$. To see this, write $\mathbf{w}$ as $\mathbf{w} = w_1\mathbf{u} + w_2\mathbf{v}$ where $w_1, w_2 \in \mathbb{Z}$. Since $|\langle \mathbf{w}, \mathbf{v}^* \rangle| \leq \|\mathbf{v}\|^2$, it follows that $|w_2| \leq \|\mathbf{v}\|^2/\|\mathbf{v}^*\|^2 = \delta_{\perp}(\mathbf{u}, \mathbf{v})^2$. So the integer w_2 has only $O(1)$ possible values: note that if η is chosen sufficiently small, we can even ensure $\delta_{\perp}(\mathbf{u}, \mathbf{v})^2 < 2$ and therefore $|w_2| \leq 1$. And for each value of w_2, the number of possibilities for the integer w_1 is at most two.

3.2 The Local Analysis of Lagrange's Algorithm

We provide another proof of the classical result that Lagrange's algorithm has quadratic complexity. Compared to other proofs, our local method closely resembles the recent one of Semaev [2001], itself relatively different from [Akhavi and Moreira dos Santos 2004; Kaib and Schnorr 1996; Lagarias 1980; Vallée 1991]. The analysis is not optimal (as opposed to [Vallée 1991]) but its basic strategy can be extended up to dimension four. This strategy gives more information on the behavior of the algorithm. Consider the value of x at Step 2:

—If $x = 0$, this must be the last iteration of the loop.

—If $|x| = 1$, there are two cases:
  —If $\|\mathbf{v} - x\mathbf{u}\| \geq \|\mathbf{u}\|$, then this is the last loop iteration.
  —Otherwise we have $\|\mathbf{u} - x\mathbf{v}\| < \|\mathbf{u}\|$, which means that $\mathbf{u}$ can be shortened with the help of $\mathbf{v}$. This can only happen if this is the first loop iteration, because of the greedy strategy: the vector $\mathbf{u}$ is the former vector $\mathbf{v}$.

—Otherwise $|x| \geq 2$, which implies that $x\mathbf{u}$ is not a Voronoï vector of the lattice spanned by $\mathbf{u}$. Intuitively, this means that $x\mathbf{u}$ is far from $\mathrm{Vor}(\mathbf{u})$, so that $\mathbf{v} - x\mathbf{u}$ is considerably shorter than $\mathbf{v}$. More precisely, if $\mathbf{v}^*$ denotes again the component of the vector $\mathbf{v}$ that is orthogonal to $\mathbf{u}$, we have $\|\mathbf{v}\|^2 > 3\|\mathbf{v} - x\mathbf{u}\|^2$ if this is not the last loop iteration. Indeed, recall that $\mathbf{v} = \frac{\langle \mathbf{v}, \mathbf{u} \rangle}{\|\mathbf{u}\|^2}\mathbf{u} + \mathbf{v}^*$. Since $x = \left\lfloor \frac{\langle \mathbf{v}, \mathbf{u} \rangle}{\|\mathbf{u}\|^2} \right\rceil$ is ≥ 2, one has $\|\mathbf{v}\|^2 \geq (3/2)^2\|\mathbf{u}\|^2 + \|\mathbf{v}^*\|^2$. Then since $\mathbf{v} - x\mathbf{u} = \left(\frac{\langle \mathbf{v}, \mathbf{u} \rangle}{\|\mathbf{u}\|^2} - \left\lfloor \frac{\langle \mathbf{v}, \mathbf{u} \rangle}{\|\mathbf{u}\|^2} \right\rceil\right)\mathbf{u} + \mathbf{v}^*$, one has $\|\mathbf{v}\|^2 \geq 2\|\mathbf{u}\|^2 + \|\mathbf{v} - x\mathbf{u}\|^2$, which is greater than $3\|\mathbf{v} - x\mathbf{u}\|^2$ provided that this is not the last loop iteration.

This shows that the product of the norms of the basis vectors decreases by a multiplicative factor of at least $\sqrt{3}$ at each loop iteration except possibly the

first and last ones. Thus, the number τ of loop iterations is upper bounded by $O(1 + \log \|\mathbf{v}\| - \log \lambda_1(L))$.

3.3 Quadratic Bit-Complexity

We proved in two different ways that the total number of loop iterations is $O(1 + \log \|\mathbf{v}\| - \log \lambda_1(L))$. To complete the proof of Theorem 3.0.3, it remains to carefully analyze the cost of each Step 2 and Step 5. Consider first the cost of each Step 2, that is, the computation of the pair (x, y) by a centered Euclidean division of $\langle \mathbf{u}, \mathbf{v} \rangle$ by $\|\mathbf{u}\|^2$. Since $\frac{|\langle \mathbf{u}, \mathbf{v} \rangle|}{\|\mathbf{u}\|^2} \leq \frac{\|\mathbf{v}\|}{\|\mathbf{u}\|}$ and $\|\mathbf{u}\| \leq \|\mathbf{v}\|$, the bit complexity of Step 2 is $O(\log \|\mathbf{v}\| \cdot [1 + \log \|\mathbf{v}\| - \log \|\mathbf{u}\|])$. For Step 5, the most expensive operation is the multiplication $x(y + g_{1,2})$. Since $|x| \leq 1/2 + \|\mathbf{v}\|/\|\mathbf{u}\|$ and $|y + g_{1,2}| \leq \|\mathbf{u}\|^2 + |\langle \mathbf{u}, \mathbf{v} \rangle| \leq 2\|\mathbf{v}\|^2\|$, the bit complexity of Step 5 is $O(\log \|\mathbf{v}\| \cdot [1 + \log \|\mathbf{v}\| - \log \|\mathbf{u}\|])$ like Step 2.

If we denote by $\mathbf{u}_i$ and $\mathbf{v}_i$ the values of $\mathbf{u}$ and $\mathbf{v}$ at the i-th iteration, then $\mathbf{v}_{i+1} = \mathbf{u}_i$ and we obtain that the bit complexity of Lagrange's algorithm is bounded by:

$$\begin{aligned} O(\sum_{i=1}^{\tau} \log \|\mathbf{v}_i\| \cdot [1 + \log \|\mathbf{v}_i\| \ - \ \log \|\mathbf{u}_i\|]) & \\ = \ O(\log \|\mathbf{v}\| \cdot \sum_{i=1}^{\tau} [1 + \log \|\mathbf{v}_i\| - \log \|\mathbf{v}_{i+1}\|]) & \\ = \ O(\log \|\mathbf{v}\| \cdot [\tau + \log \|\mathbf{v}\| - \log \lambda_1(L)]), & \end{aligned}$$

where $\tau = O(1 + \log \|\mathbf{v}\| - \log \lambda_1)$ is the total number of loop iterations. This completes the proof of Theorem 3.0.3.

4. A GREEDY GENERALIZATION OF LAGRANGE'S ALGORITHM

In the previous section, we viewed Lagrange's algorithm as a greedy algorithm based on the one-dimensional CVP. It suggests a natural generalization to arbitrary dimension that we call the greedy reduction algorithm. We study properties of the bases output by the greedy algorithm by defining a new type of reduction and comparing it to Minkowski's reduction.

4.1 The Greedy Reduction Algorithm

Lagrange's algorithm suggests the general greedy algorithm described in Figure 3, which uses reduction and closest vectors in dimension $d - 1$ to reduce bases in dimension d. We make a few simple remarks on the algorithm. If the Gram matrix is not given, we may compute it in time $O(\log^2 \|\mathbf{b}_d\|)$ for a fixed dimension d, at the beginning of the algorithm. Step 3 is easy: if this is the first iteration of the loop, the basis is already ordered; otherwise, $[\mathbf{b}_1, \ldots, \mathbf{b}_{d-1}]$ is already ordered, and only $\mathbf{b}_d$ has to be inserted among $\mathbf{b}_1, \ldots, \mathbf{b}_{d-1}$. At Step 4, the greedy algorithm calls itself recursively in dimension $d - 1$: the Gram matrix $G(\mathbf{b}_1, \ldots, \mathbf{b}_{d-1})$ does not need to be computed before calling the algorithm, since $G(\mathbf{b}_1, \ldots, \mathbf{b}_d)$ is already known. At this point, we do not explain how Step 5 (the computation of closest vectors) is performed: of course, Kannan's closest vector algorithms [Kannan 1983] could be used but they do not seem to suffice to prove a quadratic bit complexity of the greedy algorithm. We will describe in Section 5 a tailored closest vector algorithm that allows us to prove this complexity bound. And this closest vector algorithm

Name: Greedy$(\mathbf{b}_1, \ldots, \mathbf{b}_d)$.
Input: A basis $[\mathbf{b}_1, \ldots, \mathbf{b}_d]_{\leq}$ with its Gram matrix $G = (g_i, j)_{1 \leq i,j \leq d}$.
Output: An ordered basis of $L[\mathbf{b}_1, \ldots, \mathbf{b}_d]$ with its Gram matrix.

1. If $d = 1$, return $\mathbf{b}_1$.
2. Repeat
3. Sort $(\mathbf{b}_1, \ldots, \mathbf{b}_d)$ by increasing lengths and update the Gram matrix,
4. $[\mathbf{b}_1, \ldots, \mathbf{b}_{d-1}]_{\leq} :=$ Greedy$(\mathbf{b}_1, \ldots, \mathbf{b}_{d-1})$,
5. Compute a vector $\mathbf{c} \in L[\mathbf{b}_1, \ldots, \mathbf{b}_{d-1}]$ closest to $\mathbf{b}_d$,
6. $\mathbf{b}_d := \mathbf{b}_d - \mathbf{c}$ and update the Gram matrix efficiently,
7. Until $\|\mathbf{b}_d\| \geq \|\mathbf{b}_{d-1}\|$.
8. Return $[\mathbf{b}_1, \ldots, \mathbf{b}_d]_{\leq}$ and its Gram matrix.

Fig. 3. The (recursive) greedy lattice basis reduction algorithm in dimension d.

will also efficiently update the Gram matrix, as required by Step 6: a naive update of the Gram matrix would not be enough to ensure a quadratic bit complexity. Notice that for $d = 2$, the greedy algorithm is exactly Lagrange's algorithm. From a geometrical point of view, the goal of Steps 5 and 6 is to make sure that the orthogonal projection of the vector $\mathbf{b}_d$ onto the lattice spanned by $[\mathbf{b}_1, \ldots, \mathbf{b}_{d-1}]_{\leq}$ lies in the Voronoï cell of that sublattice.

An easy proof by induction on d shows that the algorithm terminates. Indeed, the new vector $\mathbf{b}_d$ of Step 6 is strictly shorter than $\mathbf{b}_{d-1}$ if the loop does not end at Step 7. Thus the product of the norms of the $\mathbf{b}_i$'s decreases strictly at each iteration of the loop that is not the last one. But for all B, the number of lattice vectors of norm less than B is finite, which completes the proof.

Although the description of the greedy algorithm is fairly simple, analyzing its complexity seems very difficult. Even the two-dimensional case of Lagrange's algorithm is not trivial.

4.2 An Iterative Description of the Greedy Algorithm

We will also use an iterative version of the greedy algorithm, described in Figure 4, and which performs exactly the same operations as the recursive version. With this alternative description, the resemblance with the usual LLL algorithm is clearer: the closest vector of Step 2 is replaced in the LLL algorithm by an approximate closest vector and the length condition of Step 4 is replaced by the so-called Lovász condition. We will use this iterative description in the bit-complexity analysis, namely in Section 7, while Sections 6 and 8 will focus on the recursive description to show that the number of loop iterations of the iterative algorithm is at most linear in the bit-size of the input.

The main result of the paper is the following:

THEOREM 4.2.1. *Let $d \leq 4$. Given as input an ordered basis $[\mathbf{b}_1, \ldots, \mathbf{b}_d]_{\leq}$ and its Gram matrix, the greedy algorithm of Figures 3 and 4 based on the closest vector algorithm of Section 5 outputs a Minkowski-reduced basis of $L[\mathbf{b}_1, \ldots, \mathbf{b}_d]$, using a number of bit operations bounded by $O(\log \|\mathbf{b}_d\| \cdot [1 + \log \|\mathbf{b}_d\| - \log \lambda_1(L)])$, where the $O()$ constant is independent of the lattice. Moreover, in dimension five, the*

Name: Iterative − Greedy($\mathbf{b}_1, \ldots, \mathbf{b}_d$).
Input: A basis $[\mathbf{b}_1, \ldots, \mathbf{b}_d]_{\leq}$ with its Gram matrix.
Output: An ordered basis of $L[\mathbf{b}_1, \ldots, \mathbf{b}_d]$ with its Gram matrix.

1. $k := 2$. While $k \leq d$, do:
2. Compute a vector $\mathbf{c} \in L[\mathbf{b}_1, \ldots, \mathbf{b}_{k-1}]$ closest to $\mathbf{b}_k$,
3. $\mathbf{b}_k := \mathbf{b}_k - \mathbf{c}$ and update the Gram matrix,
4. If $\|\mathbf{b}_k\| \geq \|\mathbf{b}_{k-1}\|$, then $k := k + 1$
5. Else insert $\mathbf{b}_k$ at his length rank k' (the vectors are sorted by increasing lengths), update the Gram matrix, $k := k' + 1$.

Fig. 4. The iterative description of the greedy algorithm.

output basis may not be Minkowski-reduced.

4.3 Greedy Reduction

Here we study some properties of the bases output by the greedy algorithm. As previously mentioned, it is not clear why Lagrange's algorithm outputs a Minkowski-reduced basis. But it is obvious that the output basis $[\mathbf{u}, \mathbf{v}]_{\leq}$ satisfies $\|\mathbf{u}\| \leq \|\mathbf{v}\| \leq \|\mathbf{v} - x\mathbf{u}\|$ for all $x \in \mathbb{Z}$. This suggests the following definition:

Definition 4.3.1. An ordered basis $[\mathbf{b}_1, \ldots, \mathbf{b}_d]_{\leq}$ is *greedy-reduced* if for all $2 \leq i \leq d$ and for all $x_1, \ldots, x_{i-1} \in \mathbb{Z}$:

$$\|\mathbf{b}_i\| \leq \|\mathbf{b}_i + x_1\mathbf{b}_1 + \ldots + x_{i-1}\mathbf{b}_{i-1}\|.$$

In other words, we have the following recursive definition: a one-dimensional basis is always greedy-reduced, and an ordered basis $[\mathbf{b}_1, \ldots, \mathbf{b}_d]_{\leq}$ is greedy-reduced if and only if $[\mathbf{b}_1, \ldots, \mathbf{b}_{d-1}]_{\leq}$ is greedy-reduced and the projection of $\mathbf{b}_d$ onto the linear span of $\mathbf{b}_1, \ldots, \mathbf{b}_{d-1}$ lies in the Voronoï cell $\mathrm{Vor}(\mathbf{b}_1, \ldots, \mathbf{b}_{d-1})$. The greedy algorithm always outputs a greedy-reduced basis and if the input basis is greedy-reduced, then the output basis will be equal to the input basis. The fact that Lagrange's algorithm outputs Minkowski-reduced bases is a particular case of the following result, which compares greedy and Minkowski reductions:

LEMMA 4.3.2. *The following statements hold:*

(*1*) *Any Minkowski-reduced basis is greedy-reduced.*

(*2*) *A basis of $d \leq 4$ vectors is Minkowski-reduced if and only if it is greedy-reduced.*

(*3*) *If $d \geq 5$, there exists a basis of d vectors that is greedy-reduced but not Minkowski-reduced.*

PROOF. The first statement follows directly from the definitions of the Minkowski and greedy reductions. The second one is obvious if one considers Theorem 2.2.2: up to dimension four the conditions involve only zeros and ones. It now remains to give a counterexample in dimension five. We consider the lattice spanned by the columns of the following basis:

$$\begin{bmatrix} 2 & 0 & 0 & 0 & 1 \\ 0 & 2 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 1 \\ 0 & 0 & 0 & 2+\varepsilon & 1+\frac{\varepsilon}{2} \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix},$$

where $\varepsilon \in \left(0, -2 + 4\frac{\sqrt{3}}{3}\right)$.

The upper bound on ε implies that $\|\mathbf{b}_1\| \leq \|\mathbf{b}_2\| \leq \|\mathbf{b}_3\| < \|\mathbf{b}_4\| < \|\mathbf{b}_5\|$. The given basis is not Minkowski-reduced because it does not reach the first four minima of the lattice: $2\mathbf{b}_5 - \mathbf{b}_4 - \mathbf{b}_3 - \mathbf{b}_2 - \mathbf{b}_1 =^t (0, 0, 0, 0, 2)$ is linearly independent with the vectors $\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3$ and is strictly shorter than the vectors $\mathbf{b}_4$ and $\mathbf{b}_5$. However, the basis is greedy-reduced: $\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \mathbf{b}_4$ are pairwise orthogonal, and the vector $\mathbf{b}_5$ cannot be longer than any linear integer combination of those four vectors added to $\mathbf{b}_5$. □

As a consequence the greedy algorithm outputs a Minkowski-reduced basis up to dimension four, thus reaching all the successive minima of the lattice. Furthermore, beyond dimension four, the greedy algorithm outputs a greedy-reduced basis that may not be Minkowski-reduced. The following lemma shows that greedy-reduced bases may considerably differ from Minkowski-reduced bases beyond dimension four:

LEMMA 4.3.3. *Let $d \geq 5$. For any $\varepsilon > 0$, there exists a lattice L and a greedy-reduced basis $[\mathbf{b}_1, \ldots, \mathbf{b}_d]_{\leq}$ of L such that $\frac{\lambda_1(L)}{\|\mathbf{b}_1\|} \leq \varepsilon$ and $\frac{\text{vol } L}{\prod_{i=1}^{d} \|\mathbf{b}_i\|} \leq \varepsilon$.*

PROOF. Consider the greedy-reduced basis spanned by the columns of the following matrix:

$$\begin{bmatrix} 2 & 0 & 0 & 0 & 1 \\ 0 & 2 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 1 \\ 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & \varepsilon \end{bmatrix},$$

where $\varepsilon > 0$ is small. Then $2\mathbf{b}_5 - \mathbf{b}_1 - \mathbf{b}_2 - \mathbf{b}_3 - \mathbf{b}_4$ is a lattice vector of length 2ε. Moreover, the vector $\mathbf{b}_1$ is of length 2, which proves the first fact. Finally, we have vol $L = 16\varepsilon$ and the product of the $\|\mathbf{b}_i\|$'s is larger than 16, which proves the second statement of the lemma. □

Such properties do not hold for Minkowski-reduced bases. The first phenomenon shows that greedy-reduced bases may be arbitrarily far from the first minimum while the second one shows that a greedy-reduced basis may be far from being orthogonal.

5. THE CLOSEST VECTOR PROBLEM IN LOW DIMENSIONS

We now explain how Steps 5 of the recursive greedy algorithm and 2 of the iterative variant can be implemented efficiently up to $d = 5$. Step 5 is trivial only when $d \leq 2$. Otherwise, notice that the $(d-1)$-dimensional basis $[\mathbf{b}_1, \ldots, \mathbf{b}_{d-1}]_{\leq}$ is greedy-reduced, and therefore Minkowski-reduced as long as $d \leq 5$. And we know the Gram matrix of $[\mathbf{b}_1, \ldots, \mathbf{b}_{d-1}, \mathbf{b}_d]_{\leq}$.

THEOREM 5.0.4. *Let $d \geq 1$ be an integer. There exists an algorithm that, given as input a Minkowski-reduced basis $[\mathbf{b}_1, \ldots, \mathbf{b}_{d-1}]_{\leq}$, a target vector $\mathbf{t}$ longer than all the $\mathbf{b}_i$'s and the Gram matrix of $[\mathbf{b}_1, \ldots, \mathbf{b}_{d-1}, \mathbf{t}]_{\leq}$, outputs a closest lattice vector $\mathbf{c}$ to $\mathbf{t}$ (in the lattice spanned by the vectors $\mathbf{b}_1, \ldots, \mathbf{b}_{d-1}$) and the Gram matrix of $(\mathbf{b}_1, \ldots, \mathbf{b}_{d-1}, \mathbf{t}-\mathbf{c})$, in time:*

$$O\left(\log \|\mathbf{t}\| \cdot [1 + \log \|\mathbf{t}\| - \log \|\mathbf{b}_\alpha\|]\right),$$

where $\alpha \in [\![1, d]\!]$ is any integer such that $[\mathbf{b}_1, \ldots, \mathbf{b}_{\alpha-1}, \mathbf{t}]_{\leq}$ is Minkowski-reduced.

The index α appearing in the statement of the theorem requires an explanation. Consider the iterative version of the greedy algorithm. The index k can increase and decrease rather arbitrarily. For a given loop iteration, the index α tells us which vectors have not changed since the last loop iteration for which the index k had the same value. Intuitively, the reason why we can make the index α appear in the statement of the theorem is that we are working in the orthogonal complement of the vectors $\mathbf{b}_1, \ldots, \mathbf{b}_{\alpha-1}$. The use of the index α is crucial. If we were using the weaker bound $O(\log \|\mathbf{t}\| \cdot [1 + \log \|\mathbf{t}\| - \log \|\mathbf{b}_1\|])$, we would not be able to prove the quadratic bit complexity of the greedy algorithm. Rather, we would obtain a cubic complexity bound. This index α is also crucial for the quadratic bit complexity of the floating-point LLL described in [Nguyen and Stehlé 2005].

Intuitively, the algorithm works as follows: an approximation of the coordinates (with respect to the $\mathbf{b}_i$'s) of the closest vector is computed using linear algebra and the approximation is then corrected by a suitable exhaustive search.

PROOF. Let $\mathbf{h}$ be the orthogonal projection of the vector $\mathbf{t}$ onto the linear span of $\mathbf{b}_1, \ldots, \mathbf{b}_{d-1}$. We do not compute $\mathbf{h}$ but introduce it to simplify the description of the algorithm. There exist $y_1, \ldots, y_{d-1} \in \mathbb{R}$ such that $\mathbf{h} = \sum_{i=1}^{d-1} y_i \mathbf{b}_i$. If $\mathbf{c} = \sum_{i=1}^{d-1} x_i \mathbf{b}_i$ is a closest vector to $\mathbf{t}$, then $\mathbf{h}-\mathbf{c}$ belongs to $\mathrm{Vor}(\mathbf{b}_1, \ldots, \mathbf{b}_{d-1})$. However, for any $C > 0$, the coordinates (with respect to any basis of orthogonality-defect $\leq C$) of any point inside the Voronoï cell can be bounded independently from the lattice (see [Stogrin 1977]). It follows that if we know an approximation of the y_i's with sufficient precision, then $\mathbf{c}$ can be derived from a $O(1)$ exhaustive search, since the coordinates $y_i - x_i$ of $\mathbf{h} - \mathbf{c}$ are bounded (the orthogonality-defect of the Minkowski-reduced basis $[\mathbf{b}_1, \ldots, \mathbf{b}_{d-1}]_{\leq}$ is bounded). This exhaustive search can be performed in time $O(\log \|\mathbf{t}\|)$ since the Gram matrix of $[\mathbf{b}_1, \ldots, \mathbf{b}_{d-1}, \mathbf{t}]_{\leq}$ is known.

To approximate the y_i's, we use basic linear algebra. Let $G = G(\mathbf{b}_1, \ldots, \mathbf{b}_{d-1})$ and $H = \left(\frac{\langle \mathbf{b}_i, \mathbf{b}_j \rangle}{\|\mathbf{b}_i\|^2}\right)_{i,j<d}$. The matrix H is exactly G, where the i-th row has been divided by $\|\mathbf{b}_i\|^2$. We have:

$$G \cdot \begin{bmatrix} y_1 \\ \vdots \\ y_{d-1} \end{bmatrix} = - \begin{bmatrix} \langle \mathbf{b}_1, \mathbf{t} \rangle \\ \vdots \\ \langle \mathbf{b}_{d-1}, \mathbf{t} \rangle \end{bmatrix}, \text{ and thus } \begin{bmatrix} y_1 \\ \vdots \\ y_{d-1} \end{bmatrix} = -H^{-1} \cdot \begin{bmatrix} \frac{\langle \mathbf{b}_1, \mathbf{t} \rangle}{\|\mathbf{b}_1\|^2} \\ \vdots \\ \frac{\langle \mathbf{b}_{d-1}, \mathbf{t} \rangle}{\|\mathbf{b}_{d-1}\|^2} \end{bmatrix}. \quad (1)$$

We use the latter formula to compute the y_i's with an absolute error $\leq 1/2$, within the expected time. Let $r = \max_i \left\lfloor \log \frac{|\langle \mathbf{b}_i, \mathbf{t} \rangle|}{\|\mathbf{b}_i\|^2} \right\rfloor$. Notice that $r = O(1 + \log \|\mathbf{t}\| -$

$\log \|\mathbf{b}_\alpha\|$), which can be obtained by bounding $\langle \mathbf{b}_i, \mathbf{t}\rangle$ depending on whether $i \geq \alpha$: if $i < \alpha$, $|\langle \mathbf{b}_i, \mathbf{t}\rangle| \leq \|\mathbf{b}_i\|^2/2$; otherwise, $|\langle \mathbf{b}_i, \mathbf{t}\rangle| \leq \|\mathbf{b}_i\|^2 \cdot \frac{\|\mathbf{t}\|}{\|\mathbf{b}_i\|} \leq \|\mathbf{b}_i\|^2 \cdot \frac{\|\mathbf{t}\|}{\|\mathbf{b}_\alpha\|}$. Notice also that the entries of H are all ≤ 1 in absolute value (because $[\mathbf{b}_1, \ldots, \mathbf{b}_{d-1}]_{\leq}$ is Minkowski-reduced and therefore pairwise Lagrange-reduced), and that $\det(H) = \frac{\det(G)}{\|\mathbf{b}_1\|^2 \ldots \|\mathbf{b}_{d-1}\|^2}$ is lower bounded by some universal constant (because the orthogonality-defect of the Minkowski-reduced basis $[\mathbf{b}_1, \ldots, \mathbf{b}_{d-1}]_{\leq}$ is bounded). It follows that one can compute the entries of the matrix H^{-1} with an absolute precision of $\Theta(r)$ bits, within $O(r^2)$ binary operations, for example by computing $\Theta(r)$-bit long approximations to both the determinant and the comatrix of H (though not efficient, it can be done with Leibniz formula). One eventually derives the y_i's with an absolute error $\leq 1/2$, by a matrix-vector multiplication involving $\Theta(r)$ bit long approximations to rational numbers.

