Reduction of Lattice Bases

Curtis Bright

April 29, 2009

Abstract

A study of multiple lattice basis reductions and their properties, culminating in LLL introduced via recursive projection.

1 Introduction

A point lattice (or simply *lattice*) is a discrete additive subgroup of $\mathbb{R}^n$. A *basis* for a lattice $\mathcal{L} \subset \mathbb{R}^n$ is a set of d linearly independent vectors $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_d \in \mathbb{R}^n$ whose 'integer span' generates $\mathcal{L}$. When $B \in \mathbb{R}^{d\times n}$ is a full-rank matrix with row vectors $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_d$ we write

$$\mathcal{L}(B) = \Big\{ \sum_{i=1}^{d} x_i \boldsymbol{b}_i : x_i \in \mathbb{Z} \Big\}$$

and say the lattice is generated by the basis B. In particular this report considers the case when $B \in \mathbb{Z}^{d\times n}$.

A lattice $\mathcal{L}(B)$ where $d = 1$ has only the single basis B (up to sign), but otherwise a lattice admits an infinite number of distinct bases. Most are cumbersome to work with, for example consider the two bases

$$B = \begin{bmatrix} -32 & 27 & 99 & 92 \\ -74 & 8 & 29 & -31 \\ -4 & 69 & 44 & 67 \end{bmatrix}$$

$$B' = \begin{bmatrix} -4339936 & -682927 & -2330272 & -6748685 \\ 268783718 & 42311760 & 144378994 & 418036006 \\ 47833660 & 7038229 & 23910075 & 72218282 \end{bmatrix}$$

where we actually have $\mathcal{L}(B) = \mathcal{L}(B')$. This can be seen by the existence of the change-of-basis matrix

$$U = \begin{bmatrix} -46154 & 78658 & -957 \\ 2859121 & -4871793 & 59273 \\ 488235 & -858094 & 10444 \end{bmatrix}$$

which satisfies $B' = UB$ as well as $B = U^{-1}B'$ where U^{-1} has integer entries.

In fact, in general if $\mathcal{L}(B) = \mathcal{L}(B')$ then any row of B' can be written as a $\mathbb{Z}$-linear combination of the rows of B and vice-versa, so a matrix U always exists such that $U, U^{-1} \in \mathbb{Z}^{d \times d}$. Such matrices are called *unimodular* and since $\det(U)$ and $\det(U^{-1}) = 1/\det(U)$ are both integers, $\det(U) = \pm 1$.

It follows that the volume of the d-dimensional parallelotope formed by the $[0, 1)$-span of the basis vectors depends only on the lattice, not on the choice of basis:

$$\begin{aligned} \operatorname{vol}(\mathcal{L}(B')) &= \sqrt{\det(B'B'^T)} \\ &= \sqrt{\det(UBB^TU^T)} \\ &= \sqrt{\det(BB^T)} \\ &= \operatorname{vol}(\mathcal{L}(B)) \end{aligned}$$

Though mathematically B and B' describe the same lattice, computationally B is generally much nicer to work with. This suggests that we develop the following:

1. A method of *ranking* the bases of a lattice in some desirable order.
2. A way to find desirable bases of a lattice when given one of its other bases, i.e., an algorithm for *basis reduction*.

2 Minkowski Reduction

The best possible basis $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_d$ of $\mathcal{L}$ would have $\boldsymbol{b}_1$ the shortest possible nonzero vector in $\mathcal{L}$ and in general $\boldsymbol{b}_i$ the shortest possible nonzero vector such that $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_i$ are linearly independent (the lengths of such vectors are called the *successive minima* of $\mathcal{L}$). Although such vectors $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_d \in \mathcal{L}$ of course always exist, it is perhaps surprising that if $d \geq 4$ such vectors do not necessarily form a basis of $\mathcal{L}$.

For example, consider the lattice $\mathcal{L}$ generated by the following basis:

$$\begin{bmatrix} 2 & & & & \\ & 2 & & & \\ & & \ddots & & \\ & & & 2 & \\ 1 & 1 & \cdots & 1 & 1 \end{bmatrix} \in \mathbb{Z}^{n \times n}$$

Note for $n \geq 5$ the shortest nonzero vector in $\mathcal{L}$ has a norm of 2 and since $2\boldsymbol{b}_n - \sum_{i=1}^{n-1} \boldsymbol{b}_i = \begin{bmatrix} 0 & 0 & \cdots & 0 & 2 \end{bmatrix}$, there are exactly n vectors (disregarding sign) which reach that minimum. These vectors are linearly independent but generate $(2\mathbb{Z})^n$ rather than $\mathcal{L}$.

