# Unifying LLL inequalities

Gábor Pataki and Mustafa Tural *

**Abstract**

The Lenstra, Lenstra, and Lovász (abbreviated as LLL) basis reduction algorithm computes a basis of a lattice consisting of short, and near orthogonal vectors. The quality of an LLL reduced basis is expressed by three fundamental inequalities, and it is natural to ask, whether these have a common generalization.

In this note we find unifying inequalities. Our main result is

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

$$\det L(b_1, \dots, b_k) \leq 2^{k(n-j)/2 + k(j-k)/4} (\det L(d_1, \dots, d_j))^{k/j}, \tag{1}$$

$$\| b_1 \| \cdots \| b_k \| \leq 2^{k(n-j)/2 + k(j-1)/4} (\det L(d_1, \dots, d_j))^{k/j}. \tag{2}$$

□

By setting $k$ and $j$ to either 1 or $n$, from (1) we can recover the first two LLL inequalities, and from (2) we can recover all three. Even with one degree of freedom left, i.e. with $k$ or $j$ fixed to 1 or $n$, or $k = j$, we obtain generalizations that seem to be new.
Our main lemma also generalizes a result of Lenstra, Lenstra and Lovász, and we believe that it is of independent interest:

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

$$\det L(d_1, \dots, d_k) \geq \min_{1 \leq i_1 < \dots < i_k \leq n} \left\{ \| b_{i_1}^* \| \dots \| b_{i_k}^* \| \right\}. \tag{3}$$

□

Mathematics subject classification codes: 11H06, 52C07

Key words: LLL basis reduction.

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

# 1 LLL reducedness, and unifying inequalities

A lattice is a set of the form

$$L = L(b_1, \ldots, b_n) = \left\{ \sum_{i=1}^{n} \lambda_i b_i \mid \lambda_i \in \mathbb{Z}, \, (i = 1, \ldots, n) \right\}, \tag{4}$$

where $b_1, \ldots, b_n$ are linearly independent vectors, and are called a *basis* of $L$. A lattice has infinitely many bases when $n \geq 2$. Computing one consisting of short, and nearly orthogonal vectors is a a fundamental algorithmic problem with uses in cryptography, optimization, and number theory.

Several concepts of reducedness of a lattice basis are known. The most widely used one is LLL reducedness, developed in the seminal paper [9] of Lenstra, Lenstra, and Lovász. For a collection of articles on the history of lattice theory, complexity aspects, and the LLL algorithm we refer to the proceedings of the LLL+25 conference [2]. Surveys and textbook treatments of lattice basis reduction can be found in [4], [5], [16], and [10].

An LLL reduced basis $b_1, \ldots, b_n$ is computable in polynomial time in the case of rational lattices, and the quality of the basis is expressed by three fundamental inequalities:

$$\| b_1 \| \leq 2^{(n-1)/4} (\det L)^{1/n}, \tag{LLL1}$$

$$\| b_1 \| \leq 2^{(n-1)/2} \, \| d \| \;\text{ for any }\; d \in L \setminus \{0\}, \tag{LLL2}$$

$$\| b_1 \| \cdots \| b_n \| \leq 2^{n(n-1)/4} \det L. \tag{LLL3}$$

Here $\det L$ is the determinant of the lattice, i.e. letting $B = [b_1, \ldots, b_n]$, it is defined as

$$\det L = \sqrt{\det B^{\mathrm{T}} B}, \tag{5}$$

with $\det L$ actually independent of the choice of the basis. Improvements of the running time of the LLL algorithm were given by Schnorr [14] and Nguyen and Stehlé in [11].

Korkhine-Zolotarev (KZ) bases were described in [7] by Korkhine, and Zolotarev, and by Kannan in [6]. These bases have stronger reducedness properties. For instance, the first vector in a KZ basis is the shortest vector of the lattice, as opposed to the weaker guarantee given by (LLL1). However, KZ bases are computable in polynomial time only when $n$ is fixed. Schnorr in [13] proposed several hierarchies of bases between LLL and KZ reduced ones: the semi block $2k$ bases among them are polynomial time computable when $k$ is fixed, and both the quality of the basis, and the complexity of the reduction algorithm increases with $k$.