From Equation (1) and the discussion above on the quantities $\frac{\langle \mathbf{b}_i, \mathbf{t}\rangle}{\|\mathbf{b}_i\|^2}$, we derive that for any i, the integer $|x_i| \leq |y_i| + O(1)$ is $O(1 + \log \|\mathbf{t}\| - \log \|\mathbf{b}_\alpha\|)$ bit long. We now explicit the computation of the Gram matrix of $(\mathbf{b}_1, \ldots, \mathbf{b}_{d-1}, \mathbf{t} - \mathbf{c})$ from the Gram matrix of $(\mathbf{b}_1, \ldots, \mathbf{b}_{d-1}, \mathbf{t})$. Only the entries from the last row (and last column, by symmetry) are changing. For the non-diagonal entries of the last row, we have:

$$\langle \mathbf{b}_i, \mathbf{t} - \mathbf{c}\rangle = \langle \mathbf{b}_i, \mathbf{t}\rangle - \sum_{j<d} x_j \langle \mathbf{b}_i, \mathbf{b}_j\rangle.$$

Because of the length upper bound on the x_j's, this computation can be performed within the expected time. The same holds for the diagonal entry, by using the equality:

$$\|\mathbf{t} - \mathbf{c}\|^2 = \|\mathbf{t}\|^2 + \sum_{i<d} x_i^2 \|\mathbf{b}_i\|^2 + 2 \sum_{i<j<d} x_i x_j \langle \mathbf{b}_i, \mathbf{b}_j\rangle - 2 \sum_{i<d} x_i \langle \mathbf{b}_i, \mathbf{t}\rangle.$$

□

It can be proved that this result remains valid when replacing Minkowski reduction by any kind of basis reduction that ensures a bounded orthogonality-defect, for example LLL-reduction. Besides, notice that Theorem 2.3.2 can be used to make Theorem 5.0.4 more practical: the bounds given in Theorem 2.3.2 help decreasing drastically the cost of the exhaustive search following the linear algebra step.

6. THE GLOBAL APPROACH

In this section we describe the global approach to prove that there is a linear number of loop iterations during the execution of the iterative version of the greedy algorithm (as described in Figure 4). The goal of this global approach is to prove Theorem 6.0.5. The proof of this last theorem can be replaced by another one that we describe in Sections 8 and 9. We call this alternative proof the local approach. In both cases, the complexity analysis of the greedy algorithm finishes with Section 7. This last section makes use of the local and global approaches only through Theorem 6.0.5.

In the present section, we describe a global analysis proving that the number of loop iterations of the iterative greedy algorithm is at most linear in $\log \|\mathbf{b}_d\|$, as

long as $d \leq 4$. More precisely, we show that:

THEOREM 6.0.5. *Let $d \leq 4$. Let $\mathbf{b}_1, \ldots, \mathbf{b}_d$ be linearly independent vectors. The number of loop iterations performed during the execution of the iterative greedy algorithm of Figure 4 given as input $\mathbf{b}_1, \ldots, \mathbf{b}_d$ is bounded by $O(1+\log \|\mathbf{b}_d\| - \log \lambda_1)$, where $\lambda_1 = \lambda_1(L[\mathbf{b}_1, \ldots, \mathbf{b}_d])$.*

To obtain this result, we show that in any dimension $d \leq 4$, there are at most $N = O(1)$ consecutive loop iterations of the recursive algorithm described in Figure 3 without a significant length decrease, i.e., without a decrease of the product of the lengths of the basis vectors by a factor higher than K for some constant $K > 1$. This fact implies that there cannot be more than $N^d = O(1)$ consecutive loop iterations of the iterative algorithm without a decrease of the product of the lengths of the basis vectors by a factor higher than K. This immediately implies Theorem 6.0.5. More precisely, we prove the following:

THEOREM 6.0.6. *Let $d \leq 4$. There exist two constants $K > 1, N$ such that in any N consecutive loop iterations of the d-dimensional recursive greedy algorithm of Figure 3, the lengths of the current basis vectors decreases by at least a factor K.*

Our proof of Theorem 6.0.6 is as follows. We first define two different phases in the execution of the recursive d-dimensional greedy algorithm. In the first phase, when a vector is shortened, its length decreases by at least a factor of $1 + \eta$ for some $\eta > 0$ to be fixed later. All these steps are good steps since they make the product of the lengths of the basis vectors decrease significantly. In the second phase, the lengths of the vectors are not decreasing much, but we will show that once we enter this phase, the basis is nearly orthogonal and there remain very few loop iterations.

6.1 Two Phases in the Recursive Greedy Algorithm

We divide the successive loop iterations of the recursive greedy algorithm into two phases: the η-phase and the remaining phase. The execution of the algorithm starts with the η-phase. The loop iterations are in the η-phase as long as the new vector $\mathbf{b}_d$ of Step 6 is at least $(1 + \eta)$ times shorter than the previous $\mathbf{b}_d$. Once there is no more a large length decrease, all the remaining loop iterations are in the remaining phase. More precisely, the η-phase is exactly made of the loop iterations of the η-greedy algorithm of Figure 5, which simulates the beginning of the execution of the greedy algorithm. The remaining phase corresponds to the execution of the recursive greedy algorithm of Figure 3 given as input the output basis of the η-greedy algorithm.

It is clear that all loop iterations in the η-phase are good loop iterations: the product of the lengths of the basis vectors decreases by a factor higher than $1 + \eta$. Moreover, if $d \leq 4$, when the execution of the algorithm enters the remaining phase, the basis has a bounded orthogonality defect:

LEMMA 6.1.1. *Let $d \leq 4$ and $\eta \in \left(0, \sqrt{\frac{4}{3}} - 1\right)$. Suppose the basis $[\mathbf{b}_1, \ldots, \mathbf{b}_d]_{\leq}$ is invariant by the η-greedy algorithm of Figure 5. Then for any $k \leq d$, we have:*

$$\|\mathbf{b}_k^*\|^2 \geq \left(\frac{1}{(1+\eta)^2} + \frac{1-k}{4}\right) \cdot \|\mathbf{b}_k\|^2.$$

Input: A basis $[\mathbf{b}_1, \ldots, \mathbf{b}_d]_\leq$ with its Gram matrix.
Output: An ordered basis of $L[\mathbf{b}_1, \ldots, \mathbf{b}_d]$ with its Gram matrix.

1. If $d = 1$, return $\mathbf{b}_1$.
2. Sort $(\mathbf{b}_1, \ldots, \mathbf{b}_d)$ by increasing lengths and update the Gram matrix,
3. $[\mathbf{b}_1, \ldots, \mathbf{b}_{d-1}]_\leq := \mathsf{Greedy}(\mathbf{b}_1, \ldots, \mathbf{b}_{d-1})$,
4. Compute a vector $\mathbf{c} \in L[\mathbf{b}_1, \ldots, \mathbf{b}_{d-1}]$ closest to $\mathbf{b}_d$,
5. $\mathbf{b}'_d := \mathbf{b}_d - \mathbf{c}$,
6. If $(1+\eta) \cdot \|\mathbf{b}'_d\| \geq \|\mathbf{b}_d\|$, goto Step 8.
7. Else, $\mathbf{b}_d := \mathbf{b}'_d$, update the Gram matrix and goto Step 2.
8. Return $[\mathbf{b}_1, \ldots, \mathbf{b}_d]_\leq$ and its Gram matrix.

Fig. 5. The η-greedy lattice basis reduction algorithm in dimension d.

Notice that if $k \leq 4$, then $\frac{1}{(1+\eta)^2} + \frac{1-k}{4} > 0$.

PROOF. Let $k \leq d$ and $\mathbf{b}'_k = \mathbf{b}_k - \mathbf{c}$ where $\mathbf{c}$ is a vector closest to $\mathbf{b}_k$ in the lattice $L[\mathbf{b}_1, \ldots, \mathbf{b}_{k-1}]$. We write $\mathbf{b}'_k = \mathbf{b}^*_k + \mathbf{b}^-_k$, where $\mathbf{b}^-_k$ is in the linear span of $(\mathbf{b}_1, \ldots, \mathbf{b}_{k-1})$. Since the vector $\mathbf{b}'_k$ cannot be shortened by adding to it an integral linear combination of the vectors $\mathbf{b}_1, \ldots, \mathbf{b}_{k-1}$, we know that:

$$\|\mathbf{b}^-_k\|^2 \leq \rho(\mathbf{b}_1, \ldots, \mathbf{b}_{k-1})^2 \leq \frac{k-1}{4} \max_{i<k} \|\mathbf{b}^*_i\|^2 \leq \frac{k-1}{4} \|\mathbf{b}_{k-1}\|^2 \leq \frac{k-1}{4} \|\mathbf{b}_k\|^2,$$

where $\rho(\mathbf{b}_1, \ldots, \mathbf{b}_{k-1})$ is the covering radius of the lattice L_{k-1} spanned by the vectors $\mathbf{b}_1, \ldots, \mathbf{b}_{k-1}$. We used the fact that any vector $\mathbf{t}$ of the span of $\mathbf{b}_1, \ldots, \mathbf{b}_{k-1}$ is at most $\frac{1}{2}\sqrt{\sum_{i<k} \|\mathbf{b}^*_i\|^2}$ away from L_{k-1}: all coefficients of $\mathbf{t}$ when written as a linear combination of the $\mathbf{b}^*_i$'s can be made smaller than $1/2$ in absolute value by subtracting from it a well-chosen integer linear combination of the $\mathbf{b}_i$'s. From the Pythagorean theorem, we derive that:

$$\begin{aligned} \|\mathbf{b}_k\|^2 \leq (1+\eta)^2 \cdot \|\mathbf{b}'_k\|^2 &\leq (1+\eta)^2 \cdot (\|\mathbf{b}^*_k\|^2 + \|\mathbf{b}^-_k\|^2) \\ &\leq (1+\eta)^2 \cdot \left(\|\mathbf{b}^*_k\|^2 + \frac{k-1}{4} \|\mathbf{b}_k\|^2 \right), \end{aligned}$$

which gives the result. □

6.2 The Greedy Algorithm with a Nearly Orthogonal Basis

We now prove that when the $\|\mathbf{b}^*_i\|/\|\mathbf{b}_i\|$'s are all lower-bounded (i.e., the orthogonality defect is bounded), then the number of loop iterations of the greedy algorithm is $O(1)$.

LEMMA 6.2.1. *Let $D \geq 2$ and $C > 0$. There exists a constant N such that for all $d \leq D$, and any basis $[\mathbf{b}_1, \ldots, \mathbf{b}_d]_\leq$ satisfying $\prod_{i=1}^{d} \frac{\|\mathbf{b}^*_i\|}{\|\mathbf{b}_i\|} \geq C$, the recursive greedy algorithm, when given as input $\mathbf{b}_1, \ldots, \mathbf{b}_d$, terminates in at most N loop iterations.*

PROOF. Since for any $i \leq d$, we have $\|\mathbf{b}^*_i\| \leq \|\mathbf{b}_i\|$, we also have $\frac{\|\mathbf{b}^*_i\|}{\|\mathbf{b}_i\|} \geq C$ for any $i \leq d$. As a consequence, if the initial basis satisfies $\prod_{i=1}^{d} \frac{\|\mathbf{b}^*_i\|}{\|\mathbf{b}_i\|} \geq C$, since the numerator is constant (it is the determinant of the lattice) and the denominator

decreases, then all the bases appearing in the execution of the greedy algorithm satisfy this condition. Any vector $\mathbf{b}_i$ appearing during the execution of the algorithm satisfies $\frac{\|\mathbf{b}_i^*\|}{\|\mathbf{b}_i\|} \geq C$.

We define $X_i = \{(x_i, \ldots, x_d), \exists (x_1, \ldots, x_{i-1}) \in \mathbb{Z}^{i-1}, \|\sum_j x_j \mathbf{b}_j\| \leq \|\mathbf{b}_i\|\}$ for $i \leq d$. We prove that $|X_i| \leq (1 + 2/C)^{d-i+1}$ by decreasing induction on i. Let $\mathbf{b} = x_1\mathbf{b}_1 + \ldots + x_d\mathbf{b}_d$ with $\|\mathbf{b}\| \leq \|\mathbf{b}_d\|$. By considering the component of the vector $\mathbf{b}$ on $\mathbf{b}_d^*$, we have that $|x_d| \leq 1/C$. Suppose now that we want to prove the fact for some $i < d$. Let $\mathbf{b} = x_1\mathbf{b}_1 + \ldots + x_d\mathbf{b}_d$ with $\|\mathbf{b}\| \leq \|\mathbf{b}_i\|$. Since the basis is ordered, we have $\|\mathbf{b}\| \leq \|\mathbf{b}_{i+1}\|$, which gives, by using the induction hypothesis, that $(x_{i+1}, \ldots, x_d)$ belongs to a finite set. Moreover, by taking the component of $\mathbf{b}$ on $\mathbf{b}_i^*$, we obtain that:

$$\left| x_i + \sum_{j=i+1}^{d} x_j \frac{\langle \mathbf{b}_j, \mathbf{b}_i^* \rangle}{\|\mathbf{b}_i^*\|^2} \right| \leq 1/C.$$

This gives that for any choice of $(x_{i+1}, \ldots, x_d)$, there are at most $2/C + 1$ possible values for x_i.

Consider now the execution of the greedy algorithm on such a basis: the number of times a vector shorter than $\mathbf{b}_1$ is created is bounded by $|X_1| \leq (1 + 2/C)^d$. Therefore we can subdivide the execution of the algorithm into phases in which $\mathbf{b}_1$ remains constant. Consider such a phase. Let $\mathbf{b}_1, \ldots, \mathbf{b}_d$ be the initial basis of this phase. It satisfies the condition $\prod_{i=1}^{d} \frac{\|\mathbf{b}_i^*\|}{\|\mathbf{b}_i\|} \geq C$. At most $|X_2| \leq (1+2/C)^{d-1}$ times in this phase a vector shorter than $\mathbf{b}_2$ can be created: for any $(x_2, \ldots, x_d) \in X_2$, there are at most two possibilities for x_1, because of the greedy choice in Steps 2 of the iterative greedy algorithm and 5 of the recursive greedy algorithm. This shows that we can subdivide the execution of the algorithm into $\leq 2(1 + 2/C)^{2d-1}$ phases in which both $\mathbf{b}_1$ and $\mathbf{b}_2$ are constant. By using the bound on $|X_i|$ and the finiteness of the number of solutions for a closest vector problem instantiation (this is the so-called kissing number, see [Conway and Sloane 1988]), this reasoning can be extended to subdivide the execution of the algorithm into phases in which $\mathbf{b}_1, \ldots, \mathbf{b}_i$ do not change, and we can bound the number of phases independently of the basis. The case $i = d$ gives the result. □

It follows that there are at most N loop iterations of the recursive algorithm without a decrease of the product of the lengths of the basis vectors by a factor at least $K = 1 + \eta$, where N is independent of the lattice. This implies that there are at most $N^d = O(1)$ consecutive loop iterations of the iterative algorithm without such a decrease, which completes the proof of Theorem 6.0.5.

7. QUADRATIC BIT COMPLEXITY

In this subsection we use Theorems 5.0.4 and 6.0.5 of the two previous sections to prove the quadratic bit complexity claimed in Theorem 4.2.1. To do this, we generalize the cancellation phenomenon used in the analysis of Lagrange's algorithm in Section 3.

Suppose that $d \leq 4$. We consider the iterative version of the d-dimensional greedy algorithm of Figure 4 and denote by $[\mathbf{b}_1^{(t)}, \ldots, \mathbf{b}_d^{(t)}]_{\leq}$ the current ordered ba-

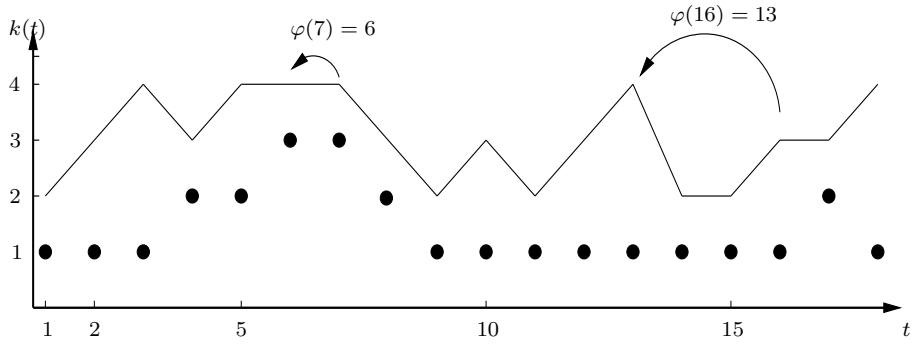

Fig. 6. A possible curve for $\kappa(t)$, with the corresponding values for $\alpha(t)$

sis at the beginning of the t-th loop iteration. Initially we have: $[\mathbf{b}_1^{(t)}, \ldots, \mathbf{b}_d^{(t)}]_{\leq} = [\mathbf{b}_1, \ldots, \mathbf{b}_d]_{\leq}$. Theorem 5.0.4 gives that the cost of the t-th loop iteration is bounded by $O\left(\log \|\mathbf{b}_d\| \cdot \left(1 + \log \left\|\mathbf{b}_{k(t)}^{(t)}\right\| - \log \left\|\mathbf{b}_{\alpha(t)}^{(t)}\right\|\right)\right)$. Theorem 6.0.5 gives that the number of loop iterations τ is bounded by $O(1 + \log \|\mathbf{b}_d\| - \log \lambda_1)$. We have two indices of interest for the cost analysis: $k(t)$ because at the t-th loop iteration, we are trying to decrease the length of $\mathbf{b}_{k(t)}^{(t)}$, and $\alpha(t)$ that we define precisely in the following lemma and that corresponds to the largest i such that none of $\mathbf{b}_1, \ldots, \mathbf{b}_i$ has been modified since the last time the index k had value $k(t)$.

Figure 6 gives a possible curve for $k(t)$ (thin continuous line) in dimension four, with the corresponding values for $\alpha(t)$ (plain dots).

LEMMA 7.0.2. *Let t be a loop iteration. Let $\varphi(t) = \max(t' < t, k(t') \geq k(t))$ if it exists and 1 otherwise, and $\alpha(t) = \min\left(k(t'), t' \in [\![\varphi(t), t-1]\!]\right) - 1$ if $k(t) \geq k(t-1)$ and $\alpha(t) = k(t) - 1$ otherwise. The cost of the t-th loop iteration of the iterative greedy algorithm is bounded by:*

$$O\left(\log \|\mathbf{b}_d\| \cdot \left[1 + \log \left\|\mathbf{b}_{k(t)}^{(t)}\right\| - \log \left\|\mathbf{b}_{\alpha(t)}^{(t)}\right\|\right]\right).$$

PROOF. Between loop iterations $\varphi(t)$ and t, the vectors $\mathbf{b}_1, \ldots, \mathbf{b}_{\alpha(t)-1}$ do not change and because of the greedy choices of the successive Steps 2 and 3, each vector $\mathbf{b}$ created during these loop iterations is such that the basis $[\mathbf{b}_1, \ldots, \mathbf{b}_{\alpha(t)-1}, \mathbf{b}]_{\leq}$ is greedy-reduced, and therefore Minkowski-reduced if $\alpha(t) \leq 4$ (because of the equivalence of greedy and Minkowski reductions up to dimension four). This includes the vector $\mathbf{b}_{k(t)}^{(t)}$. Theorem 5.0.4 gives the result because all vectors appearing during the execution of the algorithm are shorter than $\mathbf{b}_d$. □

We are to subdivide the sum of the costs of the successive loop iterations into $O(d)$ subsums according to the value of $k(t)$:

$$\sum_{t \leq \tau} \left[1 + \log \left\|\mathbf{b}_{k(t)}^{(t)}\right\| - \log \left\|\mathbf{b}_{\alpha(t)}^{(t)}\right\|\right] \leq \tau + \sum_{k=2}^{d} \sum_{t, k(t)=k} \left(\log \left\|\mathbf{b}_k^{(t)}\right\| - \log \left\|\mathbf{b}_{a(t)}^{(t)}\right\|\right).$$

For each of these subsums, we keep $k-1$ positive terms and $k-1$ negative terms,

and make the others vanish in a progressive cancellation. The crucial point to do this is the following:

LEMMA 7.0.3. *Let $k \in [\![2, d]\!]$ and $t_1 < t_2 < \ldots < t_k$ be loop iterations of the iterative greedy algorithm such that for any $j < k$, we have $k(t_j) = k$. Then there exists $j < k$ with $\left\|\mathbf{b}_{\alpha(t_j)}^{(t_j)}\right\| \geq \left\|\mathbf{b}_k^{(t_k)}\right\|$.*

PROOF. We choose $j = \max(i \leq k, \alpha(t_i) \geq i)$. Here j is well-defined because the set of indices i is non-empty (it contains 1). Since $\alpha(t_k) < k$ and $k(t_k) = k(t_{k-1}) = k$, there exists a first loop iteration $T_k \in [\![t_{k-1}, t_k - 1]\!]$ such that $k(T_k) \geq k \geq k(T_k + 1)$. Because for a given index the lengths of the vectors are always decreasing, we have:

$$\left\|\mathbf{b}_k^{(t_k)}\right\| \leq \left\|\mathbf{b}_k^{(T_k+1)}\right\| \leq \left\|\mathbf{b}_{k-1}^{(T_k)}\right\|.$$

By definition of T_k the vectors $\mathbf{b}_1, \ldots, \mathbf{b}_{k-1}$ do not change between loop iterations t_{k-1} and T_k. Therefore:

$$\left\|\mathbf{b}_k^{(t_k)}\right\| \leq \left\|\mathbf{b}_{k-1}^{(t_{k-1})}\right\|.$$

If $j = k-1$, we have the result. Otherwise there exists a first loop iteration $T_{k-1} \in [\![t_{k-2}, t_{k-1} - 1]\!]$ such that $k(T_{k-1}) \geq k - 1 \geq k(T_{k-1} + 1)$. We have:

$$\left\|\mathbf{b}_{k-1}^{(t_{k-1})}\right\| \leq \left\|\mathbf{b}_{k-1}^{(T_{k-1}+1)}\right\| \leq \left\|\mathbf{b}_{k-2}^{(T_{k-1})}\right\| \leq \left\|\mathbf{b}_{k-2}^{(t_{k-2})}\right\|.$$

If $j = k-2$ we have the result, otherwise we go on constructing such loop iterations T_i's to obtain the result. □

We can now finish the complexity analysis. Let $k \in [\![2, d]\!]$ and $t_1 < t_2 < \ldots < t_{\tau_k} = \{t \leq \tau, k(t) = k\}$. We have:

$$\sum_{i=1}^{\tau_k} \left(\log\left\|\mathbf{b}_k^{(t_i)}\right\| - \log\left\|\mathbf{b}_{\alpha(t_i)}^{(t_i)}\right\|\right) \leq k\left(\log\|\mathbf{b}_d\| - \log\lambda_1\right) + \sum_{i=k}^{\tau_k} \log\left\|\mathbf{b}_k^{(t_i)}\right\| - \sum_{i=1}^{\tau_k-k+1} \log\left\|\mathbf{b}_{\alpha(t_i)}^{(t_i)}\right\|,$$

where λ_1 is the first minimum of the lattice we are reducing. Lemma 7.0.3 helps bounding the right hand-side of the above bound. First, we apply it with $t_1, \ldots, t_k$. Thus there exists $j < k$ such that $\|\mathbf{b}_k^{(t_k)}\| \leq \|\mathbf{b}_{\alpha(t_j)}^{(t_j)}\|$. The indices "$i = k$" in the positive sum and "$i = j$" in the negative sum cancel out. Then we apply Lemma 7.0.3 to t_{k+1} and the $k-1$ first t_i's that remain in the negative sum. It is easy to see that t_{k+1} is larger than any of them, so that we can have another "positive-negative" pair that cancels out. We perform this operation $\tau_k - k + 1$ times, to obtain:

$$\sum_{i=k}^{\tau_k} \log\left\|\mathbf{b}_k^{(t_i)}\right\| - \sum_{i=1}^{\tau_k-k+1} \log\left\|\mathbf{b}_{\alpha(t_i)}^{(t_i)}\right\| \leq 0.$$

The fact that $\sum_k \tau_k = \tau = O\left(1 + \log\|\mathbf{b}_d\| - \log\lambda_1\right)$ completes the proof of Theorem 4.2.1.