Since we can't use the shortest possible linearly independent vectors in $\mathcal{L}$ as our criterion for a desirable basis, we insert a clause which ensures the previous case cannot occur.

Definition. *A basis $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_d$ of $\mathcal{L}$ is Minkowski reduced if $\boldsymbol{b}_i$ is the shortest possible vector such that $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_i$ may be extended into a basis for each $1 \leq i \leq d$.*

Unfortunately, the computation of a Minkowski reduced basis leads to a combinatorial problem with an exponential search space in d. Even the computation of $\boldsymbol{b}_1$ in a Minkowski reduced basis (known as the *Shortest Vector Problem* or SVP) seems infeasible: it is NP-hard with respect to the maximum norm [6]. With respect to the Euclidean norm, SVP is NP-hard under a randomized (opposed to deterministic) reduction [1].

3 Lagrange Reduction

Before moving to the general case it will be useful to consider a simple reduction in two dimensions. Historically this was the first lattice reduction considered (by Lagrange in 1773), and it gives rise to a simple algorithm, rather similar in style to Euclid's famous gcd algorithm: the norms of the input vectors are continually decreased by subtracting appropriate multiples of one vector from the other.

If $\|\boldsymbol{b}_1\| \leq \|\boldsymbol{b}_2\|$ then the "appropriate multiplier" here is the $v \in \mathbb{Z}$ which minimizes $\|\boldsymbol{b}_2 - v\boldsymbol{b}_1\|$. Optimally, this minimum would have value

$$\left\|\boldsymbol{b}_2 - \mathrm{proj}_{\boldsymbol{b}_1}(\boldsymbol{b}_2)\right\| = \left\|\boldsymbol{b}_2 - \tfrac{\langle \boldsymbol{b}_1, \boldsymbol{b}_2 \rangle}{\|\boldsymbol{b}_1\|^2} \boldsymbol{b}_1\right\|$$

and so $v = \frac{\langle \boldsymbol{b}_1, \boldsymbol{b}_2 \rangle}{\|\boldsymbol{b}_1\|^2}$, except that this may well not be an integer, and in which case $\boldsymbol{b}_2 - v\boldsymbol{b}_1 \notin \mathcal{L}$. Instead, taking the closest integer to $\frac{\langle \boldsymbol{b}_1, \boldsymbol{b}_2 \rangle}{\|\boldsymbol{b}_1\|^2}$ will ensure we remain in $\mathcal{L}$ while also minimizing $\|\boldsymbol{b}_2 - v\boldsymbol{b}_1\|$. In the case $\left|\frac{\langle \boldsymbol{b}_1, \boldsymbol{b}_2 \rangle}{\|\boldsymbol{b}_1\|^2}\right| \leq \frac{1}{2}$ there is no multiplier we can use to strictly decrease the norm.

Definition. *A basis $\boldsymbol{b}_1, \boldsymbol{b}_2$ of $\mathcal{L}$ is Lagrange reduced if $\|\boldsymbol{b}_1\| \leq \|\boldsymbol{b}_2\|$ and $\left|\frac{\langle \boldsymbol{b}_1, \boldsymbol{b}_2 \rangle}{\|\boldsymbol{b}_1\|^2}\right| \leq \frac{1}{2}$.*

Based on this definition, an obvious iterative algorithm presents itself:

Algorithm 1 LagrangeReduce

Input: A basis $\boldsymbol{b}_1, \boldsymbol{b}_2$ of a lattice $\mathcal{L}$
Output: A Lagrange reduced basis of $\mathcal{L}$

1: **repeat**
2: **if** $\|\boldsymbol{b}_1\| > \|\boldsymbol{b}_2\|$ **then** swap $\boldsymbol{b}_1$ and $\boldsymbol{b}_2$
3: $\boldsymbol{b}_2 := \boldsymbol{b}_2 - \text{round}\left(\frac{\langle \boldsymbol{b}_1, \boldsymbol{b}_2 \rangle}{\|\boldsymbol{b}_1\|^2}\right)\boldsymbol{b}_1$
4: **until** $\|\boldsymbol{b}_1\| \leq \|\boldsymbol{b}_2\|$
5: **return** $(\boldsymbol{b}_1, \boldsymbol{b}_2)$