It is natural to ask, whether the three beautiful inequalities (LLL1)-(LLL3) can be unified, and generalized: for instance, whether the product of the norms of the first few basis vectors can be bounded in terms of $\det L$, or if the norm of the first basis vector can be bounded by other parameters of $L$. Our Theorem 1 finds such generalizations. We think that Lemma 1 is also of interest. For $k = 1$ we can recover from it Lemma (5.3.11) in [4] (proven as part of Proposition (1.11) in [9]).

Somewhat surprisingly, even with one degree of freedom, i.e. when one of $k$ and $j$ fixed to 1 or $n$, or $k = j$ in Theorem 1 we obtain inequalities that appear to be new. We list these intermediate inequalities in

**Corollary 1.** *Let $b_1, \ldots, b_n$ be an LLL-reduced basis of the lattice $L$, and $d_1, \ldots, d_k$ arbitrary linearly independent vectors in $L$. Then*

$$\| b_1 \| \leq 2^{(n-k)/2+(k-1)/4} (\det L(d_1, \ldots, d_k))^{1/k}, \tag{6}$$

$$\det L(b_1, \ldots, b_k) \leq 2^{k(n-k)/2} \det L(d_1, \ldots, d_k), \tag{7}$$

$$\det L(b_1, \ldots, b_k) \leq 2^{k(n-k)/4} (\det L)^{k/n}, \tag{8}$$

$$\| b_1 \| \cdots \| b_k \| \leq 2^{k(n-k)/2+k(k-1)/4} \det L(d_1, \ldots, d_k), \tag{9}$$

$$\| b_1 \| \cdots \| b_k \| \leq 2^{k(n-1)/4} (\det L)^{k/n}. \tag{10}$$

□

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 1. In Section 4 we point out how our results imply that the first few vectors of an LLL reduced basis give an approximation of Rankin's constant introduced by Rankin in [12] and more recently studied by Gama et. al. in [3]. Here we also discuss how our results relate to the successive minima results in [9] and Babai's result in [1] on the shape of LLL reduced parallelepipeds.

If $b_1, \ldots, b_n$ is a basis of $L$, then the corresponding Gram-Schmidt vectors $b_1^*, \ldots, b_n^*$, are defined as

$$b_1^* = b_1 \text{ and } b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{ij} b_j \text{ for } i = 1, \ldots, n-1, \tag{11}$$

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

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

$$|\mu_{ji}| \leq 1/2 \quad (j = 2, \ldots, n;\ i = 1, \ldots, j-1), \text{ and} \tag{12}$$

$$\| b_j^* + \mu_{j,j-1} b_{j-1}^* \|^2 \geq 3/4 \, \| b_{j-1}^* \|^2 \quad (1 < j \leq n). \tag{13}$$

From (12) and (13)

$$\| b_i^* \|^2 \leq 2^{j-i} \, \| b_j^* \|^2 \quad (1 \leq i \leq j \leq n) \tag{14}$$

follows, and this is the only property of LLL reduced bases that we shall use.

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

$$\det L(b_1, \ldots, b_n) = \det L(b_1, \ldots, b_{n-1}) \, \| b' \|, \tag{15}$$

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 $\pm 1$ 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. Multiplying a matrix from the right by a unimodular $U$ is equivalent to performing a sequence of elementary column operations on it.

## 2 Proof of Lemma 1

We first need a claim.

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

$$\bar{d}_i = \sum_{j=1}^{t_i} \lambda_{ij} b_j \text{ for } i = 1, \ldots, k, \tag{16}$$

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

$$t_k > t_{k-1} > \cdots > t_1. \tag{17}$$

**Proof of Claim** Let $B = [b_1, \ldots, b_n]$, and write

$$BV = [d_1, \ldots, d_k], \tag{18}$$

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

$$t_k := \max\{\, i \,|\, \bar{v}_{ik} \neq 0 \,\} > t_{k-1} := \max\{\, i \,|\, \bar{v}_{i,k-1} \neq 0 \,\} > \ldots > t_1 := \max\{\, i \,|\, \bar{v}_{i1} \neq 0 \,\}. \tag{19}$$

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

$$B\bar{V} = [\bar{d}_1, \ldots, \bar{d}_k], \tag{20}$$

so they satisfy (16).