8. THE LOCAL APPROACH

This section and the following give another proof for Theorem 6.0.6. They give a more precise understanding of the behavior of the algorithm but may be skipped since they are not necessary to prove the main results of the paper.

In this section we give an alternative proof of Theorem 6.0.6 for $d \leq 4$, that generalizes the local analysis of Lagrange's algorithm. The result is of the same flavor, but involves a more subtle analysis of the behavior of successive loop iterations. We will obtain that except for a few initial initial and final iterations, the product of the lengths of the basis vectors decreases by at least a factor $K > 1$ every d loop iterations.

THEOREM 8.0.4. *Let $d \leq 4$. There exist three constants $K > 1, I, F$ such that in any d consecutive loop iterations of the d-dimensional recursive greedy algorithm of Figure 3, some of the iterations are in the I initial loop iterations or in the F final loop iterations, or the product of the lengths of the current basis vectors decreases by at least a factor K.*

This result clearly implies Theorem 6.0.6. The global approach has the advantage of providing a quicker proof of Theorem 6.0.6 then the local approach. However, it provides less insight on the behavior of the algorithm. The local approach explains why the algorithm actually makes progress in successive loop iterations, not only globally.

8.1 A Unified Geometric Analysis Up To Dimension Four

The local analysis of Lagrange's algorithm (Section 3) was based on the fact that if $|x| \geq 2$, the vector $x\mathbf{u}$ is far from the Voronoï cell of the lattice spanned by $\mathbf{u}$. The analysis of the number of loop iterations of the greedy algorithm in dimensions three and four relies on a similar phenomenon in dimensions two and three. However, the situation is more complex, as the following basic remarks hint:

—For $d = 2$, we considered the value of x, but if $d \geq 3$, there will be several coefficients x_i instead of a single one, and it is not clear which one will be useful in the analysis.

—For $d = 2$, Step 4 cannot change the basis, as there are only two bases in dimension one. If $d \geq 3$, Step 4 may completely change the vectors, and it could be hard to keep track of what is going on.

To prove Theorem 8.0.4, we introduce a few notations. Consider the i-th loop iteration. Let $\left[\mathbf{a}_1^{(i)}, \ldots, \mathbf{a}_d^{(i)}\right]_{\leq}$ denote the basis $[\mathbf{b}_1, \ldots, \mathbf{b}_d]_{\leq}$ at the beginning of the i-th loop iteration. The basis $\left[\mathbf{a}_1^{(i)}, \ldots, \mathbf{a}_d^{(i)}\right]_{\leq}$ becomes $\left[\mathbf{b}_1^{(i)}, \ldots, \mathbf{b}_{d-1}^{(i)}, \mathbf{a}_d^{(i)}\right]_{\leq}$ with $\left\|\mathbf{b}_1^{(i)}\right\| \leq \ldots \leq \left\|\mathbf{b}_{d-1}^{(i)}\right\|$ after Step 4, and $\left(\mathbf{b}_1^{(i)}, \ldots, \mathbf{b}_d^{(i)}\right)$ after Step 6, where $\mathbf{b}_d^{(i)} = \mathbf{a}_d^{(i)} - \mathbf{c}^{(i)}$ and $\mathbf{c}^{(i)}$ is the closest vector found at Step 5. Let p_i be the number of integers $1 \leq j \leq d$ such that $\left\|\mathbf{b}_j^{(i)}\right\| \leq \left\|\mathbf{b}_d^{(i)}\right\|$. Let π_i be the rank of $\mathbf{b}_d^{(i)}$ once $\left(\mathbf{b}_1^{(i)}, \ldots, \mathbf{b}_d^{(i)}\right)$ is sorted by length: for example, we have $\pi_i = 1$

if $\left\|\mathbf{b}_d^{(i)}\right\| < \left\|\mathbf{b}_1^{(i)}\right\|$. Notice that π_i may not be equal to p_i because there may be several choices when sorting the vectors by length in case of length equalities. Clearly $1 \leq \pi_i \leq p_i \leq d$, if $p_i = d$ then the loop terminates, and $\left\|\mathbf{a}_{\pi_i}^{(i+1)}\right\| = \left\|\mathbf{a}_{p_i}^{(i+1)}\right\|$.

Now consider the $(i+1)$-th loop iteration for some $i \geq 1$. Notice that by definition of π_i, we have $\mathbf{a}_{\pi_i}^{(i+1)} = \mathbf{b}_d^{(i)} = \mathbf{a}_d^{(i)} - \mathbf{c}^{(i)}$, while $\left\{\mathbf{a}_j^{(i+1)}\right\}_{j\neq\pi_i} = \left\{\mathbf{b}_j^{(i)}\right\}_{j<d}$. The vector $\mathbf{c}^{(i+1)}$ belongs to $L\left[\mathbf{b}_1^{(i+1)}, \ldots, \mathbf{b}_{d-1}^{(i+1)}\right] = L\left[\mathbf{a}_1^{(i+1)}, \ldots, \mathbf{a}_{d-1}^{(i+1)}\right]$: there exist integers $x_1^{(i+1)}, \ldots, x_{d-1}^{(i+1)}$ such that $\mathbf{c}^{(i+1)} = \sum_{j=1}^{d-1} x_j^{(i+1)} \mathbf{a}_j^{(i+1)}$.

We are to prove that there exists a universal constant $K > 1$ such that for any execution of the d-dimensional greedy algorithm with $d \leq 4$, in any d consecutive iterations of the loop (except eventually the first ones and the last ones), the product of the lengths of the current basis vectors decreases by some factor higher than K:

$$\frac{\left\|\mathbf{a}_1^{(i)}\right\| \ldots \left\|\mathbf{a}_d^{(i)}\right\|}{\left\|\mathbf{a}_1^{(i+d)}\right\| \ldots \left\|\mathbf{a}_d^{(i+d)}\right\|} \geq K \tag{2}$$

This will automatically ensure that the number of loop iterations is at most proportional to $\log \left\|\mathbf{a}_d^{(1)}\right\| - \log \lambda_1$.

We deal with the first difficulty mentioned above: which one will be the useful coefficient? The trick is to consider the value of $x_{\pi_i}^{(i+1)}$, i.e., the coefficient of $\mathbf{a}_{\pi_i}^{(i+1)} = \mathbf{a}_d^{(i)} - \mathbf{c}^{(i)}$ in $\mathbf{c}^{(i+1)}$, and to use the greedy properties of the algorithm. This coefficient corresponds to the vector that has been created at the previous loop iteration. Since this vector has been created so that it cannot be shortened by adding to it a combination of the others, there are only two possibilities at the current iteration: either the new vector is longer than $\mathbf{a}_{\pi_i}^{(i+1)}$, in which case p_i increases (this cannot happen during more than d successive iterations), either it is shorter and we must have $|x_{\pi_i}| \neq 1$.

LEMMA 8.1.1. *Among d consecutive iterations of the loop of the greedy algorithm of Figure 3, there is at least one iteration of index $i+1$ such that $p_{i+1} \leq p_i$. Moreover, for such a loop iteration, we have $\left|x_{\pi_i}^{(i+1)}\right| \geq 2$, or this is the last loop iteration.*

PROOF. The first statement is obvious. Consider one such loop iteration $i+1$. Suppose we have a small $|x_{\pi_i}^{(i+1)}|$, that is $x_{\pi_i}^{(i+1)} = 0$ or $\left|x_{\pi_i}^{(i+1)}\right| = 1$.

—If $x_{\pi_i}^{(i+1)} = 0$, then $\mathbf{c}^{(i+1)} \in L\left[\mathbf{a}_j^{(i+1)}\right]_{j\neq\pi_i, j<d} = L\left[\mathbf{b}_1^{(i)}, \ldots, \mathbf{b}_{d-2}^{(i)}\right]$. We claim that the $(i+1)$-th iteration must be the last one. Since the i-th loop iteration was not terminal, we have $\mathbf{a}_d^{(i+1)} = \mathbf{b}_{d-1}^{(i)}$. Moreover, the basis $\left[\mathbf{b}_1^{(i)}, \ldots, \mathbf{b}_{d-1}^{(i)}\right]_{\leq}$ is greedy-reduced because of Step 4 of the i-th loop iteration. These two facts imply

that $\mathbf{c}^{(i+1)}$ must be zero (or at least it does not make the length of $\mathbf{a}_d^{(i)}$ decrease if there are several closest lattice vectors), and the $(i+1)$-th loop iteration is the last one.

—If $|x_{\pi_i}^{(i+1)}| = 1$, we claim that $p_{i+1} > p_i$. We have $\mathbf{c}^{(i+1)} = \sum_{j=1}^{d-1} x_j^{(i+1)} \mathbf{a}_j^{(i+1)}$ where $\mathbf{a}_{\pi_i}^{(i+1)} = \mathbf{a}_d^{(i)} - \mathbf{c}^{(i)}$ and $\left\{\mathbf{a}_j^{(i+1)}\right\}_{j \neq \pi_i} = \left\{\mathbf{b}_j^{(i)}\right\}_{j<d}$. Thus, the vector $\mathbf{c}^{(i+1)}$ can be written as $\mathbf{c}^{(i+1)} = \mp\left(\mathbf{a}_d^{(i)} - \mathbf{c}^{(i)}\right) - \mathbf{e}$ where $\mathbf{e} \in L\left[\mathbf{b}_1^{(i)}, \ldots, \mathbf{b}_{d-1}^{(i)}\right]$. Therefore $\mathbf{a}_d^{(i+1)} - \mathbf{c}^{(i+1)} = \mathbf{b}_{d-1}^{(i)} \pm \left(\mathbf{a}_d^{(i)} - \mathbf{c}^{(i)}\right) + \mathbf{e}$. In other words, we have $\left\|\mathbf{a}_d^{(i+1)} - \mathbf{c}^{(i+1)}\right\| = \left\|\mathbf{a}_d^{(i)} - \mathbf{f}\right\|$ for some $\mathbf{f} \in L\left[\mathbf{b}_1^{(i)}, \ldots, \mathbf{b}_{d-1}^{(i)}\right]$. The greedy choice of $\mathbf{b}_d^{(i)}$ at the i-th loop iteration implies that $p_{i+1} \geq 1 + p_i$, which completes the proof of the claim.

□

We will see that in dimension three, any such loop iteration $i+1$ implies that at least one of the basis vectors significantly decreases in the $(i+1)$-th loop iteration, or had significantly decreased in the i-th loop iteration. This is only "almost" true in dimension four: fortunately, we will be able to isolate the bad cases and to show that when a bad case occurs, the number of remaining loop iterations can be bounded by some constant.

We now deal with the second difficulty mentioned above, that is the possible change of the vectors during the recursive call in dimension $d-1$. Recall that $\mathbf{c}^{(i+1)} = \sum_{j=1}^{d-1} x_j^{(i+1)} \mathbf{a}_j^{(i+1)}$ but the basis $\left[\mathbf{a}_1^{(i+1)}, \ldots, \mathbf{a}_{d-1}^{(i+1)}\right]_{\leq}$ is not necessarily greedy-reduced. We distinguish two cases:

(1) The ordered basis $\left[\mathbf{a}_1^{(i+1)}, \ldots, \mathbf{a}_{d-1}^{(i+1)}\right]_{\leq}$ is somehow far from being greedy-reduced. Then the vector $\mathbf{b}_d^{(i)}$ was significantly shorter than the replaced vector $\mathbf{a}_d^{(i)}$. Notice that this length decrease concerns the i-th loop iteration and not the $(i+1)$-th.

(2) Otherwise, the basis $\left[\mathbf{a}_1^{(i+1)}, \ldots, \mathbf{a}_{d-1}^{(i+1)}\right]_{\leq}$ is almost greedy-reduced. The fact that $\left|x_{\pi_i}^{(i+1)}\right| \geq 2$ roughly implies that the vector $\mathbf{c}^{(i+1)}$ is somewhat far away from the Voronoï cell $\mathrm{Vor}\left(\mathbf{a}_1^{(i+1)}, \ldots, \mathbf{a}_{d-1}^{(i+1)}\right)$: this phenomenon will be precisely captured by the so-called Gap Lemma. When this is the case, the new vector $\mathbf{b}_d^{(i+1)}$ is significantly shorter than $\mathbf{a}_d^{(i+1)}$.

To capture the property that a set of vectors is almost greedy-reduced, we introduce the so-called *ε-greedy-reduction*, which is defined as follows:

Definition 8.1.2. Let $\varepsilon \geq 0$. A single vector $[\mathbf{b}_1]$ is always ε-greedy-reduced; for $d \geq 2$, a d-tuple $[\mathbf{b}_1, \ldots, \mathbf{b}_d]_{\leq}$ is ε-greedy-reduced if $[\mathbf{b}_1, \ldots, \mathbf{b}_{d-1}]_{\leq}$ is ε-greedy-reduced and the orthogonal projection of the vector $\mathbf{b}_d$ onto the span of $[\mathbf{b}_1, \ldots, \mathbf{b}_{d-1}]_{\leq}$ belongs to $(1+\varepsilon) \cdot \mathrm{Vor}(\mathbf{b}_1, \ldots, \mathbf{b}_{d-1})$.

With this definition, a greedy-reduced basis is ε-greedy-reduced for any $\varepsilon \geq 0$. In the definition of ε-greedy-reduction, we did not assume that the $\mathbf{b}_i$'s were nonzero nor linearly independent. This is because the Gap Lemma is essentially based on compactness properties: the set of ε-greedy-reduced d-tuples needs being closed (from a topological point of view), while a limit of bases may not be a basis.

We can now give the precise statements of the two cases described just above. Lemma 8.1.3 corresponds to case 1, and Lemma 8.1.4 to case 2.

LEMMA 8.1.3. *Let $2 \leq d \leq 4$. There exists a constant $\varepsilon_1 > 0$ such that for any $\varepsilon \in (0, \varepsilon_1]$ there exists $C_\varepsilon > 1$ such that the following statement holds. Consider the $(i+1)$-th loop iteration of an execution of the d-dimensional greedy algorithm. If $\left[\mathbf{a}_1^{(i+1)}, \ldots, \mathbf{a}_{d-1}^{(i+1)}\right]_{\leq}$ is not ε-greedy-reduced, then $\left\|\mathbf{a}_d^{(i)}\right\| \geq C_\varepsilon \left\|\mathbf{b}_d^{(i)}\right\|$.*

PROOF. The statement is obvious for $d = 2$ since a single vector is always ε-greedy-reduced. Suppose that $d = 3$ and that $\left[\mathbf{a}_1^{(i+1)}, \mathbf{a}_2^{(i+1)}\right]_{\leq}$ is not ε-greedy-reduced. We have $\left|\langle \mathbf{a}_2^{(i+1)}, \mathbf{a}_1^{(i+1)} \rangle\right| \geq \frac{1+\varepsilon}{2} \left\|\mathbf{a}_1^{(i+1)}\right\|^2$. Along with this, we must have $\pi_i = 1$ (otherwise $\left[\mathbf{a}_1^{(i+1)}, \mathbf{a}_2^{(i+1)}\right]_{\leq} = \left[\mathbf{b}_1^{(i)}, \mathbf{b}_2^{(i)}\right]_{\leq}$ would be Minkowski-reduced), which implies that the vector $\mathbf{a}_1^{(i+1)} = \mathbf{b}_3^{(i)}$ cannot be shortened by adding to it multiples of $\mathbf{a}_2^{(i+1)} = \mathbf{b}_1^{(i)}$. We thus have $\left|\langle \mathbf{a}_1^{(i+1)}, \mathbf{a}_2^{(i+1)} \rangle\right| \leq \left\|\mathbf{a}_2^{(i+1)}\right\|^2 /2$. These two inequalities give:

$$(1+\varepsilon) \cdot \left\|\mathbf{a}_1^{(i+1)}\right\|^2 \leq \left\|\mathbf{a}_2^{(i+1)}\right\|^2 .$$

The facts that $\mathbf{a}_1^{(i+1)} = \mathbf{b}_3^{(i)}$ and that $\left\|\mathbf{a}_2^{(i+1)}\right\| \leq \left\|\mathbf{a}_3^{(i)}\right\|$ end the proof.

Suppose now that $d = 4$ and that the ordered basis $\left[\mathbf{a}_1^{(i+1)}, \mathbf{a}_2^{(i+1)}, \mathbf{a}_3^{(i+1)}\right]_{\leq}$ is not ε-greedy-reduced. Therefore the orthogonal projection of the vector $\mathbf{a}_2^{(i+1)}$ onto the linear span of $\mathbf{a}_1^{(i+1)}$ is not in $(1+\varepsilon) \cdot \mathrm{Vor}\left(\mathbf{a}_1^{(i+1)}\right)$, or the orthogonal projection of the vector $\mathbf{a}_3^{(i+1)}$ onto the linear span of $\left[\mathbf{a}_1^{(i+1)}, \mathbf{a}_2^{(i+1)}\right]$ is not in $(1+\varepsilon) \cdot \mathrm{Vor}\left(\mathbf{a}_1^{(i+1)}, \mathbf{a}_2^{(i+1)}\right)$. We consider these two cases separately. Suppose first that the orthogonal projection of the vector $\mathbf{a}_2^{(i+1)}$ onto the linear span of $\mathbf{a}_1^{(i+1)}$ is not in $\mathrm{Vor}\left(\mathbf{a}_1^{(i+1)}\right)$. Then $\left|\langle \mathbf{a}_1^{(i+1)}, \mathbf{a}_2^{(i+1)} \rangle\right| \geq \frac{1+\varepsilon}{2} \left\|\mathbf{a}_1^{(i+1)}\right\|^2$. Moreover, we must have $\pi_i = 1$ (otherwise $\left[\mathbf{a}_1^{(i+1)}, \mathbf{a}_2^{(i+1)}\right]_{\leq} = \left[\mathbf{b}_1^{(i)}, \mathbf{b}_2^{(i)}\right]_{\leq}$ is Minkowski-reduced), therefore the vector $\mathbf{a}_1^{(i+1)}$ cannot be shortened by adding to it multiples of the vector $\mathbf{a}_2^{(i+1)}$, which gives that $\left|\langle \mathbf{a}_1^{(i+1)}, \mathbf{a}_2^{(i+1)} \rangle\right| \leq \left\|\mathbf{a}_2^{(i+1)}\right\|^2 /2$. Then:

$$(1+\varepsilon) \cdot \left\|\mathbf{b}_4^{(i)}\right\|^2 = (1+\varepsilon) \cdot \left\|\mathbf{a}_1^{(i+1)}\right\|^2 \leq \left\|\mathbf{a}_2^{(i+1)}\right\|^2 \leq \left\|\mathbf{a}_4^{(i)}\right\|^2 .$$

We suppose now that the ordered vectors $\left[\mathbf{a}_1^{(i+1)}, \mathbf{a}_2^{(i+1)}\right]_{\leq}$ are ε-greedy-reduced

and that the orthogonal projection of the vector $\mathbf{a}_3^{(i+1)}$ onto the linear span of $\left[\mathbf{a}_1^{(i+1)}, \mathbf{a}_2^{(i+1)}\right]_{\leq}$ belongs to the set $(1+\varepsilon)\cdot \mathrm{Vor}\left(\mathbf{a}_1^{(i+1)}, \mathbf{a}_2^{(i+1)}\right)$. We distinguish two subcases: $\pi_i = 1$ and $\pi_i = 2$. Suppose first that $\pi_i = 2$. In this case $\left[\mathbf{a}_1^{(i+1)}, \mathbf{a}_2^{(i+1)}\right]_{\leq}$ is Minkowski-reduced and the possible Voronoï coordinates of $L\left[\mathbf{a}_1^{(i+1)}, \mathbf{a}_2^{(i+1)}\right]$ are the pairs $(x_1, x_2) \in \{-1, 0, 1\}^2$ (see Lemma 9.1.2). Thus a vector $\mathbf{u}$ has its orthogonal projection onto the span of $\left[\mathbf{a}_1^{(i+1)}, \mathbf{a}_2^{(i+1)}\right]_{\leq}$ in $\mathrm{Vor}\left(\mathbf{a}_1^{(i+1)}, \mathbf{a}_2^{(i+1)}\right)$ if and only if:

$$\forall (x_1, x_2) \in \{-1, 0, 1\}^2,\ \|\mathbf{u}\| \leq \left\|\mathbf{u} + x_1\mathbf{a}_1^{(i+1)} + x_2\mathbf{a}_2^{(i+1)}\right\|.$$

This implies that there exists a pair $(x_1, x_2) \in \{-1, 0, 1\}^2$ such that

$$\left|\langle \mathbf{a}_3^{(i+1)}, x_1\mathbf{a}_1^{(i+1)} + x_2\mathbf{a}_2^{(i+1)}\rangle\right| \geq \frac{1+\varepsilon}{2}\left\|x_1\mathbf{a}_1^{(i+1)} + x_2\mathbf{a}_2^{(i+1)}\right\|^2.$$

In the case when $\pi_i = 1$, we can suppose that $\left\|\mathbf{a}_1^{(i+1)}\right\| \geq (1-\varepsilon)\cdot\left\|\mathbf{a}_2^{(i+1)}\right\|$, since otherwise $\left\|\mathbf{b}_4^{(i)}\right\| = \left\|\mathbf{a}_1^{(i+1)}\right\| \leq (1-\varepsilon)\cdot\left\|\mathbf{a}_4^{(i)}\right\|$. We will see in Subsection 9.2 (Lemma 9.2.5) that for a small enough $\varepsilon > 0$, the possible Voronoï coords of such an ε-greedy-reduced basis are the same as for a Minkowski-reduced basis. Therefore, as in the previous subcase, there exists a pair $(x_1, x_2) \in \{-1, 0, 1\}^2$ such that $\left|\langle \mathbf{a}_3^{(i+1)}, x_1\mathbf{a}_1^{(i+1)} + x_2\mathbf{a}_2^{(i+1)}\rangle\right| \geq \frac{1+\varepsilon}{2}\left\|x_1\mathbf{a}_1^{(i+1)} + x_2\mathbf{a}_2^{(i+1)}\right\|^2$. We now consider the two subcases simultaneously. Suppose first that $x_2 = 0$, then necessarily $|x_1| = 1$. As in the case $d = 3$, the fact that the vector $\mathbf{a}_1^{(i+1)}$ cannot be shortened by adding to it multiples of the vector $\mathbf{a}_3^{(i+1)}$ gives the result (this is obvious if $\pi_i = 1$ and, if $\pi_i = 2$, the basis $\left[\mathbf{a}_1^{(i+1)}, \mathbf{a}_3^{(i+1)}\right]_{\leq} = \left[\mathbf{b}_1^{(i)}, \mathbf{b}_2^{(i)}\right]_{\leq}$ is Minkowski-reduced). The case $x_1 = 0$ can be dealt with in the same way. Therefore, it remains to consider the case $|x_1| = |x_2| = 1$. Wlog we suppose $x_1 = x_2 = 1$. We have:

$$\left|\langle \mathbf{a}_3^{(i+1)}, \mathbf{a}_1^{(i+1)} + \mathbf{a}_2^{(i+1)}\rangle\right| \geq \frac{1+\varepsilon}{2}\left\|\mathbf{a}_1^{(i+1)} + \mathbf{a}_2^{(i+1)}\right\|^2.$$

Since the vector $\mathbf{a}_{\pi_i}^{(i+1)}$ cannot be shortened by adding to it integer linear combinations of the two other vectors, we have $\left\|\mathbf{a}_3^{(i+1)} \pm \left(\mathbf{a}_1^{(i+1)} + \mathbf{a}_2^{(i+1)}\right)\right\| \geq \left\|\mathbf{a}_{\pi_i}^{(i+1)}\right\| = \left\|\mathbf{b}_4^{(i)}\right\|$. By considering the right choice for the "plus or minus" and using the fact that $\left\|\mathbf{a}_3^{i+1}\right\| \leq \left\|\mathbf{a}_4^{(i)}\right\|$, we obtain:

$$\begin{aligned}\left\|\mathbf{b}_4^{(i)}\right\|^2 &\leq \left\|\mathbf{a}_4^{(i)}\right\|^2 - 2\left|\langle \mathbf{a}_3^{(i+1)}, \mathbf{a}_1^{(i+1)} + \mathbf{a}_2^{(i+1)}\rangle\right| + \left\|\mathbf{a}_1^{(i+1)} + \mathbf{a}_2^{(i+1)}\right\|^2 \\ &\leq \left\|\mathbf{a}_4^{(i)}\right\|^2 - \varepsilon\cdot\left\|\mathbf{a}_1^{(i+1)} + \mathbf{a}_2^{(i+1)}\right\|^2.\end{aligned}$$

Since the basis $\left[\mathbf{a}_1^{(i+1)}, \mathbf{a}_2^{(i+1)}\right]_{\leq}$ is ε-greedy-reduced, we also have:

$$\left\|\mathbf{a}_1^{(i+1)} + \mathbf{a}_2^{(i+1)}\right\|^2 \geq \left\|\mathbf{a}_1^{(i+1)}\right\|^2 + \left\|\mathbf{a}_2^{(i+1)}\right\|^2 - (1+\varepsilon)\cdot\left\|\mathbf{a}_1^{(i+1)}\right\|^2 \geq (1-\varepsilon)\cdot\left\|\mathbf{a}_2^{(i+1)}\right\|^2,$$

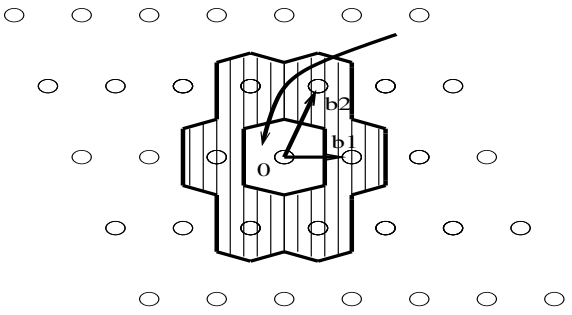

Fig. 7. The Gap Lemma in dimension 2.

from which we get $(1+\varepsilon(1-\varepsilon)) \cdot \left\|\mathbf{b}_4^{(i)}\right\|^2 \leq \left\|\mathbf{a}_4^{(i)}\right\|^2$. □

LEMMA 8.1.4. *Let $2 \leq d \leq 4$. There exist two constants $\varepsilon_2 > 0$ and $D > 0$ such that the following statement holds. Consider the $(i+1)$-th loop iteration of an execution of the d-dimensional greedy algorithm. Suppose that $\left[\mathbf{a}_1^{(i+1)}, \ldots, \mathbf{a}_{d-1}^{(i+1)}\right]_{\leq}$ is ε_2-greedy-reduced, and that $\left\|\mathbf{a}_k^{(i+1)}\right\| \geq (1-\varepsilon_2) \cdot \left\|\mathbf{a}_d^{(i+1)}\right\|$ for some $k \in [\![1, d-1]\!]$. Then, if $|x_k| \geq 2$ and if we are not in the 211-case, we have:*

$$\left\|\mathbf{b}_d^{(i+1)}\right\|^2 + D\left\|\mathbf{b}_k^{(i+1)}\right\|^2 \leq \left\|\mathbf{a}_d^{(i+1)}\right\|^2,$$

where the 211-case is: $d = 4, |x_k| = 2$ and the other $|x_j|$'s are both equal to 1.

