On sublattice determinants in reduced bases

Gábor Pataki and Mustafa Tural *
Technical Report 2008-02
Department of Statistics and Operations Research, UNC Chapel Hill

Abstract

Lenstra, Lenstra, and Lovász in [7] proved several inequalities showing that the vectors in an LLL-reduced basis are short, and near orthogonal. Here we present generalizations, from which with $k = 1$, and $k = n$ we can recover their inequalities:

Theorem 1. *Let $b_1, \ldots, b_n \in \mathbb{R}^m$ be an LLL-reduced basis of the lattice L, and $d_1, \ldots, d_k$ arbitrary linearly independent vectors in L. Then*

$$\begin{aligned} \| b_1 \| &\leq 2^{(n-k)/2+(k-1)/4}(\det L(d_1, \ldots, d_k))^{1/k}, & (1)\\ \det L(b_1, \ldots, b_k) &\leq 2^{k(n-k)/2} \det L(d_1, \ldots, d_k), & (2)\\ \det L(b_1, \ldots, b_k) &\leq 2^{k(n-k)/4}(\det L)^{k/n}, & (3)\\ \| b_1 \| \cdots \| b_k \| &\leq 2^{k(n-k)/2+k(k-1)/4} \det L(d_1, \ldots, d_k), & (4)\\ \| b_1 \| \cdots \| b_k \| &\leq 2^{k(n-1)/4}(\det L)^{k/n}. & (5) \end{aligned}$$

□

In the most general setting, we prove:

Theorem 2. *Let $b_1, \ldots, b_n \in \mathbb{R}^m$ be an LLL-reduced basis of the lattice L, $1 \leq k \leq j \leq n$, and $d_1, \ldots, d_j$ arbitrary linearly independent vectors in L. Then*

$$\begin{aligned} \det L(b_1, \ldots, b_k) &\leq 2^{k(n-j)/2+k(j-k)/4}(\det L(d_1, \ldots, d_j))^{k/j}, & (6)\\ \| b_1 \| \cdots \| b_k \| &\leq 2^{k(n-j)/2+k(j-1)/4}(\det L(d_1, \ldots, d_j))^{k/j}. & (7) \end{aligned}$$

□

Mathematics subject classification codes: 11H06, 52C07

*Department of Statistics and Operations Research, UNC Chapel Hill, **gabor@unc.edu, tural@email.unc.edu**

1 Lattices and Basis Reduction

A lattice in $\mathbb{R}^m$ is a set of the form

$$L \;=\; L(b_1, \ldots, b_n) \;=\; \left\{ \sum_{i=1}^{n} \lambda_i b_i \,|\, \lambda_i \in \mathbb{Z},\, (i = 1, \ldots, m) \right\}, \tag{8}$$

where $b_1, \ldots, b_n$ are linearly independent vectors in $\mathbb{R}^m$, and are called a *basis* of L. If $B = [b_1, \ldots, b_n]$, then we also call B a basis of L, and write $L = L(B)$. The determinant of L is

$$\det L = \sqrt{\det B^{\mathrm{T}} B}, \tag{9}$$

where B is a basis of L, with $\det L$ actually independent of the choice of B.

Finding a short, nonzero vector in a lattice is a fundamental algorithmic problem with many uses in cryptography, optimization, and number theory. For surveys we refer to [2], [3], [11], and [8]. More generally, one may want to find a reduced basis consisting of short, and nearly orthogonal vectors.