In fact, a Lagrange reduced basis is also a Minkowski reduced basis. For arbitrary $\boldsymbol{b} = \alpha\boldsymbol{b}_1 + \beta\boldsymbol{b}_2$ in $\mathcal{L}$ it may be shown using simple algebra (see [5]) that a Lagrange reduced basis satisfies

$$\left(\alpha^2 - \alpha\beta + \beta^2\right)\|\boldsymbol{b}_1\|^2 \leq \|\boldsymbol{b}\|^2 \tag{1}$$

$$\left(\beta^2 - 1\right)\left(\|\boldsymbol{b}_2\|^2 - \|\boldsymbol{b}_1\|^2\right) + \|\boldsymbol{b}_2\|^2 \leq \|\boldsymbol{b}\|^2 \tag{2}$$

If $\boldsymbol{b}$ is nonzero then $\alpha\beta \neq 0$, so $1 \leq \alpha^2 - \alpha\beta + \beta^2$ and (1) implies $\|\boldsymbol{b}_1\| \leq \|\boldsymbol{b}\|$, i.e., $\boldsymbol{b}_1$ is the shortest possible nonzero vector in $\mathcal{L}$. If $\boldsymbol{b}$ is linearly independent with $\boldsymbol{b}_1$ then $\beta \neq 0$, so $1 \leq \beta^2 - 1$ and (2) implies $\|\boldsymbol{b}_2\| \leq \|\boldsymbol{b}\|$, i.e., $\boldsymbol{b}_2$ is the shortest possible vector linearly independent with $\boldsymbol{b}_1$.

3.1 Cost of LagrangeReduce

To estimate the complexity, let $\mu = \frac{\langle \boldsymbol{b}_1, \boldsymbol{b}_2 \rangle}{\|\boldsymbol{b}_1\|^2}$ and $v = \text{round}(\mu)$ after line 2 of some iteration which is not the first or the last. Clearly we have $v \neq 0$ and $\|\boldsymbol{b}_1\| > \|\boldsymbol{b}_2 - v\boldsymbol{b}_1\|$, otherwise the **until** statement will evaluate to true and this would be the last iteration.

Now, if $v = 1$ then we have $\|\boldsymbol{b}_1\| > \|\boldsymbol{b}_2 - \boldsymbol{b}_1\|$, which means after line 3 of the previous iteration we would have had $\|\boldsymbol{b}_2\| > \|\boldsymbol{b}_1 - \boldsymbol{b}_2\| = \|\boldsymbol{b}_2 - \boldsymbol{b}_1\|$. This is impossible since it means we could've decreased $\boldsymbol{b}_2$ even more by subtracting off another copy of $\boldsymbol{b}_1$, but line 3 always chooses v such that the decrease in $\boldsymbol{b}_2$ is maximized.

Similarly for $v = -1$, so we know that $|v| \geq 2$, $|\mu| \geq \frac{3}{2}$ and of course $|\mu - v| \leq \frac{1}{2}$. Let $\boldsymbol{b}_2'$ denote the component of $\boldsymbol{b}_2$ orthogonal to $\boldsymbol{b}_1$. Then from $\boldsymbol{b}_2 = \mu\boldsymbol{b}_1 + \boldsymbol{b}_2'$ we have:

$$\begin{aligned} \boldsymbol{b}_2 - v\boldsymbol{b}_1 &= (\mu - v)\boldsymbol{b}_1 + \boldsymbol{b}_2' \\ \|\boldsymbol{b}_2 - v\boldsymbol{b}_1\|^2 &= (\mu - v)^2 \|\boldsymbol{b}_1\|^2 + \|\boldsymbol{b}_2'\|^2 \\ &\leq \tfrac{1}{4} \|\boldsymbol{b}_1\|^2 + \|\boldsymbol{b}_2'\|^2 \end{aligned} \tag{3}$$