This last lemma is a direct consequence of the Pythagorean theorem and the Gap Lemma: in Equation (3) below, set $\mathbf{u}$ as the orthogonal projection of $\mathbf{b}_d^{(i+1)}$ onto the span of $\mathbf{a}_1, \ldots, \mathbf{a}_{d-1}$ and notice that $\|\mathbf{b}_k^{(i+1)}\| \leq \|\mathbf{a}_k^{(i+1)}\|$. This result is crucial to our analysis, and Section 9 is devoted to prove it. Figure 7 illustrates the Gap Lemma: when a vector from the outer non-hashed area that is mapped to a vector within the inner non-hashed area, its length decreases significantly.

THEOREM 8.1.5 GAP LEMMA. *Let $2 \leq d \leq 4$. There exist two universal constants $\varepsilon > 0$ and $D > 0$ such that the following statement holds. Let $[\mathbf{a}_1, \ldots, \mathbf{a}_{d-1}]_{\leq}$ be ε-greedy-reduced vectors, $\mathbf{u}$ be a vector of $\mathrm{Vor}(\mathbf{a}_1, \ldots, \mathbf{a}_{d-1})$ and $x_1, \ldots, x_{d-1}$ be integers. Suppose that $\|\mathbf{a}_k\| \geq (1-\varepsilon) \cdot \|\mathbf{a}_{d-1}\|$ for some $k < d$. Suppose also that $|x_k| \geq 2$ and that if $d = 4$ the two other $|x_j|$'s are not both equal to 1. Then:*

$$\|\mathbf{u}\|^2 + D\|\mathbf{a}_k\|^2 \leq \left\|\mathbf{u} + \sum_{j=1}^{d-1} x_j \mathbf{a}_j\right\|^2. \tag{3}$$

This completes the overall description of the proof of Theorem 4.2.1. Indeed, choose three constants $\varepsilon, D > 0$ and $C > 1$ such that we can apply Lemmata 8.1.3 and 8.1.4. We prove that Equation (2) holds for $K = \min\left(C, \sqrt{1+D}, \frac{1}{1-\varepsilon}\right) > 1$. Consider a loop iteration $i+1$ such that $p_{i+1} \leq p_i$. Recall that among any d

consecutive iterations of the loop, there is at least one such iteration. For such an iteration we have $\left|x_{\pi_i}^{(i+1)}\right| \geq 2$. We distinguish four cases:

—The basis $\left[\mathbf{a}_1^{(i+1)}, \ldots, \mathbf{a}_{d-1}^{(i+1)}\right]_{\leq}$ is not ε-greedy-reduced: then Lemma 8.1.3 gives the result *via* the i-th loop iteration.

—We have $\left\|\mathbf{a}_{\pi_i}^{(i+1)}\right\| < (1-\varepsilon) \cdot \left\|\mathbf{a}_d^{(i+1)}\right\|$. Indeed, because $p_{i+1} \leq p_i$, we have:

$$\begin{aligned}\left\|\mathbf{b}_d^{(i+1)}\right\| \leq \left\|\mathbf{b}_{\pi_{i+1}}^{(i+1)}\right\| \leq \left\|\mathbf{a}_{\pi_{i+1}}^{(i+1)}\right\| &= \left\|\mathbf{a}_{p_{i+1}}^{(i+1)}\right\| \\ &\leq \left\|\mathbf{a}_{p_i}^{(i+1)}\right\| = \left\|\mathbf{a}_{\pi_i}^{(i+1)}\right\| < (1-\varepsilon) \cdot \left\|\mathbf{a}_d^{(i+1)}\right\|.\end{aligned}$$

—We are in the 211-case, i.e., $d = 4$ with $|x_{\pi_i}| = 2$ and the other $|x_j|$'s are all equal to 1. Then we refer to Subsection 8.2.

—Otherwise we apply Lemma 8.1.4, which gives the expected result *via* the $(i+1)$-th loop iteration.

8.2 Concluding in Dimension Four

In the previous subsections, we showed that there is at most a linear number of loop iterations in the iterative greedy algorithm in dimensions two and three, but we noticed that a new difficulty arose in dimension four: the Gap Lemma is useless in the so-called 211-case. This is because there are three-dimensional Minkowski-reduced bases $[\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3]_{\leq}$ for which $2\mathbf{b}_i + s_1\mathbf{b}_j + s_2\mathbf{b}_k$ — with $\{i,j,k\} = \{1,2,3\}$ and $|s_1| = |s_2| = 1$ — is a Voronoï vector. Indeed consider the lattice spanned by the columns $\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3$ of the following matrix:

$$M = \begin{bmatrix} 1 & 1 & -1 \\ 1 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

This basis is Minkowski-reduced and $\|\mathbf{b}_1 + \mathbf{b}_2 + 2\mathbf{b}_3\| = \|\mathbf{b}_1 + \mathbf{b}_2\| \leq \|(2k_1+1)\mathbf{b}_1 + (2k_2+1)\mathbf{b}_1 + 2k_3\mathbf{b}_3\|$ for any $k_1, k_2, k_3 \in \mathbb{Z}$. Therefore, a vector in the translated Voronoï cell centered in $\mathbf{b}_1 + \mathbf{b}_2 + 2\mathbf{b}_3$ can avoid being significantly shortened when translated inside the Voronoï cell centered in $\mathbf{0}$.

The Gap Lemma cannot tackle this problem. However, we notice that $(1,1,2)$ is rarely a Voronoï coordinate (with respect to a Minkowski-reduced basis), and when it is the case it cannot be a strict Voronoï coord: it can be proved easily that if $(1,1,2)$ is a Voronoï coord, then $\|\mathbf{b}_1 + \mathbf{b}_2\| = \|\mathbf{b}_1 + \mathbf{b}_2 + 2\mathbf{b}_3\|$, which tells us that $\mathbf{b}_1 + \mathbf{b}_2 + 2\mathbf{b}_3$ is not the only vector in its coset of $L/2L$ reaching the length minimum. It turns out that the lattice spanned by the columns of M is essentially the only one for which $(1,1,2)$ — modulo any change of sign and permutation of coordinates — can be a Voronoï coord. More precisely, if $(1,1,2)$ — modulo any change of sign and permutation of coordinates — is a Voronoï coord for a lattice basis, then the basis matrix can be written as rUM where r is any non-zero real number and U is any orthogonal matrix. Since a basis can be arbitrarily close to one of them without actually being one of them, we need to consider a small compact set of normalized bases around the annoying ones. More precisely, this

compact set consists in all ε-greedy-reduced bases $[\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3]_{\leq}$ such that there exists a permutation $\sigma \in \mathcal{S}_3$ with

$$\left\| \frac{1}{\|\mathbf{b}_3\|^2} \left| G\left(\mathbf{b}_{\sigma(1)}, \mathbf{b}_{\sigma(2)}, \mathbf{b}_{\sigma(3)}\right) \right| - \left| M^t M \right| \right\|_\infty \leq \varepsilon$$

for some sufficiently small $\varepsilon > 0$, where $\|M\|_\infty$ is the maximum of the absolute values of the matrix M and $|M|$ is the matrix made of the absolute values of the entries of M.

Now, consider we are in the 211-case at some loop iteration $i+1$. We distinguish three cases:

—The basis $\left[\mathbf{a}_1^{(i+1)}, \mathbf{a}_2^{(i+1)}, \mathbf{a}_3^{(i+1)}\right]_{\leq}$ is outside the compact. In this case, a variant of the Gap Lemma (Lemma 9.3.4) proved in Section 9 is valid and can be used to show that the vector $\mathbf{b}_4^{(i+1)}$ is significantly shorter than the vector $\mathbf{a}_4^{(i+1)}$.

—The basis $\left[\mathbf{a}_1^{(i+1)}, \mathbf{a}_2^{(i+1)}, \mathbf{a}_3^{(i+1)}\right]_{\leq}$ is inside the compact but the orthogonal projection of the vector $\mathbf{a}_4^{(i+1)}$ onto the linear span of $\left[\mathbf{a}_1^{(i+1)}, \mathbf{a}_2^{(i+1)}, \mathbf{a}_3^{(i+1)}\right]_{\leq}$ is far from the Voronoï cell $\mathrm{Vor}\left(\mathbf{a}_1^{(i+1)}, \mathbf{a}_2^{(i+1)}, \mathbf{a}_3^{(i+1)}\right)$. In this case, we can use Lemma 9.3.4 to show that the vector $\mathbf{b}_4^{(i+1)}$ is significantly shorter than the vector $\mathbf{a}_4^{(i+1)}$.

—Otherwise the geometry of the basis $\left[\mathbf{a}_1^{(i+1)}, \mathbf{a}_2^{(i+1)}, \mathbf{a}_3^{(i+1)}, \mathbf{a}_4^{(i+1)}\right]_{\leq}$ is very precisely known and we can show that there remain $O(1)$ loop iterations.

More precisely, by using Lemma 9.3.4, we show that:

LEMMA 8.2.1. *There exist two constants $K, \varepsilon > 0$ such that the following holds. Consider an execution of the four-dimensional greedy algorithm, and a loop iteration $i+1$ for which:*

(1) $p_{i+1} \leq p_i$,

(2) $|x_{\pi_i}| = 2$ *and* $\left(\left|x_{\sigma(1)}\right|, \left|x_{\sigma(2)}\right|, \left|x_{\sigma(3)}\right|\right) = (1,1,2)$ *for some* $\sigma \in \mathcal{S}_3$,

(3) $\left[\mathbf{a}_1^{(i+1)}, \mathbf{a}_2^{(i+1)}, \mathbf{a}_3^{(i+1)}\right]_{\leq}$ *is ε-greedy-reduced,*

(4) $\left\|\mathbf{a}_{\pi_i}^{(i+1)}\right\| \geq (1-\varepsilon) \cdot \left\|\mathbf{a}_4^{(i+1)}\right\|$.

Then either $\left\|\mathbf{a}_4^{(i+1)}\right\| \geq (1+K) \cdot \left\|\mathbf{b}_4^{(i+1)}\right\|$ *or:*

$$\left\| \frac{1}{\left\|\mathbf{a}_4^{(i+1)}\right\|^2} \left| G\left(\mathbf{a}_{\sigma(1)}^{(i+1)}, \mathbf{a}_{\sigma(2)}^{(i+1)}, \mathbf{a}_{\sigma(3)}^{(i+1)}, \mathbf{a}_4^{(i+1)}\right) \right| - A \right\|_\infty \leq \varepsilon, \text{ with } A = \begin{bmatrix} 1 & 0 & \frac{1}{2} & 0 \\ 0 & 1 & \frac{1}{2} & 0 \\ \frac{1}{2} & \frac{1}{2} & 1 & \frac{1}{2} \\ 0 & 0 & \frac{1}{2} & 1 \end{bmatrix}.$$

To prove this result, we restrict more and more the possible geometry of the basis $\left[\mathbf{a}_1^{(i)}, \mathbf{a}_2^{(i)}, \mathbf{a}_3^{(i)}, \mathbf{a}_4^{(i)}\right]_{\leq}$. Notice that this critical geometry corresponds to the root lattice D_4. This last case is considered in Lemma 8.2.2.

PROOF. The proof essentially relies on Lemma 9.3.4. We choose $\varepsilon, C > 0$ according to Lemma 9.3.4. The constant K will depend on C and ε. We first show that wlog we can suppose that the basis vectors have similar lengths, that is $(1-\varepsilon)^2 \cdot \left\|\mathbf{a}_4^{(i+1)}\right\| \leq \left\|\mathbf{a}_1^{(i+1)}\right\|$. We know that $|x_{\pi_i}| = 2$ and the two other $|x_i|$'s are 1. By hypothesis, we have $\left\|\mathbf{a}_{\pi_i}^{(i+1)}\right\| \geq (1-\varepsilon) \cdot \left\|\mathbf{a}_4^{(i+1)}\right\|$. If $\pi_i = 1$, we are done. If $\pi_i = 2$, then we apply Lemma 9.3.4 2), and if $\pi_i = 3$ we apply Lemma 9.3.4 1), in both cases along with the Pythagorean theorem. So far, we have proved that one of the following holds:

(1) $\|\mathbf{a}_4^{(i+1)}\|^2 \geq (1+C)\|\mathbf{b}_4^{(i+1)}\|^2$,
(2) $(1-\varepsilon)^2\|\mathbf{a}_4^{(i+1)}\| \leq \|\mathbf{a}_1^{(i+1)}\| \leq \|\mathbf{a}_2^{(i+1)}\| \leq \|\mathbf{a}_3^{(i+1)}\| \leq \|\mathbf{a}_4^{(i+1)}\|$.

The remainder of the proof is the same for any of the possible configurations of (x_1, x_2, x_3), thus, for the sake of simplicity, we suppose now that $(x_1, x_2, x_3) = (2, 1, 1)$. The following step of the proof is to show that we can suppose that the Gram matrix of $\left[\mathbf{a}_1^{(i+1)}, \mathbf{a}_2^{(i+1)}, \mathbf{a}_3^{(i+1)}\right]_{\leq}$ is approximately:

$$\left\|\mathbf{a}_4^{(i+1)}\right\|^2 \cdot \begin{bmatrix} 1 & -\frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & 1 & 0 \\ -\frac{1}{2} & 0 & 1 \end{bmatrix}.$$

This directly follows from Lemma 9.3.4 and the Pythagorean theorem, which give that at least one of the following holds:

(1) $\left\|\mathbf{a}_4^{(i+1)}\right\|^2 \geq (1+C)\left\|\mathbf{b}_4^{(i+1)}\right\|^2$,
(2) $\left|\langle \mathbf{a}_2^{(i+1)}, \mathbf{a}_3^{(i+1)}\rangle\right| \leq \varepsilon \left\|\mathbf{a}_3^{(i+1)}\right\|^2$ and $\left|\langle \mathbf{a}_1^{(i+1)}, \mathbf{a}_j^{(i+1)}\rangle + \frac{1}{2}\left\|\mathbf{a}_3^{(i+1)}\right\|^2\right| \leq \varepsilon \left\|\mathbf{a}_3^{(i+1)}\right\|^2$ for $j \in \{2, 3\}$.

It remains to consider the scalar products $\langle \mathbf{a}_4^{(i+1)}, \mathbf{a}_k^{(i+1)}\rangle$ for $k \in \{1, 2, 3\}$. Recall that the orthogonal projection of the vector $\mathbf{b}_4^{(i+1)} = \mathbf{a}_4^{(i+1)} - \mathbf{a}_3^{(i+1)} - \mathbf{a}_2^{(i+1)} - 2\mathbf{a}_1^{(i+1)}$ onto the linear span of $\left[\mathbf{a}_1^{(i+1)}, \mathbf{a}_2^{(i+1)}, \mathbf{a}_3^{(i+1)}\right]_{\leq}$ belongs to the Voronoï cell $\mathrm{Vor}\left(\mathbf{a}_1^{(i+1)}, \mathbf{a}_2^{(i+1)}, \mathbf{a}_3^{(i+1)}\right)$. Wlog we can suppose that $\left\|\mathbf{a}_4^{(i+1)}\right\| \geq \left\|\mathbf{b}_4^{(i+1)}\right\| \geq (1-\varepsilon) \cdot \left\|\mathbf{a}_4^{(i+1)}\right\|$, since otherwise have the result for $K = \frac{1}{1-\varepsilon}$. By expanding $\|\mathbf{b}_4\|^2$, we get:

$$\begin{aligned}(1+19\varepsilon) \cdot \left\|\mathbf{a}_4^{(i+1)}\right\|^2 &\geq 3\left\|\mathbf{a}_4^{(i+1)}\right\|^2 - 2\langle \mathbf{a}_4^{(i+1)}, 2\mathbf{a}_1^{(i+1)} + \mathbf{a}_2^{(i+1)} + \mathbf{a}_3^{(i+1)}\rangle \\ &\geq (1-19\varepsilon) \cdot \left\|\mathbf{a}_4^{(i+1)}\right\|^2,\end{aligned}$$

where we used our knowledge of the Gram matrix of $\left[\mathbf{a}_1^{(i+1)}, \mathbf{a}_2^{(i+1)}, \mathbf{a}_3^{(i+1)}\right]_{\leq}$. Thus we have:

$$\left|\langle \mathbf{a}_4^{(i+1)}, 2\mathbf{a}_1^{(i+1)} + \mathbf{a}_2^{(i+1)} + \mathbf{a}_3^{(i+1)}\rangle - \left\|\mathbf{a}_4^{(i+1)}\right\|\right| \leq 19\varepsilon \cdot \left\|\mathbf{a}_4^{(i+1)}\right\|.$$

This last equation gives that in order to end the proof, it is sufficient to prove that the scalar products $\langle \mathbf{a}_4^{(i+1)}, \mathbf{a}_2^{(i+1)} \rangle$ and $\langle \mathbf{a}_4^{(i+1)}, \mathbf{a}_3^{(i+1)} \rangle$ are small. Let $j \in \{2,3\}$. By hypothesis, for any $x \in \mathbb{Z}$, we have $\left\| \mathbf{a}_4^{(i+1)} - 2\mathbf{a}_1^{(i+1)} - x\mathbf{a}_j^{(i+1)} \right\| \geq \left\| \mathbf{a}_4^{(i+1)} - 2\mathbf{a}_1^{(i+1)} - \mathbf{a}_2^{(i+1)} - \mathbf{a}_3^{(i+1)} \right\|$. In particular, by choosing $x = 0$ and $x = 2$ and expanding the norms and using the knowledge of the Gram matrix of the ordered basis $\left[\mathbf{a}_1^{(i+1)}, \mathbf{a}_2^{(i+1)}, \mathbf{a}_3^{(i+1)} \right]_{\leq}$, one can obtain an explicit positive integer k such that $\left| \langle \mathbf{a}_4^{(i+1)}, \mathbf{a}_1^{(i+1)} \rangle \right| \leq k\varepsilon \cdot \left\| \mathbf{a}_4^{(i+1)} \right\|$.

Let $K = \min\left(1 + C, \frac{1}{(1-\varepsilon)^2}\right)$. Altogether, we have proved that there exists a constant $K' = \max(K, k, 16)$ such that:

$$\left\| \frac{1}{\left\| \mathbf{a}_4^{(i+1)} \right\|^2} G\left(\mathbf{a}_1^{(i+1)}, \mathbf{a}_2^{(i+1)}, \mathbf{a}_3^{(i+1)}, \mathbf{a}_4^{(i+1)} \right) - A \right\|_\infty \leq K'\varepsilon.$$

This completes the proof of the lemma. □

At this point of the analysis of the 211-case, we have shown that we can suppose that the shape of the basis $\left[\mathbf{a}_1^{(i+1)}, \mathbf{a}_2^{(i+1)}, \mathbf{a}_3^{(i+1)}, \mathbf{a}_4^{(i+1)} \right]_{\leq}$ is very specific: its Gram matrix is very close to A. We treat this last case by applying the following lemma, which roughly says that if the Gram matrix of a basis is sufficiently close to some invertible matrix, then the number of short vectors generated by the basis remains bounded. Since the greedy algorithm always creates smaller bases for the lexicographic order based on the lengths, if the Gram matrix of the current basis is close to the matrix A, then it remains $O(1)$ loop iterations.

LEMMA 8.2.2. *Let A be a $d \times d$ invertible matrix, and $B > 0$. There exist $\varepsilon, N > 0$ such that for any basis $(\mathbf{b}_1, \ldots, \mathbf{b}_d)$ satisfying $\left\| \frac{1}{\|\mathbf{b}_d\|^2} G(\mathbf{b}_1, \ldots, \mathbf{b}_d) - A \right\|_\infty \leq \varepsilon$, we have:*

$$|\{(x_1, \ldots, x_d), \|x_1\mathbf{b}_1 + \ldots + x_d\mathbf{b}_d\| \leq B\|\mathbf{b}_d\|\}| \leq N.$$

PROOF. Let $\varepsilon > 0$ such that for any G, if $\|G - A\|_\infty \leq \varepsilon$, then G is invertible (such an ε does exist since the set of invertible matrices is open). In that case, if $X = (x_1, \ldots, x_d)$, then

$$\left| \frac{1}{\|\mathbf{b}_d\|^2} \|x_1\mathbf{b}_1 + \ldots + x_d\mathbf{b}_d\|^2 - XAX^t \right| = |X(G - A)X^t| \leq d^2\varepsilon \cdot (XX^t),$$

where $G = \frac{1}{\|\mathbf{b}_d\|^2} G(\mathbf{b}_1, \ldots, \mathbf{b}_d)$. Therefore, if $\|x_1\mathbf{b}_1 + \ldots + x_d\mathbf{b}_d\| \leq B\|\mathbf{b}_d\|$, then, by the triangular inequality, we obtain $|XAX^t| \leq B^2 + d^2\varepsilon \cdot (XX^t)$. But $|XAX^t| \geq \frac{1}{\|A^{-1}\|}(XX^t)$, where $\|B\|$ is defined as $\max(YBY^t, Y \in \mathbb{R}^n$ and $\|Y\| = 1)$, which is positive. Therefore:

$$(XX^t) \cdot \left(\frac{1}{\|A^{-1}\|} - d^2\varepsilon \right) \leq B^2.$$

We set $\varepsilon < \frac{1}{d^2\|A^{-1}\|}$. The x_i's are integers such that the quantity (XX^t) remains

bounded, so that we are considering integer points in a d-dimensional hypersphere. There can only be finitely many such points. □

9. THE GEOMETRY OF LOW-DIMENSIONAL LATTICES

In this section, we give some results about Voronoï cells in dimensions two and three, which are crucial to the complexity analysis of the greedy algorithm described in Section 4. More precisely, the analysis is based on the Gap Lemma (given in Subsection 9.3), which is derived from the study of Voronoï cells in the case of ε-greedy-reduced vectors (see Subsection 9.2), itself derived from the study of Voronoï cells for Minkowski-reduced bases (in Subsection 9.1).