A basis $b_1, \ldots, b_n$ that is reduced according to the definition of Lenstra, Lenstra, and Lovász [7] is computable in polynomial time in the case of rational lattices, and the b_i are reasonably short, and near orthogonal, namely

$$\| b_1 \| \;\leq\; 2^{(n-1)/4} (\det L)^{1/n}, \tag{10}$$

$$\| b_1 \| \;\leq\; 2^{(n-1)/2} \, \| d \| \text{ for any } d \in L \setminus \{0\}, \tag{11}$$

$$\| b_1 \| \cdots \| b_n \| \;\leq\; 2^{n(n-1)/4} \det L. \tag{12}$$

hold. Korkhine-Zolotarev (KZ) bases, which were described in [5] by Korkhine, and Zolotarev, and by Kannan in [4] have stronger reducedness properties, for instance, the first vector in a KZ basis is the shortest vector of the lattice. However, KZ bases are computable in polynomial time only when n is fixed. Block KZ bases proposed by Schnorr in [9] form a hierarchy in between: one can trade on the quality of the basis to gain faster computing times.

Our Theorem 1 generalizes inequalities (10) through (12). For instance, (1) with $k = n$ yields (10), and with $k = 1$ yields (11). In turn, from (6) in Theorem 2 with $j = k$, and from (7) with $j = n$ we recover the inequalities of Theorem 1.

It would be interesting to see whether stronger versions of our results can be stated for KZ, or block KZ bases.

As a tool we use Lemma 1 below, which may be of independent interest. For $k = 1$ we can recover from it Lemma (5.3.11) in [2] (proven as part of Proposition (1.11) in [7]). To state it, we will recall the notion of Gram-Schmidt orthogonalization. If $b_1, \ldots, b_n \in \mathbb{R}^m$ is a basis of L, then the corresponding Gram-Schmidt vectors $b_1^*, \ldots, b_n^*$, are defined as

$$b_1^* = b_1 \text{ and } b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{ij} b_j \text{ for } i = 1, \ldots, n-1, \tag{13}$$

with $\mu_{ij} = \langle b_i, b_j^* \rangle / \langle b_j^*, b_j^* \rangle$, where $\langle ., . \rangle$ is the usual inner product on $\mathbb{R}^m$.

Lemma 1. *Let* $d_1, \ldots, d_k$ *be linearly independent vectors from the lattice* L*, and* $b_1^*, \ldots, b_n^*$ *the Gram Schmidt orthogonalization of an arbitary basis. Then*

$$\det L(d_1, \ldots, d_k) \geq \min_{1 \leq i_1 < \cdots < i_k \leq n} \left\{ \| b_{i_1}^* \| \ldots \| b_{i_k}^* \| \right\}. \tag{14}$$

□

In the rest of this section we collect necessary definitions, and results. In Section 2 we prove Lemma 1, and in Section 3 we prove Theorem 2.

We call $b_1, \ldots, b_n$ an *LLL-reduced basis of* L, if

$$|\mu_{ji}| \leq 1/2 \quad (j = 2, \ldots, n;\ i = 1, \ldots, j-1), \text{ and} \tag{15}$$

$$\| b_j^* + \mu_{j,j-1} b_{j-1}^* \|^2 \geq 3/4 \, \| b_{j-1}^* \|^2 \quad (1 < j \leq n). \tag{16}$$

From (15) and (16) it follows that

$$\| b_i^* \|^2 \leq 2^{j-i} \, \| b_j^* \|^2 \quad (1 \leq i \leq j \leq n). \tag{17}$$

If $b_1, \ldots, b_n$ are linearly independent vectors, then

$$\det L(b_1, \ldots, b_n) = \det L(b_1, \ldots, b_{n-1}) \, \| b' \|, \tag{18}$$

where b' is the projection of b_n on the orthogonal complement of the linear span of $b_1, \ldots, b_{n-1}$.

An integral square matrix U with ± 1 determinant is called unimodular. An elementary column operation performed on a matrix A is either 1) exchanging two columns, 2) multiplying a column by -1, or 3) adding an integral multiple of a column to another column. Multiplying a matrix A from the right by a unimodular U is equivalent to performing a sequence of elementary column operations on A.