Again from $\boldsymbol{b}_2 = \mu\boldsymbol{b}_1 + \boldsymbol{b}_2'$ we have:

$$\begin{aligned} \|\boldsymbol{b}_2\|^2 &= \mu^2 \|\boldsymbol{b}_1\|^2 + \|\boldsymbol{b}_2'\|^2 \\ &\geq \tfrac{9}{4} \|\boldsymbol{b}_1\|^2 + \|\boldsymbol{b}_2'\|^2 \\ &\geq 2 \|\boldsymbol{b}_1\|^2 + \|\boldsymbol{b}_2 - v\boldsymbol{b}_1\|^2 \qquad \text{from (3)} \\ &> 3 \|\boldsymbol{b}_2 - v\boldsymbol{b}_1\|^2 \end{aligned}$$

using that $\|\boldsymbol{b}_1\| > \|\boldsymbol{b}_2 - v\boldsymbol{b}_1\|$ since this isn't the last iteration. Therefore, we have that when $\boldsymbol{b}_2$ is reassigned in step 3 *its norm decreases by a factor of at least* $\sqrt{3}$ (except possibly on the first and last iterations, where it at least doesn't increase). Since $\|\boldsymbol{b}_2\| \geq 1$ we have that the number of loop iterations is $O(\log_{\sqrt{3}} \|\boldsymbol{b}_2\|)$, where $\boldsymbol{b}_2$ is the second vector before its first decrease.

As a crude upper bound, we know that the arithmetic operations in each loop take $O(\log^2 \|\boldsymbol{b}_2\|)$ bit operations, so overall the algorithm runs with $O(\log^3 \|\boldsymbol{b}_2\|)$ bit operations.

Actually, each loop costs only $O(\log \|\boldsymbol{b}_2\| (1 + \log \|\boldsymbol{b}_2\| - \log \|\boldsymbol{b}_1\|))$ and summing over all iterations (while updating the values taken by $\boldsymbol{b}_1$ and $\boldsymbol{b}_2$) leads to a cascade resulting in a $O(\log^2 \|\boldsymbol{b}_2\|)$ cost, as described in [4].

4 Recursive Projections

The reductions we will see in arbitrary dimension will generally have similar conditions for d basis vectors as Lagrange reduction did for 2 basis vectors, but there will be an extra *recursive* component: the conditions will also apply

to the basis vectors of the lattice of degree $d-1$ formed by projecting all lattice points orthogonally to the first basis vector. As previously mentioned, the basis of a lattice with $d = 1$ is always reduced and will serve as our base case for the recursion.

To this end, it will be helpful to make the following definition which applies to the vectors of a basis $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_d$.

Definition. *Define the "kth recursive projection" of* $\boldsymbol{b}_i$ *as*

$$\boldsymbol{b}_i^{(k)} := \begin{cases} \boldsymbol{b}_i & \text{if } k = 0 \\ \text{proj}_{\text{span}\left(\boldsymbol{b}_k^{(k-1)}\right)^\perp}\left(\boldsymbol{b}_i^{(k-1)}\right) & \text{if } k \geq 1 \end{cases}.$$

We will also use the following shorthand:

$$\boldsymbol{b}_i' := \boldsymbol{b}_i^{(1)}$$
$$\boldsymbol{b}_i^* := \boldsymbol{b}_i^{(i-1)}$$

Although this will be a convenient definition for our formulations of recursive reductions, the following lemma shows we also have a nice iterative form for $\boldsymbol{b}_i^{(k)}$ which is easier to actually work with.

Lemma.

$$\boldsymbol{b}_i^{(k)} = \text{proj}_{\text{span}(\boldsymbol{b}_1^*, \boldsymbol{b}_2^*, \ldots, \boldsymbol{b}_k^*)^\perp}(\boldsymbol{b}_i)$$

Proof. By induction on k. If $k = 0$ then we are projecting onto $\emptyset^\perp = \mathbb{R}^n$ and hence $\boldsymbol{b}_i^{(0)} = \boldsymbol{b}_i$ as required.

Assume the lemma holds for some $k \geq 0$. Then by definition, hypothesis, and a property of projection,

$$\begin{aligned} \boldsymbol{b}_i^{(k+1)} &= \text{proj}_{\text{span}(\boldsymbol{b}_{k+1}^*)^\perp}\left(\boldsymbol{b}_i^{(k)}\right) \\ &= \text{proj}_{\text{span}(\boldsymbol{b}_{k+1}^*)^\perp}\left(\text{proj}_{\text{span}(\boldsymbol{b}_1^*, \boldsymbol{b}_2^*, \ldots, \boldsymbol{b}_k^*)^\perp}(\boldsymbol{b}_i)\right) \\ &= \text{proj}_{\text{span}(\boldsymbol{b}_1^*, \boldsymbol{b}_2^*, \ldots, \boldsymbol{b}_k^*, \boldsymbol{b}_{k+1}^*)^\perp}(\boldsymbol{b}_i) \end{aligned}$$