9.1 Voronoï Cells in the Case of Minkowski-Reduced Bases

We start by giving some simple bounds on the diameter of the Voronoï cell and on the Gram-Schmidt orthogonalization of a Minkowski-reduced basis:

LEMMA 9.1.1. *Let $d \geq 1$. Let $[\mathbf{b}_1, \ldots, \mathbf{b}_d]_{\leq}$ be a basis of a lattice L. Then $\rho(L) \leq \frac{\sqrt{d}}{2} \cdot \|\mathbf{b}_d\|$. As a consequence, if the basis $[\mathbf{b}_1, \ldots, \mathbf{b}_d]_{\leq}$ is a Minkowski-reduced basis, then $\|\mathbf{b}_d^*\| \geq \frac{\sqrt{5-d}}{2} \cdot \|\mathbf{b}_d\|$.*

PROOF. The first part of the lemma is very classical and several different proofs can be found in the literature. For example, we can use the inequalities $\rho(L)^2 \leq \frac{1}{4}\sum_{i \leq d} \|\mathbf{b}_i^*\|^2 \leq \frac{d}{4}\|\mathbf{b}_d\|^2$, where the first one derives from Babai's nearest plane algorithm [Babai 1986].

Suppose now that the basis $[\mathbf{b}_1, \ldots, \mathbf{b}_d]_{\leq}$ is Minkowski-reduced. Then the orthogonal projection of the vector $\mathbf{b}_d$ onto the linear span of $[\mathbf{b}_1, \ldots, \mathbf{b}_{d-1}]_{\leq}$ is in $\mathrm{Vor}(\mathbf{b}_1, \ldots, \mathbf{b}_{d-1})$. Therefore, by the Pythagorean theorem, we get: $\|\mathbf{b}_d^*\|^2 \geq \|\mathbf{b}_d\|^2 - \frac{d-1}{4}\|\mathbf{b}_{d-1}\|^2$. The fact that $\|\mathbf{b}_{d-1}\| \leq \|\mathbf{b}_d\|$ completes the proof. □

The following lemma provides the possible Voronoï vectors of a lattice of dimension two given by a Minkowski-reduced basis (recall that we cannot directly use Theorem 2.3.1 because it only considers strict Voronoï coordinates). Such a basis confines the coordinates of the Voronoï vectors:

LEMMA 9.1.2. *In dimension two, the possible Voronoï coords are $(1, 0)$ and $(1, 1)$, modulo any change of signs and permutation of coordinates, i.e., any nonzero $(\varepsilon_1, \varepsilon_2)$ where $|\varepsilon_1|, |\varepsilon_2| \leq 1$.*

The proof relies on a detailed study of the quantity $\|(2x_1 + \varepsilon_1) \cdot \mathbf{b}_1 + (2x_2 + \varepsilon_2) \cdot \mathbf{b}_2\|^2 - \|\varepsilon_1\mathbf{b}_1 + \varepsilon_2\mathbf{b}_2\|^2$, where the basis $[\mathbf{b}_1, \mathbf{b}_2]_{\leq}$ is Minkowski-reduced, $\varepsilon_1, \varepsilon_2 \in \{0, 1\}$ and $x_1, x_2 \in \mathbb{Z}$. Indeed, since the Voronoï coords of a lattice L are given by the minima of the non-zero cosets of $L/2L$, it suffices to show that if $x_1 \neq 0$ or $x_2 \neq 0$, then this expression is strictly positive.

PROOF. Recall that the possible Voronoï coords can be obtained by considering the short elements of $L/2L$, given a Minkowski-reduced basis of L. Let $[\mathbf{b}_1, \mathbf{b}_2]_{\leq}$ be a reduced basis. By eventually replacing the vector $\mathbf{b}_i$ by $-\mathbf{b}_i$ for $i \in \{1, 2\}$, it is clearly sufficient to show that for any $x_1, x_2 \geq 0$, and for any $\varepsilon_1, \varepsilon_2 \in \{0, 1\}$, if $x_1 \geq 1$ or $x_2 \geq 1$, then:

$$\|(2x_1 + \varepsilon_1) \cdot \mathbf{b}_1 + (2x_2 + \varepsilon_2) \cdot \mathbf{b}_2\|^2 > \|\varepsilon_1 \cdot \mathbf{b}_1 + \varepsilon_2 \cdot \mathbf{b}_2\|^2.$$

First of all:

$$\begin{aligned}\|(2x_1+\varepsilon_1)\cdot\mathbf{b}_1 \;+\; (2x_2+\varepsilon_2)\cdot\mathbf{b}_2\|^2 - \|\varepsilon_1\cdot\mathbf{b}_1+\varepsilon_2\cdot\mathbf{b}_2\|^2 \\ = \left((2x_1+\varepsilon_1)^2-\varepsilon_1^2\right)\cdot\|\mathbf{b}_1\|^2 + \left((2x_2+\varepsilon_2)^2-\varepsilon_2^2\right)\cdot\|\mathbf{b}_2\|^2 \\ +2((2x_1+\varepsilon_1)(2x_2+\varepsilon_2)-\varepsilon_1\varepsilon_2)\cdot\langle\mathbf{b}_1,\mathbf{b}_2\rangle.\end{aligned}$$

Since $x_1, x_2 \geq 0$, we have that $(2x_2+\varepsilon_2)^2-\varepsilon_2^2 \geq 0$ and $(2x_1+\varepsilon_1)(2x_2+\varepsilon_2)-\varepsilon_1\varepsilon_2 \geq 0$. Moreover, the basis $[\mathbf{b}_1,\mathbf{b}_2]_\leq$ is reduced and therefore $\|\mathbf{b}_2\| \geq \|\mathbf{b}_1\|$ and $2\langle\mathbf{b}_1,\mathbf{b}_2\rangle \geq -\|\mathbf{b}_1\|^2$. From these facts, we obtain:

$$\begin{aligned}\|(2x_1+\varepsilon_1)\cdot\mathbf{b}_1 \;+\; (2x_2+\varepsilon_2)\cdot\mathbf{b}_2\|^2 - \|\varepsilon_1\mathbf{b}_1+\varepsilon_2\mathbf{b}_2\|^2 \\ \geq\; 2\left[2x_1^2+2x_2^2-2x_1x_2+x_1(2\varepsilon_1-\varepsilon_2)+x_2(2\varepsilon_2-\varepsilon_1)\right]\cdot\|\mathbf{b}_1\|^2.\end{aligned}$$

This last expression is strictly positive as long as $(x_1,x_2)\neq(0,0)$. Indeed:

—if $\varepsilon_1=\varepsilon_2=0$, the factor is $4\left((x_1-x_2)^2+x_1x_2\right)$,

—if $\varepsilon_1=0$ and $\varepsilon_2=1$, the factor is $2\left(x_2^2+2x_2+(x_2-x_1)^2+(x_1^2-x_1)\right)$,

—the case $\varepsilon_1=1$ and $\varepsilon_2=0$ is symmetric,

—if $\varepsilon_1=\varepsilon_2=1$, the factor is $2\left((x_2-x_1)^2+(x_2^2+x_2)+(x_1^2+x_1)\right)$.

□

We generalize this analysis to the three-dimensional case. The underlying ideas of the proof are the same, but the increase of the number of variables makes the analysis more tedious.

LEMMA 9.1.3. *In dimension three, the possible Voronoï coordinates are among* $(1,0,0)$, $(1,1,0)$, $(1,1,1)$ *and* $(2,1,1)$, *modulo any change of signs and permutation of coordinates.*

PROOF. We generalize the proof of Lemma 9.1.2. We show that for any integers x_1,x_2,x_3 and any $\varepsilon_1,\varepsilon_2,\varepsilon_3\in\{0,1\}$, if $(2x_1+\varepsilon_1,2x_2+\varepsilon_2,2x_3+\varepsilon_3)$ is not in the desired list of Voronoï coords, then:

$$\|(2x_1+\varepsilon_1)\cdot\mathbf{b}_1+(2x_2+\varepsilon_2)\cdot\mathbf{b}_2+(2x_3+\varepsilon_3)\cdot\mathbf{b}_3\|^2-\|\varepsilon_1\mathbf{b}_1+\varepsilon_2\mathbf{b}_2+\varepsilon_3\mathbf{b}_3\|^2>0.$$

By replacing the vector $\mathbf{b}_i$ by $-\mathbf{b}_i$, we see that wlog the proof can be restricted to the case $x_1,x_2,x_3\geq 0$. Moreover, because we already considered the two-dimensional case in Lemma 9.1.2, we can suppose that for any $i\in\{1,2,3\}$, we have $(x_i,\varepsilon_i)\neq(0,0)$.

From Lemma 9.1.1, we know that since the basis $[\mathbf{b}_1,\mathbf{b}_2,\mathbf{b}_3]_\leq$ is Minkowski-reduced, we have $\|\mathbf{b}_3^*\|\geq\|\mathbf{b}_3\|/\sqrt{2}$. As a consequence, if $2x_3+\varepsilon_3\geq 5$, then:

$$\|(2x_1+\varepsilon_1)\cdot\mathbf{b}_1+(2x_2+\varepsilon_2)\cdot\mathbf{b}_2+(2x_3+\varepsilon_3)\cdot\mathbf{b}_3\|^2\geq 25\cdot\|\mathbf{b}_3^*\|^2\geq\frac{25}{2}\cdot\|\mathbf{b}_3\|^2,$$

and the triangular inequality gives that $\|\varepsilon_1\cdot\mathbf{b}_1+\varepsilon_2\cdot\mathbf{b}_2+\varepsilon_3\cdot\mathbf{b}_3\|^2\leq 9\cdot\|\mathbf{b}_3\|^2$. This gives the result when $2x_3+\varepsilon_3\geq 5$. The same argument holds for $(x_3,\varepsilon_3)=(2,0)$, and for $(x_3,\varepsilon_3)\in\{(1,1),(1,0)\}$ with $\varepsilon_1\cdot\varepsilon_2=0$. Therefore, it remains to consider

the three cases $(x_3, \varepsilon_3) = (1,1)$ with $\varepsilon_1 = \varepsilon_2 = 1$, $(x_3, \varepsilon_3) = (1,0)$ with $\varepsilon_1 = \varepsilon_2 = 1$, and $(x_3, \varepsilon_3) = (0,1)$.

Case 1: Suppose that $(x_3, \varepsilon_3) = (1,1)$ and $\varepsilon_1 = \varepsilon_2 = 1$. Since the ordered basis $[\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3]_{\leq}$ is Minkowski-reduced, we have $\langle \mathbf{b}_i, \mathbf{b}_j \rangle \geq -\|\mathbf{b}_i\|^2/2$ for any $1 \leq i < j \leq 3$, which gives:

$$\begin{aligned}
& \|(2x_1+1)\cdot\mathbf{b}_1 + (2x_2+1)\cdot\mathbf{b}_2 + 3\cdot\mathbf{b}_3\|^2 - \|\mathbf{b}_1+\mathbf{b}_2+\mathbf{b}_3\|^2 \\
= \; & 4\left(x_1^2+x_1\right)\cdot\|\mathbf{b}_1\|^2 + 4\left(x_2^2+x_2\right)\cdot\|\mathbf{b}_2\|^2 + 8\cdot\|\mathbf{b}_3\|^2 \\
& +4(3x_1+1)\cdot\langle\mathbf{b}_1,\mathbf{b}_3\rangle + 4(3x_2+1)\cdot\langle\mathbf{b}_2,\mathbf{b}_3\rangle + 4(2x_1x_2+x_1+x_2)\cdot\langle\mathbf{b}_1,\mathbf{b}_2\rangle \\
\geq \; & \left(4x_1^2 - 4x_1x_2 - 4x_1 - 2x_2 - 2\right)\cdot\|\mathbf{b}_1\|^2 + \left(4x_2^2 - 2x_2 - 2\right)\|\mathbf{b}_2\|^2 + 8\|\mathbf{b}_3\|^2.
\end{aligned}$$

If $x_2 = 0$, it suffices to lower-bound $\left(x_1^2 - x_1\right)\cdot\|\mathbf{b}_1\|^2 + \|\mathbf{b}_3\|^2$, which is always greater than $\|\mathbf{b}_3\|^2$ and therefore strictly positive. Suppose now that $x_2 \geq 1$. Then $4x_2^2 - 2x_2 - 2 \geq 0$ and we obtain:

$$\begin{aligned}
\|(2x_1+1)\cdot\mathbf{b}_1 \; + \; & (2x_2+1)\cdot\mathbf{b}_2 + 3\cdot\mathbf{b}_3\|^2 - \|\mathbf{b}_1+\mathbf{b}_2+\mathbf{b}_3\|^2 \\
& \geq \; 4\left(x_1^2 + x_2^2 - x_1x_2 - x_1 - x_2 + 1\right)\cdot\|\mathbf{b}_1\|^2 \\
& \geq \; 4\left((x_1-x_2)^2 + (x_1x_2 - x_1 - x_2) + 1\right)\cdot\|\mathbf{b}_1\|^2.
\end{aligned}$$

It is clear that this last expression is strictly positive for any $x_1, x_2 \geq 0$ except when $x_1 = x_2 = 1$. In this last situation, we use the fact that $\|3\cdot\mathbf{b}_1 + 3\cdot\mathbf{b}_2 + 3\cdot\mathbf{b}_3\|^2 - \|\mathbf{b}_1+\mathbf{b}_2+\mathbf{b}_3\|^2 = 8\cdot\|\mathbf{b}_1+\mathbf{b}_2+\mathbf{b}_3\|^2$.

Case 2: Suppose now that $(x_3, \varepsilon_3) = (1,0)$ and $\varepsilon_1 = \varepsilon_2 = 1$. Similarly, we have:

$$\begin{aligned}
& \|(2x_1+1)\cdot\mathbf{b}_1 + (2x_2+1)\cdot\mathbf{b}_2 + 2\cdot\mathbf{b}_3\|^2 - \|\mathbf{b}_1+\mathbf{b}_2\|^2 \\
= \; & 4\left(x_1^2+x_1\right)\cdot\|\mathbf{b}_1\|^2 + 4\left(x_2^2+x_2\right)\cdot\|\mathbf{b}_2\|^2 + 4\cdot\|\mathbf{b}_3\|^2 \\
& +4(2x_1+1)\cdot\langle\mathbf{b}_1,\mathbf{b}_3\rangle + 4(2x_2+1)\cdot\langle\mathbf{b}_2,\mathbf{b}_3\rangle + 4(2x_1x_2+x_1+x_2)\cdot\langle\mathbf{b}_1,\mathbf{b}_2\rangle \\
\geq \; & \left(4x_1^2 - 4x_1x_2 - 2x_1 - 2x_2 - 2\right)\cdot\|\mathbf{b}_1\|^2 + \left(4x_2^2 - 2\right)\cdot\|\mathbf{b}_2\|^2 + 4\|\mathbf{b}_3\|^2.
\end{aligned}$$

If $x_2 = 0$, it suffices to lower-bound $\left(2x_1^2 - x_1 - 1\right)\cdot\|\mathbf{b}_1\|^2 + \|\mathbf{b}_3\|^2$, which is strictly positive if $x_1 \geq 1$. If $x_1 = 0$, then we have one of the possible Voronoï coords. Suppose now that $x_2 \geq 1$. In that case $4x_2^2 - 2 \geq 0$, which ensures that:

$$\begin{aligned}
\|(2x_1+1)\cdot\mathbf{b}_1 \; + \; & (2x_2+1)\cdot\mathbf{b}_2 + 2\cdot\mathbf{b}_3\|^2 - \|\mathbf{b}_1+\mathbf{b}_2\|^2 \\
& \geq \; 2\left(2x_1^2 + 2x_2^2 - 2x_1x_2 - x_1 - x_2\right)\cdot\|\mathbf{b}_1\|^2 \\
& \geq \; 2\left((x_1-x_2)^2 + (x_1^2 - x_1) + (x_2^2 - x_2)\right)\cdot\|\mathbf{b}_1\|^2.
\end{aligned}$$

If $x_1 \geq 2$ or $x_2 \geq 2$ or $x_1 \neq x_2$, this is strictly positive. Therefore it remains to consider the case $x_1 = x_2 = 1$. We have:

$$\|3\cdot\mathbf{b}_1+3\cdot\mathbf{b}_2+2\cdot\mathbf{b}_3\|^2 - \|\mathbf{b}_1+\mathbf{b}_2\|^2 = 4\cdot\left(\|\mathbf{b}_3\|^2 + 3\cdot\langle\mathbf{b}_3, \mathbf{b}_1+\mathbf{b}_2\rangle + 2\cdot\|\mathbf{b}_1+\mathbf{b}_2\|^2\right).$$

Since the basis $[\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3]_{\leq}$ is reduced, we have $\langle \mathbf{b}_3, \mathbf{b}_1+\mathbf{b}_2\rangle \geq -\|\mathbf{b}_1+\mathbf{b}_2\|^2/2$,

which gives the expected result.

Case 3: Suppose now that $(x_3, \varepsilon_3) = (0, 1)$. Similarly, we have the inequalities:

$$\begin{aligned}\|(2x_1+\varepsilon_1)\cdot\mathbf{b}_1 \;+\; (2x_2+\varepsilon_2)\cdot\mathbf{b}_2+\mathbf{b}_3\|^2 - \|\varepsilon_1\cdot\mathbf{b}_1+\varepsilon_2\cdot\mathbf{b}_2+\mathbf{b}_3\|^2 \\ = 4\left(x_1^2+\varepsilon_1 x_1\right)\cdot\|\mathbf{b}_1\|^2 + 4\left(x_2^2+\varepsilon_2 x_2\right)\cdot\|\mathbf{b}_2\|^2 + 4x_1\cdot\langle\mathbf{b}_1,\mathbf{b}_3\rangle \\ +4x_2\cdot\langle\mathbf{b}_2,\mathbf{b}_3\rangle + 4(2x_1x_2+x_1\varepsilon_2+x_2\varepsilon_1)\cdot\langle\mathbf{b}_1,\mathbf{b}_2\rangle \\ \geq \left(4x_1^2-4x_1x_2+(4\varepsilon_1-2-2\varepsilon_2)x_1-2x_2\varepsilon_1\right)\cdot\|\mathbf{b}_1\|^2 \\ +\left(4x_2^2+(4\varepsilon_2-2)x_2\right)\cdot\|\mathbf{b}_2\|^2.\end{aligned}$$

If $x_2 = 0$, it suffices to lower-bound $4x_1^2+(4\varepsilon_1-2-2\varepsilon_2)x_1$. It is strictly positive as soon as $x_1 \geq 1$ except in the case $(x_1, \varepsilon_1, \varepsilon_2) = (1, 0, 1)$, which corresponds to one of the possible Voronoï coords. If $x_1 = 0$, we only have possible Voronoï coords. Suppose now that $x_2 \geq 1$. In that case $4x_2^2+(4\varepsilon_2-2)x_2 \geq 0$ and:

$$\begin{aligned}\|(2x_1+\varepsilon_1)\cdot\mathbf{b}_1+(2x_2+\varepsilon_2)\cdot\mathbf{b}_2+\mathbf{b}_3\|^2 - \|\varepsilon_1\cdot\mathbf{b}_1+\varepsilon_2\cdot\mathbf{b}_2+\mathbf{b}_3\|^2 \\ \geq \left(4x_1^2+4x_2^2-4x_1x_2+(4\varepsilon_1-2-2\varepsilon_2)x_1+(4\varepsilon_2-2-2\varepsilon_1)x_2\right)\cdot\|\mathbf{b}_1\|^2.\end{aligned}$$

For $(\varepsilon_1, \varepsilon_2) = (0, 0)$, we get $2\left((x_1-x_2)^2+(x_1^2-x_1)+(x_2^2-x_2)\right)$, which is strictly positive as soon as $x_1 \neq x_2$ or $x_1 \geq 2$ or $x_2 \geq 2$. The only remaining case that does not provide a possible Voronoï coord is $x_1 = x_2 = 1$. Notice that $\|2\mathbf{b}_1+2\mathbf{b}_2+\mathbf{b}_3\|^2 > \|\mathbf{b}_3\|^2$ is equivalent to $\|\mathbf{b}_1+\mathbf{b}_2\|^2+\langle\mathbf{b}_1+\mathbf{b}_2,\mathbf{b}_3\rangle > 0$, which is implied by $\langle\mathbf{b}_1+\mathbf{b}_2,\mathbf{b}_3\rangle \geq -\|\mathbf{b}_1+\mathbf{b}_2\|^2/2$ (the vector $\mathbf{b}_3$ has its orthogonal projection onto the span of $[\mathbf{b}_1, \mathbf{b}_2]$ inside $\mathrm{Vor}(\mathbf{b}_1, \mathbf{b}_2)$).

For $(\varepsilon_1, \varepsilon_2) = (1, 0)$, we get $2(x_1-x_2)^2+2(x_2^2-2x_2)+2x_1^2+2x_1$. If $x_2 \geq 2$, this is clearly strictly positive. If $x_2 = 1$, we obtain $4x_1^2-2x_1$, which is strictly positive unless $x_1 = 0$ (one of the possible Voronoï coords). We have already considered the case $x_2 = 0$. The case $(\varepsilon_1, \varepsilon_2) = (0, 1)$ is symmetric.

Finally, if $(\varepsilon_1, \varepsilon_2) = (1, 1)$, we obtain $2\left((x_1-x_2)^2+x_1^2+x_2^2\right)$, which is strictly positive unless $x_1 = x_2 = 0$ (one of the possible Voronoï coords). This completes the proof of the lemma. □

The possible Voronoï coord $(2, 1, 1)$ creates difficulties when analyzing the greedy algorithm in dimension four because it contains a two, which cannot be handled with the greedy argument used for the ones. We tackle this problem as follows: we show that when $(2, 1, 1)$ happens to be a Voronoï coord, the lattice has a very specific shape, for which the behavior of the algorithm is well-understood.

LEMMA 9.1.4. *Suppose the basis $[\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3]_{\leq}$ is Minkowski-reduced.*

(1) If $(s_1, s_2, 2)$ is a Voronoï coord with $s_i = \pm 1$ for $i \in \{1, 2\}$, then $\|\mathbf{b}_1\| = \|\mathbf{b}_2\| = \|\mathbf{b}_3\|$, $\langle\mathbf{b}_1, \mathbf{b}_2\rangle = 0$ and $\langle\mathbf{b}_i, \mathbf{b}_3\rangle = -\frac{s_i}{2}\cdot\|\mathbf{b}_1\|^2$ for $i \in \{1, 2\}$.

(2) If $(s_1, 2, s_3)$ is a Voronoï coord with $s_i = \pm 1$ for $i \in \{1, 3\}$, then $\|\mathbf{b}_1\| = \|\mathbf{b}_2\|$. Moreover, if $\|\mathbf{b}_1\| = \|\mathbf{b}_2\| = \|\mathbf{b}_3\|$, then $\langle\mathbf{b}_1, \mathbf{b}_3\rangle = 0$ and $\langle\mathbf{b}_i, \mathbf{b}_2\rangle = -\frac{s_i}{2}\cdot\|\mathbf{b}_1\|^2$ for $i \in \{1, 3\}$.

(3) If $(2, s_2, s_3)$ is a Voronoï coord with $s_i = \pm 1$ for $i \in \{2, 3\}$ and $\|\mathbf{b}_1\| = \|\mathbf{b}_2\| = \|\mathbf{b}_3\|$, then $\langle\mathbf{b}_2, \mathbf{b}_3\rangle = 0$ and $\langle\mathbf{b}_i, \mathbf{b}_1\rangle = -\frac{s_i}{2}\cdot\|\mathbf{b}_1\|^2$ for $i \in \{2, 3\}$.

PROOF. Wlog we suppose that for any i, we have $s_i = 1$. In the first situation we consider the inequality $\|\mathbf{b}_1 + \mathbf{b}_2 + 2\cdot\mathbf{b}_3\|^2 \leq \|\mathbf{b}_1 + \mathbf{b}_2\|^2$: it is equivalent to $\|\mathbf{b}_3\|^2 + \langle \mathbf{b}_1, \mathbf{b}_3\rangle + \langle \mathbf{b}_2, \mathbf{b}_3\rangle \leq 0$. Since the basis is reduced, we must have $\langle \mathbf{b}_1, \mathbf{b}_3\rangle \geq -\|\mathbf{b}_1\|^2/2$ and $\langle \mathbf{b}_2, \mathbf{b}_3\rangle \geq -\|\mathbf{b}_2\|^2/2$. Thus $2\cdot\|\mathbf{b}_3\|^2 - \|\mathbf{b}_1\|^2 - \|\mathbf{b}_2\|^2 \leq 0$. Consequently, the length equalities hold and the inequalities on the scalar products above are equalities. It remains to prove that $\langle \mathbf{b}_1, \mathbf{b}_2\rangle = 0$. Since $\mathbf{b}_1$ is a shortest vector, we have $\|\mathbf{b}_3 + \mathbf{b}_2 + \mathbf{b}_1\|^2 \geq \|\mathbf{b}_1\|^2$, which is equivalent to $\langle \mathbf{b}_1, \mathbf{b}_2\rangle \geq 0$. Moreover, we have $\langle \mathbf{b}_1, \mathbf{b}_2\rangle \leq 0$ from the expansion of $\|\mathbf{b}_1 + \mathbf{b}_2 + 2\cdot\mathbf{b}_3\|^2 \leq \|\mathbf{b}_1 - \mathbf{b}_2\|^2$.