2 Proof of Lemma 1

We need the following

Claim There are elementary column operations performed on $d_1, \ldots, d_k$ that yield $\bar{d}_1, \ldots, \bar{d}_k$ with

$$\bar{d}_i = \sum_{j=1}^{t_i} \lambda_{ij} b_j \text{ for } i = 1, \ldots, k, \tag{19}$$

where $\lambda_{ij} \in \mathbb{Z}$, $\lambda_{i,t_i} \neq 0$, and

$$t_k > t_{k-1} > \cdots > t_1. \tag{20}$$

Proof of Claim Let us write

$$BV \quad = \quad [d_1, \ldots, d_k], \tag{21}$$

with V an integral matrix. Analogously to how the Hermite Normal Form of an integral matrix is computed, we can do elementary column operations on V to obtain $\bar{V}$ with

$$t_k := \max \{ i \,|\, \bar{v}_{ik} \neq 0 \} \;>\; t_{k-1} := \max \{ i \,|\, \bar{v}_{i,k-1} \neq 0 \} \;>\; \ldots \;>\; t_1 := \max \{ i \,|\, \bar{v}_{i1} \neq 0 \}. \tag{22}$$

Performing the same elementary column operations on $d_1, \ldots, d_k$ yield $\bar{d}_1, \ldots, \bar{d}_k$ which satisfy

$$B\bar{V} \quad = \quad [\bar{d}_1, \ldots, \bar{d}_k], \tag{23}$$

so they satisfy (19).

End of proof of Claim

Obviously

$$\det\; L(\bar{d}_1, \ldots, \bar{d}_k) \;=\; \det\; L(d_1, \ldots, d_k). \tag{24}$$

Substituting from (13) for b_i we can rewrite (19) as

$$\bar{d}_i = \sum_{j=1}^{t_i} \lambda^*_{ij} b^*_j \text{ for } i = 1, \ldots, k, \tag{25}$$

where the λ^*_{ij} are now reals, but $\lambda^*_{i,t_i} = \lambda_{i,t_i}$ nonzero integers.

For all i we have

$$\text{lin} \{ \bar{d}_1, \ldots, \bar{d}_{i-1} \} \;\subseteq\; \text{lin}\{ b^*_1, \ldots, b^*_{t_{i-1}} \}. \tag{26}$$

Therefore

$$\|\,\text{Proj}\; \{ \bar{d}_i \,|\, \{ \bar{d}_1, \ldots, \bar{d}_{i-1} \}^{\perp} \} \,\| \geq \|\,\text{Proj}\; \{ \bar{d}_i \,|\, \{ b^*_1, \ldots, b^*_{t_{i-1}} \}^{\perp} \} \,\| \geq \|\, \lambda_{i,t_i} b^*_{t_i} \,\| \geq \|\, b^*_{t_i} \,\| \tag{27}$$

holds, with the second inequality coming from (20). So applying (18) repeatedly we get

$$\begin{aligned} \det\; L(\bar{d}_1, \ldots, \bar{d}_k) \quad &\geq \quad \det L(\bar{d}_1, \ldots, \bar{d}_{k-1}) \,\|\, b^*_{t_k} \,\| \\ &\ldots \\ &\geq \quad \|\, b^*_{t_1} \,\| \|\, b^*_{t_2} \,\| \ldots \|\, b^*_{t_k} \,\|, \end{aligned} \tag{28}$$

which together with (24) completes the proof. □

3 Proof of Theorem 1 and Theorem 2

The plan of the proof is as follows: we first prove (1) through (3) in Theorem 1. Then we prove Theorem 2. Finally, (4) follows as a special case of (7) with $j = k$; and (5) as a special case of (7) with $j = n$.