and the lemma holds for $k + 1$ as well. □

It follows that the vectors $\boldsymbol{b}_i^*$ are in fact the standard Gram-Schmidt orthogonalization defined by

$$\boldsymbol{b}_i^* = \text{proj}_{\text{span}(\boldsymbol{b}_1^*, \ldots, \boldsymbol{b}_{i-1}^*)^\perp}(\boldsymbol{b}_i) = \boldsymbol{b}_i - \sum_{j=1}^{i-1} \mu_{i,j} \boldsymbol{b}_j^* \quad \text{with} \quad \mu_{i,j} = \frac{\langle \boldsymbol{b}_i, \boldsymbol{b}_j^* \rangle}{\|\boldsymbol{b}_j^*\|^2}.$$

And $\boldsymbol{b}_i^{(k)}$ for $1 \leq k \leq i-2$ is the 'truncated' Gram-Schmidt orthogonalization $\boldsymbol{b}_i^{(k)} = \boldsymbol{b}_i - \sum_{j=1}^{k} \mu_{i,j} \boldsymbol{b}_j^*$.

5 Korkin-Zolotarev Reduction

If $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_d$ are a basis for $\mathcal{L}$ then we previously defined $\boldsymbol{b}'_2, \ldots, \boldsymbol{b}'_d$ to be the components of $\boldsymbol{b}_2, \ldots, \boldsymbol{b}_d$ orthogonal to $\boldsymbol{b}_1$, i.e., their projections over the orthogonal component of $\text{span}(\boldsymbol{b}_1)$. As a natural extension of this notation, define $\mathcal{L}'$ to be the lattice generated by $\boldsymbol{b}'_2, \ldots, \boldsymbol{b}'_d$.

Definition. *A basis $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_d$ of $\mathcal{L}$ is Korkin-Zolotarev reduced if*

- $\boldsymbol{b}_1$ *is the shortest possible nonzero vector of* $\mathcal{L}$
- $\boldsymbol{b}'_2, \ldots, \boldsymbol{b}'_d$ *is a Korkin-Zolotarev reduced basis of* $\mathcal{L}'$
- $\boldsymbol{b}_2, \ldots, \boldsymbol{b}_d$ *are as short as possible without changing* $\boldsymbol{b}'_2, \ldots, \boldsymbol{b}'_d$*, i.e.,* $|\mu_{i,1}| \leq \frac{1}{2}$ *for* $2 \leq i \leq d$

Again we have a reduction which requires solving SVP and so shouldn't be expected to be practical for large d. However, Korkin-Zolotarev reduced do have some nice properties, for example:

$$\prod_{i=1}^{d} \|\boldsymbol{b}_i\| \leq \left(\tfrac{4}{3}\right)^{d(d-1)/4} \text{vol}(\mathcal{L})$$

Later we will show that Hermite reduced bases satisfy this bound and simultaneously get it for Korkin-Zolotarev bases (since they are Hermite reduced bases as well). Note the similarity with Hadamard's bound (which follows from Gram-Schmidt):

$$\text{vol}(\mathcal{L}) \leq \prod_{i=1}^{d} \|\boldsymbol{b}_i\|$$

with equality if and only if the $\boldsymbol{b}_i$ are orthogonal. So intuitively

$$\prod_{i=1}^{d} \|\boldsymbol{b}_i\| \,/\, \text{vol}(\mathcal{L})$$

measures the amount of "nonorthogonality" in a basis and is sometimes called the *orthogonality defect*. We would like to show that the basis reductions we consider have a bounded orthogonality defect which only depends on some function of the lattice dimension d.

5.1 Size Reduction

Notice that while the second KZ condition ensures that $\boldsymbol{b}'_2, \ldots, \boldsymbol{b}'_d$ are short vectors, this does not ensure that $\boldsymbol{b}_2, \ldots, \boldsymbol{b}_d$ are short vectors since there are an infinite number of possible ways to 'lift' the $\boldsymbol{b}'_i \in \mathcal{L}'$ into $\boldsymbol{b}_i \in \mathcal{L}$ (most of them yielding huge $\boldsymbol{b}_i$). We of course want the shortest possible 'lifts' from $\mathcal{L}'$ to $\mathcal{L}$, so this is what the third condition ensures.