In the second situation, expanding $\|\mathbf{b}_1 + 2\cdot\mathbf{b}_2 + \mathbf{b}_3\|^2 \leq \|\mathbf{b}_1 + \mathbf{b}_3\|^2$ gives the length equality. In the case of the additional hypothesis $\|\mathbf{b}_1\| = \|\mathbf{b}_2\| = \|\mathbf{b}_3\|$, the basis $[\mathbf{b}_1, \mathbf{b}_3, \mathbf{b}_2]_{\leq}$ is also reduced and we can apply the result of the first situation. This last argument also holds in the third situation. □

9.2 Voronoï Cells in the Case of ε-Greedy-Reduced Vectors

We extend the results of the previous subsection to the case of ε-greedy-reduced vectors. The idea is that if we compactify the set of Minkowski-reduced bases and slightly enlarge it, the possible Voronoï coords remain the same. Unfortunately, by doing so, some of the vectors we consider may be zero and this creates an infinity of possible Voronoï coords: for example, if $\mathbf{b}_1 = \mathbf{0}$, any pair $(x_1, 0)$ is a Voronoï coord of $[\mathbf{b}_1, \mathbf{b}_2]_{\leq}$. To tackle this problem, we restrict to vectors $\mathbf{b}_i$ with "similar" lengths. More precisely, we use the so-called Topological Lemma: if we can guarantee that the possible Voronoï coords of the enlargement of the initial compact set of bases are bounded, then for a sufficiently small enlargement, the possible Voronoï coords remain the same. We first give rather simple results on ε-greedy-reduced vectors and their Gram-Schmidt orthogonalization, then we introduce the Topological Lemma (Lemma 9.2.3), from which we finally derive the relaxed versions of Lemmata 9.1.2, 9.1.3 and 9.1.4.

LEMMA 9.2.1. *For any $\varepsilon > 0$, if $[\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3]_{\leq}$ are ε-greedy-reduced, then the following inequalities hold:*

$$\forall i < j,\ |\langle \mathbf{b}_i, \mathbf{b}_j\rangle| \leq \frac{1+\varepsilon}{2}\cdot\|\mathbf{b}_i\|^2,$$
$$\forall s_1, s_2 \in \{-1, 1\}, |\langle \mathbf{b}_3, s_1\cdot\mathbf{b}_1 + s_2\cdot\mathbf{b}_2\rangle| \leq \frac{1+\varepsilon}{2}\cdot\|s_1\cdot\mathbf{b}_1 + s_2\cdot\mathbf{b}_2\|^2.$$

PROOF. Since $[\mathbf{b}_1, \mathbf{b}_2]_{\leq}$ are ε-greedy-reduced, we have that $\mathbf{b}_2' \in (1+\varepsilon)\cdot\mathrm{Vor}(\mathbf{b}_1)$, where $\mathbf{b}_2'$ is the orthogonal projection of the vector $\mathbf{b}_2$ onto the span of $\mathbf{b}_1$. As a consequence, we can write $\mathbf{b}_2' = (1+\varepsilon)\cdot\mathbf{u}$ with $\mathbf{u} \in \mathrm{Vor}(\mathbf{b}_1)$. By expanding the inequalities $\|\mathbf{u} \pm \mathbf{b}_1\|^2 \geq \|\mathbf{u}\|^2$, we obtain that $|\langle \mathbf{u}, \mathbf{b}_1\rangle| \leq \|\mathbf{b}_1\|^2/2$. Therefore, $|\langle \mathbf{b}_3, \mathbf{b}_1\rangle| \leq \frac{1+\varepsilon}{2}\cdot\|\mathbf{b}_1\|^2$.

Moreover $[\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3]_{\leq}$ are ε-greedy-reduced, so that $\mathbf{b}_3' \in (1+\varepsilon)\cdot\mathrm{Vor}(\mathbf{b}_1, \mathbf{b}_2)$, where $\mathbf{b}_3'$ is the orthogonal projection of the vector $\mathbf{b}_3$ onto the span of $[\mathbf{b}_1, \mathbf{b}_2]_{\leq}$. As a consequence, we can write $\mathbf{b}_3' = (1+\varepsilon)\cdot\mathbf{u}$ with $\mathbf{u} \in \mathrm{Vor}(\mathbf{b}_1, \mathbf{b}_2)$. We proceed exactly as above by expanding the inequalities $\|\mathbf{u} + s_1\cdot\mathbf{b}_1 + s_2\cdot\mathbf{b}_2\|^2 \geq \|\mathbf{u}\|^2$ for any $s_1, s_2 \in \{-1, 0, 1\}$, and this provides the result. □

The previous lemma implies that if $[\mathbf{b}_1, \ldots, \mathbf{b}_d]_{\leq}$ are ε-greedy-reduced, the only case for which the $\mathbf{b}_i$'s can be linearly dependent is when some of them are zero,

but this case cannot be avoided since we need compactifying the set of Minkowski-reduced bases. The following lemma generalizes Lemma 9.1.1. It shows that even with ε-greedy-reduced vectors, if the dimension is below four then the Gram-Schmidt orthogonalization process cannot arbitrarily decrease the lengths of the initial vectors.

LEMMA 9.2.2. *There exists $C > 0$ such that for any $1 \leq d \leq 4$ and any sufficiently small $\varepsilon > 0$, if $[\mathbf{b}_1, \ldots, \mathbf{b}_d]_{\leq}$ are ε-greedy-reduced vectors, then we have $\|\mathbf{b}_d^*\| \geq C \cdot \|\mathbf{b}_d\|$.*

PROOF. Since $[\mathbf{b}_1, \ldots, \mathbf{b}_d]_{\leq}$ are ε-greedy-reduced, we know that if $\mathbf{b}'_d$ is the orthogonal projection of the vector $\mathbf{b}_d$ onto the span of $[\mathbf{b}_1, \ldots, \mathbf{b}_{d-1}]_{\leq}$, then $\mathbf{b}'_d \in (1+\varepsilon) \cdot \mathrm{Vor}(\mathbf{b}_1, \ldots, \mathbf{b}_{d-1})$. Therefore, because of Lemma 9.1.1 and because the vectors are ordered,

$$\|\mathbf{b}'_d\| \leq (1+\varepsilon)\frac{\sqrt{d-1}}{2} \cdot \|\mathbf{b}_{d-1}\| \leq (1+\varepsilon)\frac{\sqrt{d-1}}{2} \cdot \|\mathbf{b}_d\|.$$

Besides, from the Pythagorean theorem, we have $\|\mathbf{b}_d\|^2 = \|\mathbf{b}_d^*\|^2 + \|\mathbf{b}'_d\|^2$, which completes the proof. □

The Topological Lemma is the key argument when extending the results on possible Voronoï coords from Minkowski-reduced bases to ε-greedy-reduced vectors. When applying it, X_0 will correspond to the x_i's, K_0 to the $\mathbf{b}_i$'s that are ε-greedy-reduced, X to the possible Voronoï coordinates, K to a compact subset of the Minkowski-reduced bases, and f to the continuous function of real variables $f : (y_i)_{i \leq d}, (\mathbf{b}_i)_{i \leq d} \longrightarrow \|y_1\mathbf{b}_1 + \ldots + y_d\mathbf{b}_d\|$.

LEMMA 9.2.3 TOPOLOGICAL LEMMA. *Let $n, m \geq 1$. Let X_0 and K_0 be compact sets of $\mathbb{R}^n$ and $\mathbb{R}^m$. Let f be a continuous function from $K_0 \times X_0$ to $\mathbb{R}$. For any $a \in K_0$ we define $M_a = \{x \in X_0 \cap \mathbb{Z}^n, f(a,x) = \min_{x' \in X_0 \cap \mathbb{Z}^n} f(a,x')\}$. Let $K \subset K_0$ be a compact and $X = \cup_{a \in K} M_a \subset X_0 \cap \mathbb{Z}^n$. With these notations, there exists $\varepsilon > 0$ such that if $b \in K_0$ satisfies $\mathrm{dist}(b, K) \leq \varepsilon$, we have $M_b \subset X$.*

PROOF. First, all the notations of the result make sense: $X_0 \cap \mathbb{Z}^n$ is finite so the minimum of $f(a, \cdot)$ over it does exist and M_a is finite. Since $X \subset X_0 \cap \mathbb{Z}^n$, X is finite. Finally, since K is compact, the notation $\mathrm{dist}(\cdot, K)$ makes sense too.

For each $x \in X_0$ we define $K_x = \{a \in K_0, x \in M_a\}$. The set K_x is compact. Indeed, it is obviously bounded, and if (a_k) is a sequence of elements of K_x that converges towards an $a \in K_0$, we show that $a \in K_x$. For all $x' \in X_0 \cap \mathbb{Z}^n$ and for all k, we have $f(a_k, x) \leq f(a_k, x')$. By continuity, this holds for a too, which proves that $x \in M_a$.

Now we fix an $x \in X_0 \cap \mathbb{Z}^n \setminus X$. Since K_x and K are both compact and $x \notin X$ (which implies $K \cap K_x = \emptyset$), $\mathrm{dist}(K_x, K) > 0$. Finally, set

$$\varepsilon = \frac{1}{2}\min\left(\mathrm{dist}(K_x, K), x \in (X_0 \cap \mathbb{Z}^n) \setminus X\right),$$

which exists since $(X_0 \cap \mathbb{Z}^n) \setminus X$ is finite. Now, let $b4 \in K_0$ such that $\mathrm{dist}(b, K) \leq \varepsilon$. For any $x_0 \in M_b$, we have $b \in K_{x_0}$. Then necessarily $x_0 \in X$, since otherwise one would have $\mathrm{dist}(K_{x_0}, K) > \varepsilon \geq \mathrm{dist}(b, K)$, which cannot be the case because $b \in K_{x_0}$. □

In order to apply the Topological Lemma, we need to map the relaxed bases into a compact set. For any $\varepsilon \geq 0$ and any $\alpha \in [0,1]$, we define:

$$\begin{aligned} K_2(\varepsilon,\alpha) &= \{(\mathbf{b}_1,\mathbf{b}_2), \mathbf{b}_1, \mathbf{b}_2 \ \varepsilon\text{-greedy-reduced}, \alpha \leq \|\mathbf{b}_1\| \leq \|\mathbf{b}_2\| = 1\} \\ K_3(\varepsilon,\alpha) &= \{(\mathbf{b}_1,\mathbf{b}_2,\mathbf{b}_3), \mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3 \ \varepsilon\text{-greedy-reduced}, \\ &\qquad \alpha \leq \|\mathbf{b}_1\| \leq \|\mathbf{b}_2\| \leq \|\mathbf{b}_3\| = 1\}. \end{aligned}$$

LEMMA 9.2.4. *If $\varepsilon \geq 0$ and $\alpha \in [0,1]$, $K_2(\varepsilon,\alpha)$ and $K_3(\varepsilon,\alpha)$ are compact sets.*

The following lemma is the relaxed version of Lemma 9.1.2. It can also be viewed as a reciprocal to Lemma 9.2.1.

LEMMA 9.2.5. *There exists $\varepsilon > 0$ such that for any $\alpha \in (0,1]$, the possible Voronoï coords of $[\mathbf{b}_1,\mathbf{b}_2]_\leq \in K_2(\varepsilon,\alpha)$ are the same as for Minkowski-reduced bases, i.e., $(1,0)$ and $(1,1)$, modulo any change of signs and permutation of coordinates.*

PROOF. Recall that there is a set of possible Voronoï coords for each non-zero element of $(\mathbb{Z}/2\mathbb{Z})^2$: we look at the minima of the cosets of $L/2L$. Since there is a finite number of such cosets (three in dimension two), we treat them separately. Let $(a_1,a_2) \in \{0,1\}^2$. We are looking for the pairs $(k_1,k_2) \in \mathbb{Z}^2$ that minimize the quantity $\|(a_1+2k_1)\cdot\mathbf{b}_1 + (a_2+2k_2)\cdot\mathbf{b}_2\|$, where $[\mathbf{b}_1,\mathbf{b}_2]_\leq$ are ε-greedy-reduced. We first prove that the minimum over (k_1,k_2) can be taken over a finite domain. Notice that if (k_1^*,k_2^*) is optimal:

$$2 \geq \|\mathbf{b}_1\| + \|\mathbf{b}_2\| \geq \|a_1\cdot\mathbf{b}_1 + a_2\cdot\mathbf{b}_2\| \geq \|(a_1+2k_1^*)\cdot\mathbf{b}_1 + (a_2+2k_2^*)\cdot\mathbf{b}_2\|.$$

Moreover, Lemma 9.2.2 gives that:

$$\|(a_1+2k_1^*)\cdot\mathbf{b}_1 + (a_2+2k_2^*)\cdot\mathbf{b}_2\| \geq |a_2+2k_2^*|\cdot\|\mathbf{b}_2^*\| \geq |a_2+2k_2^*|C,$$

which gives the result for k_2^*. By applying the triangular inequality, we get the result for k_1^*:

$$|a_1+2k_1^*|\alpha \leq \|(a_1+2k_1^*)\cdot\mathbf{b}_1\| \leq 2 + \|(a_2+2k_2^*)\cdot\mathbf{b}_2\| \leq 2 + |a_2+2k_2^*|.$$

From this we deduce that $(k_1^*,k_2^*) \in \mathbb{Z}^2$ can be bounded independently of $(\mathbf{b}_1,\mathbf{b}_2)$. From Lemma 9.2.4, we know that $K_2(\varepsilon,\alpha)$ is compact and therefore we can apply the Topological Lemma. This gives the expected result. □

We now relax Lemma 9.1.3 in the same manner. To do this, we proceed exactly like in the proof above.

LEMMA 9.2.6. *There exists $\varepsilon > 0$ such that for any $\alpha \in (0,1]$, the possible Voronoï coords of $[\mathbf{b}_1,\mathbf{b}_2,\mathbf{b}_3]_\leq \in K_3(\varepsilon,\alpha)$ are the same as for Minkowski-reduced bases.*

PROOF. We consider each non-zero coset of $L/2L$ separately (there are seven of them in dimension three). Let $(a_1,a_2,a_3) \in \{0,1\}^3$. We are looking for the triples $(k_1,k_2,k_3) \in \mathbb{Z}^3$ minimizing the quantity $\|(a_1+2k_1)\cdot\mathbf{b}_1 + (a_2+2k_2)\cdot\mathbf{b}_2 + (a_3+2k_3)\cdot\mathbf{b}_3\|$, where $[\mathbf{b}_1,\mathbf{b}_2,\mathbf{b}_3]_\leq$ are ε-greedy-reduced. In order to apply Lemma 9.2.4, from which the result can be deduced easily, it is sufficient to prove that the minimum over (k_1,k_2,k_3) can be taken over a finite domain. Notice that if (k_1^*,k_2^*,k_3^*) is optimal:

$$3 \geq \|a_1\cdot\mathbf{b}_1 + a_2\cdot\mathbf{b}_2 + a_3\cdot\mathbf{b}_3\| \geq \|(a_1+2k_1^*)\cdot\mathbf{b}_1 + (a_2+2k_2^*)\cdot\mathbf{b}_2 + (a_3+2k_3^*)\cdot\mathbf{b}_3\|.$$

Moreover, Lemma 9.2.2 gives that:

$$\|(a_1+2k_1^*)\cdot\mathbf{b}_1+(a_2+2k_2^*)\cdot\mathbf{b}_2+(a_3+2k_3^*)\cdot\mathbf{b}_3\| \geq |a_3+2k_3^*|\cdot\|\mathbf{b}_3^*\| \geq |a_3+2k_3^*|C,$$

for any sufficiently small $\varepsilon > 0$. This gives the result for k_3^*.

From the triangular inequality, Lemma 9.2.2, and the fact that $\|\mathbf{b}_2\| \geq \alpha$, we have:

$$3+|a_3+2k_3^*| \geq \|(a_1+2k_1^*)\cdot\mathbf{b}_1+(a_2+2k_2^*)\cdot\mathbf{b}_2\| \geq |a_2+2k_2^*|\cdot\|\mathbf{b}_2^*\| \geq |a_2+2k_2^*|C\alpha.$$

The fact that k_3^* is bounded ensures that k_2^* is bounded.

To obtain the result on k_1^*, it suffices to apply the triangular inequality once more:

$$3+|a_3+2k_3^*|+|a_2+2k_2^*| \geq \|(a_1+2k_1^*)\cdot\mathbf{b}_1\| \geq |a_1+2k_1^*|\alpha.$$

□

The following result generalizes Lemma 9.1.4 about the possible Voronoï coord $(1,1,2)$. As opposed to the two previous results, there is no need using the Topological Lemma in this case, because only a finite number of (x_1,x_2,x_3)'s is considered.

LEMMA 9.2.7. *There exists $c > 0$ such that for any sufficiently small $\varepsilon > 0$, if $[\mathbf{b}_1,\mathbf{b}_2,\mathbf{b}_3]_\leq$ are ε-greedy-reduced and $\|\mathbf{b}_3\| = 1$, then:*

(1) If $(s_1,s_2,2)$ is a Voronoï coord with $s_i = \pm 1$ for $i \in \{1,2\}$, then: $\|\mathbf{b}_1\| \geq 1-c\varepsilon$, $|\langle\mathbf{b}_1,\mathbf{b}_2\rangle| \leq c\varepsilon$ and $\left|\langle\mathbf{b}_i,\mathbf{b}_3\rangle + \frac{s_i}{2}\cdot\|\mathbf{b}_1\|^2\right| \leq c\varepsilon$ for $i \in \{1,2\}$.

(2) If $(s_1,2,s_3)$ is a Voronoï coord with $s_i = \pm 1$ for $i \in \{1,3\}$, then $(1-c\varepsilon)\cdot\|\mathbf{b}_2\| \leq \|\mathbf{b}_1\| \leq \|\mathbf{b}_2\|$. Moreover, if $\|\mathbf{b}_1\| \geq 1-\varepsilon$, then: $|\langle\mathbf{b}_1,\mathbf{b}_3\rangle| \leq c\varepsilon$ and $\left|\langle\mathbf{b}_i,\mathbf{b}_2\rangle + \frac{s_i}{2}\cdot\|\mathbf{b}_1\|^2\right| \leq c\varepsilon$ for $i \in \{1,3\}$.

(3) If $(2,s_2,s_3)$ is a Voronoï coord with $s_i = \pm 1$ for $i \in \{2,3\}$ and if $\|\mathbf{b}_1\| \geq 1-\varepsilon$, then: $|\langle\mathbf{b}_2,\mathbf{b}_3\rangle| \leq c\varepsilon$ and $\left|\langle\mathbf{b}_i,\mathbf{b}_1\rangle + \frac{s_i}{2}\cdot\|\mathbf{b}_1\|^2\right| \leq c\varepsilon$ for $i \in \{2,3\}$.

The proof is a straightforward modification of the proof of Lemma 9.1.4.

PROOF. Wlog we suppose that for any i, we have s_i=1. The proofs of the other cases are very similar. We only prove the statement in the case of the first situation.

We consider the inequality $\|\mathbf{b}_1+\mathbf{b}_2+2\cdot\mathbf{b}_3\|^2 \leq \|\mathbf{b}_1+\mathbf{b}_2\|^2$: it is equivalent to $\|\mathbf{b}_3\|^2+\langle\mathbf{b}_1,\mathbf{b}_3\rangle+\langle\mathbf{b}_2,\mathbf{b}_3\rangle \leq 0$. Since $[\mathbf{b}_1,\mathbf{b}_2,\mathbf{b}_3]_\leq$ are ε-greedy-reduced, by using Lemma 9.2.1 we obtain that we must have $\langle\mathbf{b}_1,\mathbf{b}_3\rangle \geq -\frac{1+\varepsilon}{2}\cdot\|\mathbf{b}_1\|^2$ and $\langle\mathbf{b}_2,\mathbf{b}_3\rangle \geq -\frac{1+\varepsilon}{2}\cdot\|\mathbf{b}_2\|^2$. Thus $2\cdot\|\mathbf{b}_3\|^2-(1+\varepsilon)\cdot\|\mathbf{b}_1\|^2-(1+\varepsilon)\cdot\|\mathbf{b}_2\|^2 \leq 0$. Consequently, the length "quasi-equality" holds, and the inequalities on the scalar products above are "quasi-equalities".

It remains to prove that $|\langle\mathbf{b}_1,\mathbf{b}_2\rangle|$ is very small. Expanding the relation $\|\mathbf{b}_1+\mathbf{b}_2+2\cdot\mathbf{b}_3\|^2 \leq \|\mathbf{b}_1-\mathbf{b}_2\|^2$ gives that $\langle\mathbf{b}_1,\mathbf{b}_2\rangle \leq c_1\varepsilon$ for some constant $c_1 > 0$. Similarly, expanding the relation $|\langle\mathbf{b}_3,\mathbf{b}_1+\mathbf{b}_2\rangle| \leq \frac{1+\varepsilon}{2}\cdot\|\mathbf{b}_1+\mathbf{b}_2\|^2$ (which comes from Lemma 9.2.1 gives $\langle\mathbf{b}_1,\mathbf{b}_2\rangle \geq -c_2\varepsilon$ for some constant $c_2 > 0$. □

9.3 The Gap Lemma

The goal of this subsection is to prove that even with relaxed bases, if one adds a lattice vector with not too small coordinates to a vector of the Voronoï cell, this

vector becomes significantly longer. This result was used the other way round: if the x_i's found at Step 5 of the recursive greedy algorithm are not too small, then the vector $\mathbf{b}_d$ is significantly shorter than the vector $\mathbf{a}_d$. We first generalize the compact sets K_2 and K_3. For any $\varepsilon \geq 0$ and any $\alpha \in [0,1]$, we define:

$$K_2'(\varepsilon,\alpha) = \{(\mathbf{b}_1,\mathbf{b}_2,\mathbf{u}), (\mathbf{b}_1,\mathbf{b}_2) \in K_2(\varepsilon,\alpha) \text{ and } \mathbf{u} \in \mathrm{Vor}(\mathbf{b}_1,\mathbf{b}_2)\}$$
$$K_3'(\varepsilon,\alpha) = \{(\mathbf{b}_1,\mathbf{b}_2,\mathbf{b}_3,\mathbf{u}), (\mathbf{b}_1,\mathbf{b}_2,\mathbf{b}_3) \in K_3(\varepsilon,\alpha) \text{ and } \mathbf{u} \in \mathrm{Vor}(\mathbf{b}_1,\mathbf{b}_2)\}.$$

LEMMA 9.3.1. *If $\varepsilon \geq 0$ and $\alpha \in [0,1]$, the sets $K_2'(\varepsilon,\alpha)$ and $K_3'(\varepsilon,\alpha)$ are compact.*

PROOF. Since the proofs in the two and three dimensional cases are the same, we only consider $K_2'(\varepsilon,\alpha)$. It is sufficient to show that $K_2'(\varepsilon,\alpha)$ is closed and bounded. The fact it is bounded is obvious since $\|\mathbf{b}_1\| \leq \|\mathbf{b}_2\| = 1$ and $\|\mathbf{u}\| \leq \|\mathbf{b}_1\| + \|\mathbf{b}_2\| \leq 2$. We suppose now that $K_2'(\varepsilon,\alpha)$ is not closed and we look for a contradiction. Let $\left(\mathbf{b}_1^{(n)}, \mathbf{b}_2^{(n)}, \mathbf{u}^{(n)}\right)$ be a sequence of elements of $K_2'(\varepsilon,\alpha)$ that converges to $(\mathbf{b}_1,\mathbf{b}_2,\mathbf{u}) \notin K_2'(\varepsilon,\alpha)$. By definition of $K_2'(\varepsilon,\alpha)$, there exists $(x_1,x_2) \neq (0,0)$ such that $\|x_1 \cdot \mathbf{b}_1 + x_2 \cdot \mathbf{b}_2 + \mathbf{u}\| > \|\mathbf{u}\|$. Thus there exists an integer $n \geq 0$ such that $\left\|x_1\mathbf{b}_1^{(n)} + x_2\mathbf{b}_2^{(n)} + \mathbf{u}^{(n)}\right\| > \left\|\mathbf{u}^{(n)}\right\|$. In that case, we have $\mathbf{u}^{(n)} \notin \mathrm{Vor}\left(\mathbf{b}_1^{(n)}, \mathbf{b}_2^{(n)}\right)$, which is impossible. □

The next result is the two-dimensional version of the Gap Lemma.