Proof of (1) and (2) Lemma 1 implies

$$\det\ L(d_1, \ldots, d_k) \quad \geq \quad \| b^*_{t_1} \| \| b^*_{t_2} \| \ldots \| b^*_{t_k} \| \tag{29}$$

for some $t_1, \ldots, t_k \in \{1, \ldots, n\}$ distinct indices. Clearly

$$t_1 + \cdots + t_k \leq kn - k(k-1)/2 \tag{30}$$

holds. Applying first (17), then (30) yields

$$\begin{aligned} (\det\ L(d_1, \ldots, d_k))^2 \quad &\geq \quad \| b^*_1 \|^2\, 2^{(1-t_1)} \ldots \| b^*_1 \|^2\, 2^{(1-t_k)} \\ &= \quad \| b^*_1 \|^{2k}\, 2^{k-(t_1+\cdots+t_k)} \\ &\geq \quad \| b_1 \|^{2k}\, 2^{k(k+1)/2-kn}, \end{aligned} \tag{31}$$

which is equivalent to (1). Similarly,

$$\begin{aligned} (\det\ L(d_1, \ldots, d_k))^2 \quad &\geq \quad \| b^*_1 \|^2\, 2^{(1-t_1)}\, \| b^*_2 \|^2\, 2^{(2-t_2)} \ldots \| b^*_k \|^2\, 2^{(k-t_k)} \\ &= \quad \| b^*_1 \|^2 \ldots \| b^*_k \|^2\, 2^{(1+\cdots+k)-(t_1+\cdots+t_k)} \\ &\geq \quad \| b^*_1 \|^2 \ldots \| b^*_k \|^2\, 2^{k(k-n)}, \end{aligned} \tag{32}$$

which is equivalent to (2).

□

Proof of (3) The proof is by induction. Let us write $D_k = (\det L(b_1, \ldots, b_k))^2$. For $k = n-1$, multiplying the inequalities

$$\| b^*_i \|^2 \leq 2^{n-i}\, \| b^*_n \|^2 \ \ (\, i = 1, \ldots, n-1) \tag{33}$$

gives

$$D_{n-1} \quad \leq \quad 2^{n(n-1)/2} (\| b^*_n \|^2)^{n-1} \tag{34}$$

$$\quad = \quad 2^{n(n-1)/2} \left(\frac{D_n}{D_{n-1}} \right)^{n-1}, \tag{35}$$

and after simplifying, we get

$$D_{n-1} \quad \leq \quad 2^{(n-1)/2} (D_n)^{1-1/n}. \tag{36}$$

Suppose that (3) is true for $k \leq n-1$; we will prove it for $k-1$. Since $b_1, \ldots, b_k$ forms an LLL-reduced basis of $L(b_1, \ldots, b_k)$ we can replace n by k in (36) to get

$$D_{k-1} \quad \leq \quad 2^{(k-1)/2} (D_k)^{(k-1)/k}. \tag{37}$$

By the induction hypothesis,

$$D_k \quad \leq \quad 2^{k(n-k)/2} (D_n)^{k/n}, \tag{38}$$

from which we obtain

$$(D_k)^{(k-1)/k} \quad \leq \quad 2^{(k-1)(n-k)/2}(D_n)^{(k-1)/n}. \tag{39}$$

Using the upper bound on $(D_k)^{(k-1)/k}$ from (39) in (37) yields

$$\begin{aligned} D_{k-1} &\leq 2^{(k-1)/2}2^{(k-1)(n-k)/2}(D_n)^{(k-1)/k} & (40)\\ &= 2^{(k-1)(n-(k-1))/2}(D_n)^{(k-1)/n}, & (41) \end{aligned}$$

as required.

□

Proof of Theorem 2 From (3) and (2) we have

$$\begin{aligned} \det L(b_1,\ldots,b_k) &\leq 2^{k(j-k)/4}(\det L(b_1,\ldots,b_j))^{k/j}, & (42)\\ \det L(b_1,\ldots,b_j) &\leq 2^{j(n-j)/2}\det L(d_1,\ldots,d_j). & (43) \end{aligned}$$

Raising (43) to the power of k/j gives

$$(\det L(b_1,\ldots,b_j))^{k/j} \quad \leq \quad 2^{k(n-j)/2}\det(L(d_1,\ldots,d_j))^{k/j}, \tag{44}$$

and plugging (44) into (42) proves (6).