**End of proof of Claim**

Obviously

$$\det \; L(\bar{d}_1, \ldots, \bar{d}_k) = \det \; L(d_1, \ldots, d_k). \tag{21}$$

Substituting from (11) for $b_i$ we rewrite (16) as

$$\bar{d}_i = \sum_{j=1}^{t_i} \lambda^*_{ij} b^*_j \text{ for } i = 1, \ldots, k, \tag{22}$$

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

For all $i$ we have

$$\text{lin}\{\,\bar d_1,\ldots,\bar d_{i-1}\,\} \subseteq \text{lin}\{\,b^*_1,\ldots,b^*_{t_{i-1}}\,\}. \tag{23}$$

Therefore

$$\|\,\text{Proj}\ \{\,\bar d_i\,|\,\{\,\bar d_1,\ldots,\bar d_{i-1}\,\}^\perp\,\}\,\| \geq \|\,\text{Proj}\ \{\,\bar d_i\,|\,\{\,b^*_1,\ldots,b^*_{t_{i-1}}\,\}^\perp\,\}\,\| \geq \|\,\lambda_{i,t_i} b^*_{t_i}\,\| \geq \|\,b^*_{t_i}\,\| \tag{24}$$

holds, with the second inequality coming from (17). So applying (15) repeatedly we get

$$\begin{aligned} \det\ L(\bar d_1,\ldots,\bar d_k) &\geq \det L(\bar d_1,\ldots,\bar d_{k-1})\,\|\,b^*_{t_k}\,\| \\ &\ldots \\ &\geq \|\,b^*_{t_1}\,\|\|\,b^*_{t_2}\,\| \ldots \|\,b^*_{t_k}\,\|, \end{aligned} \tag{25}$$

which together with (21) completes the proof. □

## 3 Proof of Theorem 1

Theorem 1 will follow from the special cases of Corollary 1, so we first prove (7) and (8) in the latter, then complete the proof of Theorem 1.

**Proof of (7)** Lemma 1 implies

$$\det\ L(d_1,\ldots,d_k) \geq \|\,b^*_{t_1}\,\|\|\,b^*_{t_2}\,\| \ldots \|\,b^*_{t_k}\,\| \tag{26}$$

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

$$t_1 + \cdots + t_k \leq kn - k(k-1)/2 \tag{27}$$

holds. Applying first (14), then (27) yields

$$\begin{aligned} (\det\ L(d_1,\ldots,d_k))^2 &\geq \|\,b^*_1\,\|^2\ 2^{(1-t_1)}\ \|\,b^*_2\,\|^2\ 2^{(2-t_2)} \ldots \|\,b^*_k\,\|^2\ 2^{(k-t_k)} \\ &= \|\,b^*_1\,\|^2 \ldots \|\,b^*_k\,\|^2\ 2^{(1+\cdots+k)-(t_1+\cdots+t_k)} \\ &\geq \|\,b^*_1\,\|^2 \ldots \|\,b^*_k\,\|^2\ 2^{k(k-n)}, \end{aligned} \tag{28}$$

which is equivalent to (7).

□

**Proof of (8)** We use induction. Let us write $D_k = (\det L(b_1,\ldots,b_k))^2$. For $k = n-1$, multiplying the inequalities

$$\|\,b^*_i\,\|^2 \leq 2^{n-i}\ \|\,b^*_n\,\|^2\ \ (\,i = 1,\ldots,n-1) \tag{29}$$

gives

$$D_{n-1} \leq 2^{n(n-1)/2}(\|b_n^*\|^2)^{n-1} \tag{30}$$

$$= 2^{n(n-1)/2}\left(\frac{D_n}{D_{n-1}}\right)^{n-1}, \tag{31}$$

and after simplifying, we get

$$D_{n-1} \leq 2^{(n-1)/2}(D_n)^{1-1/n}. \tag{32}$$

Suppose that (8) 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 (32) to get

$$D_{k-1} \leq 2^{(k-1)/2}(D_k)^{(k-1)/k}. \tag{33}$$

By the induction hypothesis,

$$D_k \leq 2^{k(n-k)/2}(D_n)^{k/n}, \tag{34}$$

from which we obtain

$$(D_k)^{(k-1)/k} \leq 2^{(k-1)(n-k)/2}(D_n)^{(k-1)/n}. \tag{35}$$

Using the upper bound on $(D_k)^{(k-1)/k}$ from (35) in (33) yields

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

$$= 2^{(k-1)(n-(k-1))/2}(D_n)^{(k-1)/n}, \tag{37}$$

as required.