LEMMA 9.3.2. *There exist two constants $\varepsilon, C > 0$ such that for any ε-greedy-reduced vectors $[\mathbf{b}_1,\mathbf{b}_2]_\leq$ and any $\mathbf{u} \in \mathrm{Vor}(\mathbf{b}_1,\mathbf{b}_2)$, if at least one of the following conditions holds, then: $\|\mathbf{u} + x_1\mathbf{b}_1 + x_2\mathbf{b}_2\|^2 \geq \|\mathbf{u}\|^2 + C\|\mathbf{b}_2\|^2$.*

(1) $|x_2| \geq 2$,
(2) $|x_1| \geq 2$ *and* $\|\mathbf{b}_1\| \geq (1-\varepsilon) \cdot \|\mathbf{b}_2\|$.

PROOF. The proof involves three claims. The first one helps compactifying the set of the variables $[\mathbf{b}_1,\mathbf{b}_2]$. The second one shows that we can suppose that the vectors $\mathbf{b}_1$ and $\mathbf{b}_2$ have similar lengths, and the third one is the key step when showing that we can use Lemma 9.2.5 to end the proof.

Claim 1: Wlog we can suppose $\|\mathbf{b}_2\| = 1$.

Let $(*)$ be the following statement: "There exist two constants $\varepsilon, C > 0$ such that for any ε-greedy-reduced vectors $[\mathbf{b}_1,\mathbf{b}_2]_\leq$ with $\|\mathbf{b}_2\| = 1$, and any $\mathbf{u} \in \mathrm{Vor}(\mathbf{b}_1,\mathbf{b}_2)$, if one of the following conditions is not satisfied then $\|\mathbf{u} + x_1 \cdot \mathbf{b}_1 + x_2 \cdot \mathbf{b}_2\|^2 \geq \|\mathbf{u}\|^2 + C$.

—A- $|x_2| \geq 2$,
—B- $|x_1| \geq 2$ and $\|\mathbf{b}_1\| \geq 1 - \varepsilon$."

We keep the same constants $\varepsilon, C > 0$. Let $[\mathbf{b}_1,\mathbf{b}_2]_\leq$ be ε-greedy-reduced vectors. If $\|\mathbf{b}_2\| = 0$, the result is obvious. Otherwise, let $\mathbf{b}_i' = \frac{1}{\|\mathbf{b}_2\|} \cdot \mathbf{b}_i$ for $i \in \{1,2\}$. We apply $(*)$ to the ε-greedy-reduced vectors $[\mathbf{b}_1',\mathbf{b}_2']_\leq$. Let $\mathbf{u} \in \mathrm{Vor}(\mathbf{b}_1,\mathbf{b}_2)$ and $\mathbf{u}' = \frac{1}{\|\mathbf{b}_2\|} \cdot \mathbf{u}$. Then $\mathbf{u}' \in \mathrm{Vor}(\mathbf{b}_1',\mathbf{b}_2')$. If condition (1) or condition (2) is satisfied,

then $\|\mathbf{u}' + x_1 \cdot \mathbf{b}_1' + x_2 \cdot \mathbf{b}_2'\|^2 \geq \|\mathbf{u}'\|^2 + C$. Multiplying both sides by $\|\mathbf{b}_2\|^2$ gives the result. □

We now distinguish two cases: either the vector $\mathbf{b}_1$ has approximately the length of the vector $\mathbf{b}_2$, or it is far shorter (which cannot happen in situation (2)). The idea of the following claim is that when $\mathbf{b}_1$ converges to $\mathbf{0}$, $(\mathbf{b}_1, \mathbf{b}_2, \mathbf{u})$ converges to $(0, \mathbf{b}_2, \mathbf{u}')$ where $\mathbf{u}'$ is close to $\mathrm{Vor}(\mathbf{b}_2)$.

Claim 2: There exist $C, \alpha, \varepsilon > 0$ such that for any $(\mathbf{b}_1, \mathbf{b}_2, \mathbf{u}) \in K_2'(\varepsilon, 0)$ with $\|\mathbf{b}_1\| \leq \alpha$, as soon as $|x_2| \geq 2$:

$$\|\mathbf{u} + x_1 \cdot \mathbf{b}_1 + x_2 \cdot \mathbf{b}_2\|^2 - \|\mathbf{u}\|^2 \geq C.$$

Since $\mathbf{u} \in \mathrm{Vor}(\mathbf{b}_1, \mathbf{b}_2)$, we have $|\langle \mathbf{u}, \mathbf{b}_i \rangle| \leq \|\mathbf{b}_i\|^2/2$ for $i \in \{1, 2\}$. Therefore:

$$\begin{aligned}
\|\mathbf{u} + x_1 \cdot \mathbf{b}_1 + x_2 \cdot \mathbf{b}_2\|^2 \ - \ \|\mathbf{u}\|^2 &= \|x_1 \cdot \mathbf{b}_1 + x_2 \cdot \mathbf{b}_2\|^2 + 2\langle \mathbf{u}, x_1 \cdot \mathbf{b}_1 + x_2 \cdot \mathbf{b}_2 \rangle \\
&\geq \|x_1 \cdot \mathbf{b}_1 + x_2 \cdot \mathbf{b}_2\|^2 - |x_1| \cdot \|\mathbf{b}_1\|^2 - |x_2| \\
&\geq (x_1^2 - |x_1|) \cdot \|\mathbf{b}_1\|^2 + (x_2^2 - |x_2|) - 2|x_1 x_2| \cdot |\langle \mathbf{b}_1, \mathbf{b}_2 \rangle|.
\end{aligned}$$

Since $[\mathbf{b}_1, \mathbf{b}_2]_{\leq}$ are ε-greedy-reduced, by Lemma 9.2.1 we have $|\langle \mathbf{b}_1, \mathbf{b}_2 \rangle| \leq \frac{1+\varepsilon}{2} \cdot \|\mathbf{b}_1\|^2$, from which we get:

$$\|\mathbf{u} + x_1 \cdot \mathbf{b}_1 + x_2 \cdot \mathbf{b}_2\|^2 - \|\mathbf{u}\|^2 \geq |x_1|(|x_1| - |x_2|(1+\varepsilon) - 1) \cdot \|\mathbf{b}_1\|^2 + (x_2^2 - |x_2|).$$

We now minimize this last expression as regard to the variable $|x_1|$ (this is a degree-2 polynomial), and with the extremal choice "$|x_1| = \frac{(1+\varepsilon)|x_2|+1}{2}$" we obtain:

$$\begin{aligned}
\|\mathbf{u} + x_1 \cdot \mathbf{b}_1 + x_2 \cdot \mathbf{b}_2\|^2 \ - \ \|\mathbf{u}\|^2 & \\
&\geq -\frac{(|x_2|(1+\varepsilon) + 1^2}{4} \cdot \|\mathbf{b}_1\|^2 + (x_2^2 - |x_2|) \\
&\geq \left(1 - \frac{\alpha^2(1+\varepsilon)^2}{4}\right)|x_2|^2 - \left(1 + \frac{\alpha^2(1+\varepsilon)}{2}\right)|x_2| - \frac{\alpha^2}{4}
\end{aligned}$$

For a small enough α, the minimum of this degree-2 polynomial in $|x_2|$ is reached for "$|x_2| \leq 2$", and is increasing as regard to $|x_2| \geq 2$. By hypothesis $|x_2| \geq 2$, therefore we have:

$$\|\mathbf{u} + x_1 \cdot \mathbf{b}_1 + x_2 \cdot \mathbf{b}_2\|^2 - \|\mathbf{u}\|^2 \geq 2 - \alpha^2(9/4 + 3\varepsilon + \varepsilon^2),$$

which gives the result. □

The constant $\alpha > 0$ is fixed to satisfy the constraint of Claim 2, and we fix $\varepsilon > 0$ to satisfy the constraints of Claim 2 and Lemmata 9.2.2 and 9.2.5. We now consider a sequence $\left(\mathbf{b}_1^{(k)}, \mathbf{b}_2^{(k)}, \mathbf{u}^{(k)}, x_1^{(k)}, x_2^{(k)}\right)_k$ such that:

(1) $\left(\mathbf{b}_1^{(k)}, \mathbf{b}_2^{(k)}, \mathbf{u}^{(k)}\right) \in K_2'(\varepsilon, \alpha)$,

(2) $x_1^{(k)}, x_2^{(k)}$ are integers with $|x_2^{(k)}| \geq 2$ (respectively $|x_1^{(k)}| \geq 2$),

(3) $\left\|\mathbf{u}^{(k)} + x_1^{(k)} \cdot \mathbf{b}_1^{(k)} + x_2^{(k)} \cdot \mathbf{b}_2^{(k)}\right\|^2 - \left\|\mathbf{u}^{(k)}\right\|^2 \to 0$ when $k \to \infty$.

If no such sequence exists, then (1) (respectively (2)) is proved. To end the proof of Lemma 9.3.2, suppose to the contrary that such a sequence does exist: there will be a contradiction with Voronoï coords.

Claim 3: For any sufficiently small $\varepsilon > 0$ and for any $\alpha > 0$, the sequences $x_2^{(k)}$ and $x_1^{(k)}$ remain bounded.

Suppose that this is not the case. We show that this implies that the quantity $\left\|\mathbf{u}^{(k)} + x_1^{(k)} \cdot \mathbf{b}_1^{(k)} + x_2^{(k)} \cdot \mathbf{b}_2^{(k)}\right\|^2 - \left\|\mathbf{u}^{(k)}\right\|^2$ is not bounded, which is impossible. By the Cauchy-Schwarz inequality, we have:

$$\begin{aligned}\|\mathbf{u}^{(k)} \; + \; & x_1^{(k)} \cdot \mathbf{b}_1^{(k)} + x_2^{(k)} \cdot \mathbf{b}_2^{(k)}\|^2 - \left\|\mathbf{u}^{(k)}\right\|^2 \\ & \geq \left\|x_1^{(k)} \cdot \mathbf{b}_1^{(k)} + x_2^{(k)} \cdot \mathbf{b}_2^{(k)}\right\| \left(\left\|x_1^{(k)} \cdot \mathbf{b}_1^{(k)} + x_2^{(k)} \cdot \mathbf{b}_2^{(k)}\right\| - 2\left\|\mathbf{u}^{(k)}\right\|\right).\end{aligned}$$

Since $\left\|\mathbf{u}^{(k)}\right\|$ is bounded, it suffices to show that $\left\|x_1^{(k)} \cdot \mathbf{b}_1^{(k)} + x_2^{(k)} \cdot \mathbf{b}_2^{(k)}\right\|$ is not bounded. From Lemma 9.2.2, we have:

$$\left\|x_1^{(k)} \cdot \mathbf{b}_1^{(k)} + x_2^{(k)} \cdot \mathbf{b}_2^{(k)}\right\| \geq \left|x_2^{(k)}\right| \cdot \left\|\mathbf{b}_2^{(k)*}\right\| \geq C\left|x_2^{(k)}\right|.$$

Therefore, the sequence $x_2^{(k)}$ is bounded. The triangular inequality and the fact that $\left\|\mathbf{b}_1^{(k)}\right\| \geq \alpha$ ensure that the sequence $x_1^{(k)}$ remains bounded too. □

The previous claim and Lemma 9.3.1 imply that $\left(\mathbf{b}_1^{(k)}, \mathbf{b}_2^{(k)}, \mathbf{u}^{(k)}, x_1^{(k)}, x_2^{(k)}\right)$ remains in a compact subset of $\mathbb{R}^{3n} \times \mathbb{Z}^2$. Therefore we can extract a subsequence that converges to a limit $(\mathbf{b}_1, \mathbf{b}_2, \mathbf{u}, x_1, x_2)$ that lies in the same compact and satisfies: $\|\mathbf{u} + x_1 \cdot \mathbf{b}_1 + x_2 \cdot \mathbf{b}_2\| = \|\mathbf{u}\|$. This means that $x_1 \cdot \mathbf{b}_1 + x_2 \cdot \mathbf{b}_2$ is a Voronoï vector of the lattice spanned by $[\mathbf{b}_1, \mathbf{b}_2]_{\leq} \in K_2'(\varepsilon, \alpha)$, which contradicts Lemma 9.2.5. □

We now give the three-dimensional Gap Lemma, on which relies the analysis of the four-dimensional greedy algorithm.

LEMMA 9.3.3. *There exist two constants $\varepsilon, C > 0$ such that for any ε-greedy-reduced vectors $[\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3]_{\leq}$ and any $\mathbf{u} \in \mathrm{Vor}(\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3)$, if at least one of the following conditions holds, then:*

$$\|\mathbf{u} + x_1 \cdot \mathbf{b}_1 + x_2 \cdot \mathbf{b}_2 + x_3 \cdot \mathbf{b}_3\|^2 \geq \|\mathbf{u}\|^2 + C \cdot \|\mathbf{b}_3\|^2.$$

(1) $|x_3| \geq 3$, *or* $|x_3| = 2$ *with* $(|x_1|, |x_2|) \neq (1, 1)$.

(2) $\|\mathbf{b}_2\| \geq (1 - \varepsilon) \cdot \|\mathbf{b}_3\|$ *and:* $|x_2| \geq 3$, *or* $|x_2| = 2$ *with* $(|x_1|, |x_3|) \neq (1, 1)$.

(3) $\|\mathbf{b}_1\| \geq (1 - \varepsilon) \cdot \|\mathbf{b}_3\|$ *and:* $|x_1| \geq 3$, *or* $|x_1| = 2$ *with* $(|x_2|, |x_3|) \neq (1, 1)$.

PROOF. It is easy to see that similarly to Lemma 9.3.2 we can suppose that $\|\mathbf{b}_3\| = 1$. We consider three cases: both vectors $\mathbf{b}_1$ and $\mathbf{b}_2$ are significantly shorter than the vector $\mathbf{b}_3$, the vector $\mathbf{b}_1$ is very short but the vectors $\mathbf{b}_2$ and $\mathbf{b}_3$ have

similar lengths, and finally all the vectors have similar lengths.

Claim 1: There exist $C, \alpha, \varepsilon > 0$ such that for any $(\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \mathbf{u}) \in K_3'(\varepsilon, 0)$ with $\|\mathbf{b}_2\| \leq \alpha$, as soon as $|x_3| \geq 2$, we have $\|\mathbf{u}+x_1\cdot\mathbf{b}_1+x_2\cdot\mathbf{b}_2+x_3\cdot\mathbf{b}_3\|^2-\|\mathbf{u}\|^2 \geq C$.

Because the vector $\mathbf{u}$ lies in the Voronoï cell of the lattice spanned by the vectors $\mathbf{b}_1, \mathbf{b}_2$ and $\mathbf{b}_3$, and because of Lemma 9.2.1, we have the following inequalities:

$$\begin{aligned}\|\mathbf{u} + x_1 \cdot \mathbf{b}_1 \ &+\ x_2 \cdot \mathbf{b}_2 + x_3 \cdot \mathbf{b}_3\|^2 - \|\mathbf{u}\|^2 \\ &= \|x_1 \cdot \mathbf{b}_1 + x_2 \cdot \mathbf{b}_2 + x_3 \cdot \mathbf{b}_3\|^2 + 2\langle \mathbf{u}, x_1 \cdot \mathbf{b}_1 + x_2 \cdot \mathbf{b}_2 + x_3 \cdot \mathbf{b}_3\rangle \\ &\geq \left(x_1^2 - (1+\varepsilon)|x_1|(|x_2| + |x_3|) - |x_1|\right) \cdot \|\mathbf{b}_1\|^2 \\ &\quad + \left(x_2^2 - (1+\varepsilon)|x_2|\|x_3| - |x_2|\right) \cdot \|\mathbf{b}_2\|^2 + x_3^2 - |x_3|.\end{aligned}$$

We minimize this degree-2 polynomial of the variable $|x_1|$, and with the choice "$x_1 = \frac{(1+\varepsilon)(|x_2|+|x_3|)+1}{2}$", we obtain that $\|\mathbf{u} + x_1 \cdot \mathbf{b}_1 + x_2 \cdot \mathbf{b}_2 + x_3 \cdot \mathbf{b}_3\|^2 - \|\mathbf{u}\|^2$ is:

$$\begin{aligned}&\geq\ -\frac{((1+\varepsilon)(|x_2| + |x_3|) + 1)^2}{4} \cdot \|\mathbf{b}_1\|^2 + \left(x_2^2 - (1+\varepsilon)|x_2||x_3| - |x_2|\right) \cdot \|\mathbf{b}_2\|^2 \\ &\quad + x_3^2 - |x_3| \\ &\geq\ \left(\frac{3 - 2\varepsilon - \varepsilon^2}{4} x_2^2 - \left(\frac{3 + 4\varepsilon + \varepsilon^2}{2}|x_3| + \frac{3+\varepsilon}{2}\right)|x_2| - \frac{((1+\varepsilon)|x_3| + 1)^2}{4}\right) \|\mathbf{b}_2\|^2 \\ &\quad + x_3^2 - |x_3|,\end{aligned}$$

because $\|\mathbf{b}_1\| \leq \|\mathbf{b}_2\|$. The left-hand term is a degree-2 polynomial in $|x_2|$, whose first coefficient is positive (for a small enough $\varepsilon > 0$). It is lower-bounded by its minimum over $\mathbb{Z}$ and the minimum is reached for $|x_2| = |x_3| + 1$ when $\varepsilon = 0$. This gives:

$$\|\mathbf{u}+x_1\cdot\mathbf{b}_1+x_2\cdot\mathbf{b}_2+x_3\cdot\mathbf{b}_3\|^2-\|\mathbf{u}\|^2 \geq \left(a_2(\varepsilon)x_3^2 + a_1(\varepsilon)|x_3| + a_0(\varepsilon)\right)\cdot\|\mathbf{b}_2\|^2+x_3^2-|x_3|,$$

where $a_2(\varepsilon) \to -1, a_2(\varepsilon) \to -2$ and $a_0(\varepsilon) \to -1$ when $\varepsilon \to 0$. When $\varepsilon > 0$ is small enough, the factor in front of $\|\mathbf{b}_2\|^2$ is negative, and since $\|\mathbf{b}_2\| \leq \alpha$, we get:

$$\begin{aligned}\mathbf{u} + x_1 \cdot \mathbf{b}_1 + x_2 \cdot \mathbf{b}_2 \ &+\ x_3 \cdot \mathbf{b}_3\|^2 - \|\mathbf{u}\|^2 \\ &\geq \left(1 + \alpha^2 a_2(\varepsilon)\right) x_3^2 + \left(-1 + \alpha^2 a_1(\varepsilon)\right)|x_3| + \alpha^2 a_0(\varepsilon).\end{aligned}$$

For small enough constants $\alpha, \varepsilon > 0$, this degree-2 polynomial of the variable $|x_3|$ is strictly increasing over $[2, \infty)$ so that we can replace $|x_3|$ by 2 in the right hand side:

$$\|\mathbf{u}+x_1\cdot\mathbf{b}_1+x_2\cdot\mathbf{b}_2+x_3\cdot\mathbf{b}_3\|^2-\|\mathbf{u}\|^2 \geq 4\left(1 + \alpha^2 a_2(\varepsilon)\right) - 2\left(1 - \alpha^2 a_1(\varepsilon)\right) + \alpha^2 a_0(\varepsilon).$$

When $\alpha > 0$ is small enough, this quantity becomes larger than a constant $C > 0$.

Claim 2: There exist $C, c'', \varepsilon, \alpha > 0$ such that for any $(\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \mathbf{u}) \in K_3'(\varepsilon, 0)$ with $\|\mathbf{b}_1\| \leq \alpha$ and $\|\mathbf{b}_2\| \geq c''\alpha$, as soon as $|x_3| \geq 2$, $\|\mathbf{u} + x_1 \cdot \mathbf{b}_1 + x_2 \cdot \mathbf{b}_2 + x_3 \cdot \mathbf{b}_3\|^2 - \|\mathbf{u}\|^2 \geq C$.

The proof looks like the one of Claim 2 of Lemma 9.3.2, but is slightly more

technical. We have the following inequalities:

$$\begin{aligned}
&\|\mathbf{u}+x_1\cdot\mathbf{b}_1+x_2\cdot\mathbf{b}_2+x_3\cdot\mathbf{b}_3\|^2-\|\mathbf{u}\|^2\\
=\;&\|x_1\cdot\mathbf{b}_1+x_2\cdot\mathbf{b}_2+x_3\cdot\mathbf{b}_3\|^2+2\langle\mathbf{u},x_1\cdot\mathbf{b}_1+x_2\cdot\mathbf{b}_2+x_3\cdot\mathbf{b}_3\rangle\\
\geq\;&\left(x_1^2-(1+\varepsilon)|x_1|(|x_2|+|x_3|)-|x_1|\right)\cdot\|\mathbf{b}_1\|^2\\
&+\|x_2\cdot\mathbf{b}_2+x_3\cdot\mathbf{b}_3\|^2+2\langle\mathbf{u},x_2\cdot\mathbf{b}_2+x_3\cdot\mathbf{b}_3\rangle\\
\geq\;&-\frac{\alpha^2}{4}\left((1+\varepsilon)(|x_2|+|x_3|)+1\right)^2+\|x_2\cdot\mathbf{b}_2+x_3\cdot\mathbf{b}_3\|^2+2\langle\mathbf{u},x_2\cdot\mathbf{b}_2+x_3\cdot\mathbf{b}_3\rangle.
\end{aligned}$$

We write $\mathbf{u}=\mathbf{u}'+\mathbf{u}''$, where $\mathbf{u}'$ is in the span of $[\mathbf{b}_2,\mathbf{b}_3]$, and $\mathbf{u}''$ is orthogonal to it. It is clear that the vector $\mathbf{u}'$ is in the Voronoï cell of $L[\mathbf{b}_2,\mathbf{b}_3]$. By Lemma 9.1.1, we know that $\|\mathbf{u}'\|\leq 1/\sqrt{2}$. Besides, as soon as $|x_3|\geq 2$:

$$\begin{aligned}
\|x_2\cdot\mathbf{b}_2+x_3\cdot\mathbf{b}_3\|^2&\geq\left(x_2^2-(1+\varepsilon)|x_2x_3|\right)\cdot\|\mathbf{b}_2\|^2+x_3^2\\
&\geq-\frac{((1+\varepsilon)|x_3|)^2}{4}\cdot\|\mathbf{b}_2\|^2+x_3^2\\
&\geq x_3^2\left(1-\frac{(1+\varepsilon)^2}{4}\right)\\
&\geq 3-2\varepsilon-\varepsilon^2.
\end{aligned}$$

Consequently $\sqrt{2}\leq\sqrt{\frac{2}{3-2c\varepsilon-c^2\varepsilon^2}}\cdot\|x_2\cdot\mathbf{b}_2+x_3\cdot\mathbf{b}_3\|$, which gives, by using the Cauchy-Schwarz inequality:

$$\langle\mathbf{u},x_2\cdot\mathbf{b}_2+x_3\cdot\mathbf{b}_3\rangle\geq-\frac{\sqrt{2}}{2}\cdot\|x_2\cdot\mathbf{b}_2+x_3\cdot\mathbf{b}_3\|\geq-\frac{1}{2}\sqrt{\frac{2}{3-2\varepsilon-\varepsilon^2}}\|x_2\cdot\mathbf{b}_2+x_3\cdot\mathbf{b}_3\|^2.$$

From this, we get:

$$\begin{aligned}
&\|\mathbf{u}\;+\;x_1\cdot\mathbf{b}_1+x_2\cdot\mathbf{b}_2+x_3\cdot\mathbf{b}_3\|^2-\|\mathbf{u}\|^2\\
&\quad\geq-\frac{\alpha^2}{4}((1+\varepsilon)(|x_2|+|x_3|)+1)^2+\left(1-\sqrt{\frac{2}{3-2\varepsilon-\varepsilon^2}}\right)\cdot\|x_2\cdot\mathbf{b}_2+x_3\cdot\mathbf{b}_3\|^2\\
&\quad\geq-\frac{\alpha^2}{4}((1+\varepsilon)(|x_2|+|x_3|)+1)^2\\
&\qquad+\left(1-\sqrt{\frac{2}{3-2\varepsilon-\varepsilon^2}}\right)\left((x_2^2-(1+2\varepsilon)|x_2\|x_3|)\cdot\|\mathbf{b}_2\|^2+x_3^2\right).
\end{aligned}$$

Because $|x_2x_3|\leq(x_2^2+x_3^2)/2$, we obtain, for any sufficiently small $\varepsilon>0$, a lower bound of the form:

$$\begin{aligned}
&\|\mathbf{u}+x_1\cdot\mathbf{b}_1+x_2\cdot\mathbf{b}_2+x_3\cdot\mathbf{b}_3\|^2-\|\mathbf{u}\|^2\\
\geq\;&\left(\alpha^2f_1(\varepsilon)+g_1(\varepsilon)\cdot\|\mathbf{b}_2\|^2\right)x_2^2+\left(\alpha^2f_2(\varepsilon)+g_2(\varepsilon)\cdot\|\mathbf{b}_2\|^2+g_3(\varepsilon)\right)x_3^2+\alpha^2f_3(\varepsilon),
\end{aligned}$$

where, when ε converges to zero: $f_i(\varepsilon)=O(1)$, $\lim_\varepsilon g_1(\varepsilon)>0$, $0\leq|\lim_\varepsilon g_2(\varepsilon)|<\lim_\varepsilon g_3(\varepsilon)$. It follows that for a suitable $c''>0$, there exists $C'>0$ such that for any sufficiently small $\alpha>0$ and any sufficiently small $\varepsilon>0$, and any $(\mathbf{b}_1,\mathbf{b}_2,\mathbf{b}_3,\mathbf{u})\in K_3'(\varepsilon,0)$ with $\|\mathbf{b}_1\|\leq\alpha$ and $\|\mathbf{b}_2\|\geq c''\alpha$, in the lower bound above, the coefficient

of x_2^2 is non-negative and the coefficient of x_3^2 is greater than C'. This completes the proof of Claim 2. □

The rest of the proof is identical to the end of the proof of Lemma 9.3.2: we choose an $\alpha > 0$ satisfying the conditions of the two previous claims and we consider a sequence $\left(\mathbf{b}_1^{(k)}, \mathbf{b}_2^{(k)}, \mathbf{b}_3^{(k)}, \mathbf{u}^{(k)}, x_1^{(k)}, x_2^{(k)}, x_3^{(k)}\right)_k$ such that:

(1) $\left(\mathbf{b}_1^{(k)}, \mathbf{b}_2^{(k)}, \mathbf{b}_3^{(k)}, \mathbf{u}^{(k)}\right) \in K_3'(\varepsilon, \alpha)$,

(2) $x_1^{(k)}, x_2^{(k)}, x_3^{(k)}$ are integers with $\left|x_3^{(k)}\right| \geq 3$ or $\left|x_3^{(k)}\right| = 2$ and $\left(|x_1^{(k)}|, |x_2^{(k)}|\right) \neq (1,1)$ (respectively $\left|x_i^{(k)}\right| \geq 3$ or etc. for $i \in \{1,2\}$),

(3) $\left\|\mathbf{u}^{(k)} + x_1^{(k)} \cdot \mathbf{b}_1^{(k)} + x_2^{(k)} \cdot \mathbf{b}_2^{(k)} + x_3^{(k)} \cdot \mathbf{b}_3^{(k)}\right\|^2 - \left\|\mathbf{u}^{(k)}\right\|^2 \to 0$ when $k \to \infty$.