It is shown in [7] that

$$\|\, b_i \,\|^2 \quad \leq \quad 2^{i-1}\,\|\, b_i^* \,\|^2 \ \text{ for } \ i = 1,\ldots,n. \tag{45}$$

Multiplying these inequalities for $i = 1,\ldots,k$ yields

$$\|\, b_1 \,\| \cdots \|\, b_k \,\| \quad \leq \quad 2^{k(n-1)/4}\det L(b_1,\ldots,b_k), \tag{46}$$

and using (46) with (6) yields (7).

□

Remark 1. The kth successive minimum of L is defined as the smallest real number t, such that there are k linearly independent vectors in L with length bounded by t. It is denoted by $\lambda_k(L)$. With the same setup as for (10)-(12) it is shown in [7] that

$$\|\, b_i \,\| \quad \leq \quad 2^{n-1}\lambda_i(L) \text{ for } i = 1,\ldots,n. \tag{47}$$

For KZ, and block KZ bases similar results were shown in [6], and [10], resp.

The successive minimum results (47) give a more global, and refined view of the lattice, and the reduced basis, than (10) through (12). Our Theorems 1 and 2 are similar in this respect, but they seem to be independent of (47). Of course, multiplying the latter for $i = 1,\ldots,k$ gives an upper bound on $\|\, b_1 \,\| \cdots \|\, b_k \,\|$, but in different terms.

The quantites $\det L(b_1, \ldots, b_k)$ and $\| b_1 \| \ldots \| b_k \|$ are also connected by

$$\det L(b_1, \ldots, b_k) = \| b_1 \| \ldots \| b_k \| \sin\theta_2 \ldots \sin\theta_k, \tag{48}$$

where θ_i is the angle of b_i with the subspace spanned by $b_1, \ldots, b_{i-1}$. In [1] Babai showed that the sine of the angle of *any* basis vector with the subspace spanned by the other basis vectors in a d-dimensional lattice is at least $(\sqrt{2}/3)^d$. One could combine the lower bounds on $\sin\theta_i$ with the upper bounds on $\det L(b_1, \ldots, b_k)$ to find an upper bound on $\| b_1 \| \ldots \| b_k \|$. However, the result would be weaker than (4) and (5).

Acknowledgement The first author thanks Ravi Kannan for helpful discussions.

References

[1] László Babai. On lovász lattice reduction, and the nearest lattice point problem. *Combinatorica*, 6:1–13, 1986.

[2] Martin Grötschel, Lászlo Lovász, and Alexander Schrijver. *Geometric Algorithms and Combinatorial Optimization*, volume 2 of *Algorithms and Combinatorics*. Springer, second corrected edition edition, 1993.

[3] Ravi Kannan. Algorithmic geometry of numbers. *Annual Review of Computer Science*, 2:231–267, 1987.

[4] Ravi Kannan. Minkowski's convex body theorem and integer programming. *Mathematics of Operations Research*, 12(3):415–440, 1987.

[5] A. Korkine and G. Zolotarev. Sur les formes quadratiques. *Mathematische Annalen*, 6:366–389, 1873.

[6] Jeffrey C. Lagarias, Hendrik W. Lenstra, and Claus P. Schnorr. Korkine-zolotarev bases and successive minina of a lattice and its reciprocal lattice. *Combinatorica*, 10(4):333–348, 1990.

[7] Arjen K. Lenstra, Hendrik W. Lenstra, Jr., and László Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261:515–534, 1982.

[8] D. Micciancio. *Complexity of lattice problems: a cryptographic perspective.* Kluwer Academic Publishers, 2002.

[9] Claus P. Schnorr. A hierarchy of polynomial time lattice basis reduction algorithms. *Theoretical Computer Science*, 53:201–225, 1987.

[10] Claus P. Schnorr. Block reduced lattice bases and successive minima. *Combinatorics, Probability, and Computing*, 3:507–533, 1994.

[11] Alexander Schrijver. *Theory of Linear and Integer Programming.* Wiley, Chichester, United Kingdom, 1986.