□

**Proof of Theorem 1** From (8) and (7) we obtain

$$\det L(b_1, \ldots, b_k) \leq 2^{k(j-k)/4}(\det L(b_1, \ldots, b_j))^{k/j}, \tag{38}$$

$$\det L(b_1, \ldots, b_j) \leq 2^{j(n-j)/2} \det L(d_1, \ldots, d_j). \tag{39}$$

Raising (39) to the power of $k/j$ gives

$$(\det L(b_1, \ldots, b_j))^{k/j} \leq 2^{k(n-j)/2} \det(L(d_1, \ldots, d_j))^{k/j}, \tag{40}$$

and plugging (40) into (38) proves (1).

It is shown in [9] that

$$\|b_i\|^2 \leq 2^{i-1}\|b_i^*\|^2 \text{ for } i = 1, \ldots, n. \tag{41}$$

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

$$\|b_1\| \cdots \|b_k\| \leq 2^{k(n-1)/4} \det L(b_1, \ldots, b_k), \tag{42}$$

and combining (42) with (1) yields (2).

□

# 4 Discussion

Rankin's invariant $\gamma_{n,k}(L)$ for an $n$-dimensional lattice $L$ is defined as

$$\gamma_{n,k}(L) = \min_{S \text{ is a sublattice of } L, \dim S = k} \left( \frac{\det S}{(\det L)^{k/n}} \right)^2, \tag{43}$$

and Rankin's constant $\gamma_{n,k}$ is the maximum of the $\gamma_{n,k}(L)$ over all $n$-dimensional lattices. In Gama et al [3] upper and lower bounds were proven for $\gamma_{2k,k}$. Our inequality (8) implies that for an $n$-dimensional lattice $L$

$$\gamma_{n,k}(L) \leq 2^{k(n-k)/2} \tag{44}$$

holds, and this inequality is achieved by the sublattice generated by first $k$ vectors of an LLL reduced basis of $L$.

The $k$th successive minimum of $L$ is 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 (LLL1)-(LLL3) it is shown in [9] that

$$\| b_i \| \leq 2^{n-1} \lambda_i(L) \text{ for } i = 1, \dots, n. \tag{45}$$

For KZ, and block KZ bases similar results were shown in [8], and [15], resp.

The successive minimum results (45) give a more global view of the lattice, and the reduced basis, than (LLL1) through (LLL3). Our Theorem 1 is similar in this respect, but it seems to be independent of (45). Of course, multiplying the latter for $i = 1, \dots, k$ gives an upper bound on $\| b_1 \| \cdots \| b_k \|$, but in different terms.

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

$$\det L(b_1, \dots, b_k) = \| b_1 \| \dots \| b_k \| \sin \theta_2 \dots \sin \theta_k, \tag{46}$$

where $\theta_i$ is the angle of $b_i$ with the subspace spanned by $b_1, \dots, b_{i-1}$. 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 $\det L(b_1, \dots, b_k)$ to find an upper bound on $\| b_1 \| \dots \| b_k \|$ . However, the result would be weaker than (9) and (10).

# References


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

[2] P. Nguyen et al, editor. *Proceedings of the LLL+25 conference.* University of Caen, France, 2007.

[3] Nicolas Gama, Nick Howgrave-Graham, Henrik Koy, and Phong Q. Nguyen. Rankin's constant and blockwise lattice reduction. In *CRYPTO*, pages 112–130, 2006.

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

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

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

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

[8] 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.

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

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

[11] Phong Q. Nguyen and Damien Stehlé. An lll algorithm with quadratic complexity. *SIAM J. on Computing*, to appear, 2009.

[12] R. A. Rankin. On positive definite quadratic forms. *J. London Math Soc*, 28:309–314, 1953.

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

[14] Claus P. Schnorr. A more efficient algorithm for lattice basis reduction. *J. of Algorithms*, 9(1):47–62, 1988.

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

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