If no such sequence exists, then the lemma is proved. We assume that there is one and we look for a contradiction with Voronoï coords.

Claim 3: For any sufficiently small $\varepsilon, \alpha > 0$, the sequences $x_3^{(k)}, x_2^{(k)}$ and $x_1^{(k)}$ are bounded.

Suppose this is not the case. We show that this implies that the quantity $\left\|\mathbf{u}^{(k)} + x_1^{(k)} \cdot \mathbf{b}_1^{(k)} + x_2^{(k)} \cdot \mathbf{b}_2^{(k)} + x_3^{(k)} \cdot \mathbf{b}_3^{(k)}\right\|^2 - \left\|\mathbf{u}^{(k)}\right\|^2$ is not bounded, which is impossible. By the Cauchy-Schwarz inequality, we have:

$$\begin{aligned}\left\|\mathbf{u}^{(k)} + x_1^{(k)} \cdot \mathbf{b}_1^{(k)} \right. &+ \left. x_2^{(k)} \cdot \mathbf{b}_2^{(k)} + x_3^{(k)} \cdot \mathbf{b}_3^{(k)}\right\|^2 - \left\|\mathbf{u}^{(k)}\right\|^2 \\ &\geq \left\|x_1^{(k)} \cdot \mathbf{b}_1^{(k)} + x_2^{(k)} \cdot \mathbf{b}_2^{(k)} + x_3^{(k)} \cdot \mathbf{b}_3^{(k)}\right\| \\ &\quad \cdot \left(\left\|x_1^{(k)} \cdot \mathbf{b}_1^{(k)} + x_2^{(k)} \cdot \mathbf{b}_2^{(k)} + x_3^{(k)} \cdot \mathbf{b}_3^{(k)}\right\| - 2\left\|\mathbf{u}^{(k)}\right\|\right).\end{aligned}$$

Since the sequence $\left\|\mathbf{u}^{(k)}\right\|$ is bounded, it suffices to show that the quantity $\left\|x_1^{(k)} \cdot \mathbf{b}_1^{(k)} + x_2^{(k)} \cdot \mathbf{b}_2^{(k)} + x_3^{(k)} \cdot \mathbf{b}_3^{(k)}\right\|$ is not bounded. We take a small enough $\varepsilon > 0$ to apply Lemma 9.2.2. Let $C > 0$ denote the corresponding constant. We have:

$$\left\|x_1^{(k)} \cdot \mathbf{b}_1^{(k)} + x_2^{(k)} \cdot \mathbf{b}_2^{(k)} + x_3^{(k)} \cdot \mathbf{b}_3^{(k)}\right\| \geq \left|x_3^{(k)}\right| \cdot \left\|\mathbf{b}_3^{(k)*}\right\| \geq C \cdot \left|x_3^{(k)}\right|.$$

Therefore, the sequence $x_3^{(k)}$ is bounded. If the sequence $x_2^{(k)}$ is bounded, by the triangular inequality, so is the sequence $x_1^{(k)}$. Now we show that the sequence $x_2^{(k)}$ remains bounded. We have the following inequality:

$$\left\|x_1^{(k)} \cdot \mathbf{b}_1^{(k)} + x_2^{(k)} \cdot \mathbf{b}_2^{(k)} + x_3^{(k)} \cdot \mathbf{b}_3^{(k)}\right\| \geq \left|x_2^{(k)}\right| \cdot \left\|\mathbf{b}_2^{(k)*}\right\| - \left|x_3^{(k)}\right| \cdot \left\|\mathbf{b}_3^{(k)}\right\|.$$

Since $\left[\mathbf{b}_1^{(k)}, \mathbf{b}_2^{(k)}\right]_{\leq}$ are ε-greedy-reduced and $1 \geq \left\|\mathbf{b}_2^{(k)}\right\| \geq \left\|\mathbf{b}_1^{(k)}\right\| \geq \alpha$, we have a situation similar to the third claim of Lemma 9.3.2 and this gives us a strictly

positive lower bound on $\|\mathbf{b}_2^{(k)*}\|$ that depends on ε and α. This completes the proof of the claim. □

This claim and Lemma 9.3.1 imply that $\left(\mathbf{b}_1^{(k)}, \mathbf{b}_2^{(k)}, \mathbf{b}_3^{(k)}, \mathbf{u}^{(k)}, x_1^{(k)}, x_2^{(k)}, x_3^{(k)}\right)$ remains in a compact subset of $\mathbb{R}^{4n+3}$. Therefore we can extract a subsequence that converges to a limit $(\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \mathbf{u}, x_1, x_2, x_3)$ that is in the same compact and satisfies: $\|\mathbf{u} + x_1 \cdot \mathbf{b}_1 + x_2 \cdot \mathbf{b}_2 + x_3 \cdot \mathbf{b}_3\| = \|\mathbf{u}\|$. This means that $x_1 \cdot \mathbf{b}_1 + x_2 \cdot \mathbf{b}_2 + x_3 \cdot \mathbf{b}_3$ is a Voronoï vector of the lattice spanned by $[\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3]_{\leq} \in K_3'(\varepsilon, \alpha)$. From Lemma 9.2.6, this is impossible. □

Like in the previous subsections, we now consider the case of the possible Voronoï coords $(\pm 1, \pm 1, \pm 2)$ modulo any permutation of coordinates.

LEMMA 9.3.4. *There exist two constants $\varepsilon, C > 0$ such that for any ε-greedy-reduced vectors $[\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3]_{\leq}$ and any vector $\mathbf{u} \in \mathrm{Vor}(\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3)$, if at least one of the following conditions holds, then:*

$$\|\mathbf{u} + x_1 \cdot \mathbf{b}_1 + x_2 \cdot \mathbf{b}_2 + x_3 \cdot \mathbf{b}_3\|^2 \geq \|\mathbf{u}\|^2 + C \cdot \|\mathbf{b}_3\|^2.$$

(1) $(x_1, x_2, x_3) = (s_1, s_2, 2)$, $|s_i| = 1$ *for* $i \in \{1, 2\}$ *and at least one of the following conditions holds:*
$\|\mathbf{b}_1\| \leq (1-\varepsilon)\|\mathbf{b}_3\|$, *or* $\|\mathbf{b}_2\| \leq (1-\varepsilon)\|\mathbf{b}_3\|$, *or* $|\langle \mathbf{b}_1, \mathbf{b}_2 \rangle| \geq \varepsilon \|\mathbf{b}_3\|^2$, *or* $\left|\langle \mathbf{b}_1, \mathbf{b}_3 \rangle + \frac{s_1}{2}\|\mathbf{b}_1\|^2\right| \geq \varepsilon \|\mathbf{b}_3\|^2$, *or* $\left|\langle \mathbf{b}_2, \mathbf{b}_3 \rangle + \frac{s_2}{2}\|\mathbf{b}_1\|^2\right| \geq \varepsilon \|\mathbf{b}_3\|^2$.

(2) $(x_1, x_2, x_3) = (s_1, 2, s_3)$, $|s_i| = 1$ *for* $i \in \{1, 3\}$ *and* $\|\mathbf{b}_1\| \leq (1-\varepsilon)\|\mathbf{b}_2\|$.

(3) $(x_1, x_2, x_3) = (s_1, 2, s_3)$, $|s_i| = 1$ *for* $i \in \{1, 3\}$, $\|\mathbf{b}_1\| \geq (1-\varepsilon)\|\mathbf{b}_3\|$ *and at least one of the following conditions holds:* $|\langle \mathbf{b}_1, \mathbf{b}_3 \rangle| \geq \varepsilon \|\mathbf{b}_3\|^2$, *or* $|\langle \mathbf{b}_1, \mathbf{b}_2 \rangle + \frac{s_1}{2}\|\mathbf{b}_1\|^2| \geq \varepsilon \|\mathbf{b}_3\|^2$, *or* $|\langle \mathbf{b}_3, \mathbf{b}_2 \rangle + \frac{s_3}{2}\|\mathbf{b}_1\|^2| \geq \varepsilon \|\mathbf{b}_3\|^2$.

(4) $(x_1, x_2, x_3) = (2, s_2, s_3)$, $|s_i| = 1$ *for* $i \in \{2, 3\}$, $\|\mathbf{b}_1\| \geq (1-\varepsilon)\|\mathbf{b}_3\|$ *and at least one of the following conditions holds:* $|\langle \mathbf{b}_2, \mathbf{b}_3 \rangle| \geq \varepsilon \|\mathbf{b}_3\|^2$, *or* $|\langle \mathbf{b}_2, \mathbf{b}_1 \rangle + \frac{s_2}{2}\|\mathbf{b}_1\|^2| \geq \varepsilon \|\mathbf{b}_3\|^2$, *or* $|\langle \mathbf{b}_3, \mathbf{b}_1 \rangle + \frac{s_3}{2}\|\mathbf{b}_1\|^2| \geq \varepsilon \|\mathbf{b}_3\|^2$.

PROOF. Wlog we suppose that $\|\mathbf{b}_3\| = 1$. We consider each subcase and each triple (x_1, x_2, x_3) separately (there is a finite number of subcases and of triples to consider). The constant $\varepsilon > 0$ is fixed such that if any of the conditions of the considered subcase is not fulfilled, then the result of Lemma 9.2.7 is wrong. In that case, the triple (x_1, x_2, x_3) cannot be a Voronoï coord for the ε-greedy-reduced vectors $[\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3]_{\leq}$. This implies that $\mathrm{dist}(V + x_1 \cdot \mathbf{b}_1 + x_2 \cdot \mathbf{b}_2 + x_3 \cdot \mathbf{b}_3, V) > 0$, where $V = \mathrm{Vor}(\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3)$. The facts that the function $\mathrm{dist}(V + x_1 \cdot \mathbf{b}_1 + x_2 \cdot \mathbf{b}_2 + x_3 \cdot \mathbf{b}_3, V)$ is continuous as regard to the variables $(\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3)$ and that the variables $(\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3)$ belong to a compact set provide the expected result. □

10. DIFFICULTIES ARISING IN DIMENSION 5

We have seen that the greedy algorithm can output arbitrarily bad bases in dimension 5. By using Minkowski's conditions, it is easy to see that the following generalization of the greedy algorithm computes a Minkowski-reduced basis in dimensions five and six: at Steps 2 and 3 of the iterative version of the greedy algorithm, instead of shortening the vector $\mathbf{b}_k$ by using an integer linear combination of $\mathbf{b}_1, \ldots, \mathbf{b}_{k-1}$, the algorithm may also use $\mathbf{b}_{k+1}, \ldots, \mathbf{b}_d$, see Figure 8. We

Input: An basis $[\mathbf{b}_1, \ldots, \mathbf{b}_d]_{\leq}$ with its Gram matrix.
Output: An ordered basis of $L[\mathbf{b}_1, \ldots, \mathbf{b}_d]$ with its Gram matrix.

1. $k := 2$. While $k \leq d$, do:
2. Compute a vector $\mathbf{c}$ closest to $\mathbf{b}_k$, in $L[\mathbf{b}_1, \ldots, \mathbf{b}_{k-1}, \mathbf{b}_{k+1}, \ldots, \mathbf{b}_d]$,
3. $\mathbf{b}_k := \mathbf{b}_k - \mathbf{c}$ and update the Gram matrix,
4. If $\|\mathbf{b}_k\| \geq \|\mathbf{b}_{k-1}\|$, $k := k + 1$
5. Else insert $\mathbf{b}_k$ at his length rank k', update the Gram matrix, $k := k' + 1$.

Fig. 8. A generalization of the greedy algorithm.

know very little about this algorithm when the dimension is higher than six: does it compute a Minkowski-reduced basis? is there a good bound on the number of loop iterations? does this algorithm admit a polynomial-time complexity bound?

Despite the fact that the greedy algorithm does not return a Minkowski-reduced basis, one may wonder if the quadratic complexity bound remains valid. To make the technique developed in Section 7 ready for use, it suffices to show that the iterative greedy algorithm in dimension 5 admits a linear bound (as regard to the input size) on its number of loop iterations. In dimensions below four, it was possible to use both local and global approaches.

With the global approach, it seems possible to show that the number of loop iterations of the recursive version of the greedy algorithm in dimension five is linear, which does not suffice. Besides, the result seems hard to get: Lemma 6.1.1 is not valid anymore. Nevertheless, it seems possible to determine precisely the bad cases: roughly speaking, these are the bases that resemble the one given in Lemma 4.3.3. It could then be shown that if we are not in this situation then Lemma 6.1.1 is correct, and that we can use Lemma 6.2.1 (it remains valid in dimension five). If we are in the bad situation, the geometry of the current basis could be made precise, and it should be possible to show that two loop iterations after the end of the η-phase, there is some significant length decrease.

The local analysis in dimensions two, three and four essentially relies on the fact that if one of the x_j's found at Step 5, of the recursive version of the greedy algorithm, has absolute value higher than 2, then $\left\|\mathbf{b}_d^{(i)}\right\|$ is significantly shorter than $\left\|\mathbf{a}_d^{(i)}\right\|$. This fact is derived from the so-called Gap Lemma. In dimension four, this was only partly true, but the exception (the 211-case) occurred in very few cases and could be dealt with by considering the very specific shape of the lattices for which it could go wrong. Things worsen in dimension five. Indeed, for Minkowski-reduced bases, $(1, 1, 1, 2)$ and $(1, 1, 2, 2)$ — modulo any change of sign and permutation of coordinates — are possible Voronoï coords. Here is an example

of a lattice for which $(1,1,2,2)$ is a Voronoï coord:

$$\begin{bmatrix} 1 & -1 & 0 & 0 \\ 1 & 1 & -1 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

The lattice basis given by the columns is Minkowski-reduced (since it is greedy-reduced), but:

$$\begin{aligned} \|\mathbf{b}_1 + \mathbf{b}_2 + 2\cdot\mathbf{b}_3 \ + \ 2\cdot\mathbf{b}_4\| &= 2 = \|\mathbf{b}_1 + \mathbf{b}_2\| \\ &\leq \|(2k_1+1)\cdot\mathbf{b}_1 + (2k_2+1)\cdot\mathbf{b}_2 + 2k_3\cdot\mathbf{b}_3 + 2k_4\cdot\mathbf{b}_4\|, \end{aligned}$$

for any $k_1, k_2, k_3, k_4 \in \mathbb{Z}$. Notice that $(1,1,2,2)$ cannot be a strict Voronoï coord: if $\mathbf{b}_1 + \mathbf{b}_2 + 2\cdot\mathbf{b}_3 + 2\cdot\mathbf{b}_4$ reaches the length minimum of its coset of $L/2L$, then so does $\mathbf{b}_1 + \mathbf{b}_2$. Thus it might be possible to work around the difficulty coming from $(1,1,2,2)$ like in the 211-case. However, the case $(1,1,1,2)$ would still remain, and this possible Voronoï coordinate can be strict.

ACKNOWLEDGMENTS

We thank Ali Akhavi, Florian Hess, Igor Semaev, Markus Rückert, Jacques Stern and Gilles Villard for helpful discussions and comments. We also thank the referees for their remarks. Significant parts of the writing of the present paper was performed while the second author was visiting the Universities of Bristol, whose hospitality is gratefully acknowledged, and while he was completing his PhD thesis at the University of Nancy 1.

REFERENCES

Ajtai, M. 1996. Generating hard instances of lattice problems (extended abstract). In *Proceedings of the 28th Symposium on the Theory of Computing (STOC 1996)*. ACM Press, 99–108.

Ajtai, M. 1998. The shortest vector problem in l_2 is NP-hard for randomized reductions (extended abstract). In *Proceedings of the 30th Symposium on the Theory of Computing (STOC 1998)*. ACM Press, 284–293.

Akhavi, A. 2000. Worst-case complexity of the optimal LLL algorithm. In *Proceedings of the 2000 Latin American Theoretical Informatics (LATIN 2000)*. Lecture Notes in Computer Science, vol. 1776. Springer-Verlag, 355–366.

Akhavi, A. and Moreira dos Santos, C. 2004. Another view of the Gaussian algorithm. In *Proceedings of the 2004 Latin American Theoretical Informatics (LATIN 2004)*. Lecture Notes in Computer Science, vol. 2976. Springer-Verlag, 474–487.

Babai, L. 1986. On Lovász lattice reduction and the nearest lattice point problem. *Combinatorica 6*, 1–13.

Cassels, J. W. S. 1971. *An Introduction to the Geometry of Numbers, 2nd edition*. Springer-Verlag.

Conway, J. H. and Sloane, N. J. A. 1988. *Sphere Packings, Lattices and Groups*. Springer-Verlag.

Delone, B. N. and Sandakova, N. N. 1961. Theory of stereohedra. *Trudy Mathematics Institute Steklov 64*, 28–51.

Eisenbrand, F. and Rote, G. 2001. Fast reduction of ternary quadratic forms. In *Proceedings of the 2001 Cryptography and Lattices Conference (CALC'01)*. Lecture Notes in Computer Science, vol. 2146. Springer-Verlag, 32–44.

Gama, N. and Nguyen, P. Q. 2008. Finding short lattice vectors within Mordell's inequality. In *STOC '08 – Proc. 40th ACM Symposium on the Theory of Computing*. ACM.

Gauss, C. F. 1801. *Disquisitiones Arithmeticæ*. Springer-Verlag.

Helfrich, B. 1985. Algorithms to construct Minkowski reduced and Hermite reduced lattice bases. *Theoretical Computer Science 41*, 125–139.

Hermite, C. 1850. Extraits de lettres de M. Hermite à M. Jacobi sur différents objets de la théorie des nombres, deuxième lettre. *Journal für die reine und angewandte Mathematik 40*, 279–290.

Hermite, C. 1905. *Œuvres*. Gauthiers-Villars.

Kaib, M. and Schnorr, C. P. 1996. The generalized Gauss reduction algorithm. *Journal of Algorithms 21,* 3, 565–578.

Kannan, R. 1983. Improved algorithms for integer programming and related lattice problems. In *Proceedings of the 15th Symposium on the Theory of Computing (STOC 1983)*. ACM Press, 99–108.

Korkine, A. and Zolotarev, G. 1873. Sur les formes quadratiques. *Mathematische Annalen 6*, 336–389.

Lagarias, J. C. 1980. Worst-case complexity bounds for algorithms in the theory of integral quadratic forms. *Journal of Algorithms 1*, 142–186.

Lagarias, J. C., Lenstra, W. H., and Schnorr, C. P. 1990. Korkine-Zolotarev bases and successive minimal of a lattice and its reciprocal lattice. *Combinatorica 10*, 333–348.

Lagrange, J. L. 1773. Recherches d'arithmétique. *Nouveaux Mémoires de l'Académie de Berlin*.

Lenstra, A. K., Lenstra, Jr., H. W., and Lovász, L. 1982. Factoring polynomials with rational coefficients. *Mathematische Annalen 261*, 513–534.

Martinet, J. 2002. *Perfect Lattices in Euclidean Spaces*. Springer-Verlag.

Micciancio, D. and Goldwasser, S. 2002. *Complexity of lattice problems: a cryptographic perspective*. Kluwer Academic Press.

Minkowski, H. 1896. *Geometrie der Zahlen*. Teubner-Verlag.

Nguyen, P. Q. and Stehlé, D. 2004. Low-dimensional lattice basis reduction revisited (extended abstract). In *Proceedings of the 6th Algorithmic Number Theory Symposium (ANTS VI)*. Lecture Notes in Computer Science, vol. 3076. Springer-Verlag, 338–357.

Nguyen, P. Q. and Stehlé, D. 2005. Floating-point LLL revisited. In *Proceedings of Eurocrypt 2005*. Lecture Notes in Computer Science, vol. 3494. Springer-Verlag, 215–233.

Nguyen, P. Q. and Stern, J. 2001. The two faces of lattices in cryptology. In *Proceedings of the 2001 Cryptography and Lattices Conference (CALC'01)*. Lecture Notes in Computer Science, vol. 2146. Springer-Verlag, 146–180.

Ryskov, S. S. 1972. On Hermite, Minkowski and Venkov reduction of positive quadratic forms in n variables. *Soviet Mathematics Doklady 13*, 1676–1679.

Schnorr, C. P. 1987. A hierarchy of polynomial lattice basis reduction algorithms. *Theoretical Computer Science 53*, 201–224.

Schnorr, C. P. and Euchner, M. 1994. Lattice basis reduction: improved practical algorithms and solving subset sum problems. *Mathematics of Programming 66*, 181–199.

Schnorr, C. P. and Hörner, H. H. 1995. Attacking the Chor-Rivest cryptosystem by improved lattice reduction. In *Proceedings of Eurocrypt 1995*. Lecture Notes in Computer Science, vol. 921. Springer-Verlag, 1–12.

Schönhage, A. and Strassen, V. 1971. Schnelle Multiplikation grosser Zahlen. *Computing 7*, 281–292.

Semaev, I. 2001. A 3-dimensional lattice reduction algorithm. In *Proceedings of the 2001 Cryptography and Lattices Conference (CALC'01)*. Lecture Notes in Computer Science, vol. 2146. Springer-Verlag, 181–193.

Siegel, C. L. 1989. *Lectures on the Geometry of Numbers*. Springer-Verlag.

Stogrin, M. I. 1977. Regular Dirichlet-Voronoï partitions for the second triclinic group. *American Mathematical Society*. English translation of the proceedings of the Steklov Institute of Mathematics, Number 123 (1973).

Tammela, P. P. 1973. On the reduction theory of positive quadratic forms. *Soviet Mathematics Doklady 14*, 651–655.

Vallée, B. 1986. Une approche géométrique de la réduction des réseaux en petite dimension. Ph.D. thesis, Université de Caen.

Vallée, B. 1991. Gauss' algorithm revisited. *Journal of Algorithms 12*, 556–572.

Voronoï, G. 1908. Nouvelles applications des paramètres continus à la théorie des formes quadratiques. *Journal für die reine und angewandte Mathematik 134*, 198–287.

van der Waerden, B. L. 1956. Die Reduktionstheorie der positiven quadratischen Formen. *Acta Mathematica 96*, 265–309.

Received May 2006; revised October 2008; accepted xxxx