The condition that $|\mu_{i,j}| \leq \frac{1}{2}$ for all $1 \leq j < i$ is sometimes called *size reduction*. This property is not explicitly stated in recursive formulations but may be inferred from the third condition: for every $1 \leq j < i$ we consider the jth recursive lattice and see that the definition requires

$$\frac{1}{2} \geq \left| \frac{\langle \boldsymbol{b}_i^{(j-1)}, \boldsymbol{b}_j^* \rangle}{\|\boldsymbol{b}_j^*\|^2} \right| = \left| \frac{\langle \boldsymbol{b}_i - \sum_{k=1}^{j-1} \mu_{i,k} \boldsymbol{b}_k^*, \boldsymbol{b}_j^* \rangle}{\|\boldsymbol{b}_j^*\|^2} \right| = \left| \frac{\langle \boldsymbol{b}_i, \boldsymbol{b}_j^* \rangle}{\|\boldsymbol{b}_j^*\|^2} \right| = |\mu_{i,j}|,$$

using that $\langle \boldsymbol{b}_k^*, \boldsymbol{b}_j^* \rangle = 0$ for $k \neq j$.

It is simple to transform any basis into a size reduced one by using the same technique that was used in Lagrange's algorithm, i.e., adding a suitable multiple of one vector to another. For example, if $|\mu_{i,j}| > \frac{1}{2}$, then we replace $\boldsymbol{b}_i$ with $\boldsymbol{b}_i - \lfloor \mu_{i,j} \rceil \boldsymbol{b}_j$; the new value of $\mu_{i,j}$ will then be $\mu_{i,j} - \lfloor \mu_{i,j} \rceil \in [-\frac{1}{2}, \frac{1}{2}]$. Since this is such a straightforward method of reduction it will continue to be used in the following reductions we will see.

6 Hermite Reduction

Hermite was apparently the first person to consider reduction in arbitrary dimension when in 1845 he described a general reduction in a letter to Jacobi (as noted in [3]). The first basis vector satisfies $\|\boldsymbol{b}_1\| \leq \left(\frac{4}{3}\right)^{(d-1)/4} \operatorname{vol}(\mathcal{L})^{1/d}$ but otherwise the reduction lacks desirable properties like a bound on the orthogonality defect. However, in a second letter Hermite proposed a different reduction which bounds the orthogonality defect by $\left(\frac{4}{3}\right)^{d(d-1)/4}$. We give his second reduction here.

Definition. *A basis $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_d$ of $\mathcal{L}$ is Hermite reduced if*

- $\|\boldsymbol{b}_1\| \leq \|\boldsymbol{b}_i\|$ *for all* i
- $\boldsymbol{b}'_2, \ldots, \boldsymbol{b}'_d$ *is a Hermite reduced basis of* $\mathcal{L}'$
- $\boldsymbol{b}_2, \ldots, \boldsymbol{b}_d$ *are lifted from* $\mathcal{L}'$ *minimally:* $|\mu_{i,1}| \leq \frac{1}{2}$ *for* $2 \leq i \leq d$

Before showing the orthogonality defect is bounded we show the following helpful lemma.

Lemma. *If $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_d$ is a Hermite reduced basis then*

$$\|\boldsymbol{b}_i\|^2 \leq \tfrac{4}{3} \|\boldsymbol{b}_i'\|^2 .$$

Proof. In the following we use the inequalities $\mu_{i,1}^2 \leq \frac{1}{4}$ and $\|\boldsymbol{b}_1\| \leq \|\boldsymbol{b}_i\|$, as well as the fact that $\boldsymbol{b}_1$ and $\boldsymbol{b}_i'$ are orthogonal.

$$\begin{aligned}
\boldsymbol{b}_i &= \boldsymbol{b}_i' + \mu_{i,1}\boldsymbol{b}_1 \\
\|\boldsymbol{b}_i\|^2 &= \|\boldsymbol{b}_i'\|^2 + \mu_{i,1}^2 \|\boldsymbol{b}_1\|^2 \\
\|\boldsymbol{b}_i\|^2 &\leq \|\boldsymbol{b}_i'\|^2 + \tfrac{1}{4} \|\boldsymbol{b}_i\|^2 \\
\tfrac{3}{4} \|\boldsymbol{b}_i\|^2 &\leq \|\boldsymbol{b}_i'\|^2 \\
\|\boldsymbol{b}_i\|^2 &\leq \tfrac{4}{3} \|\boldsymbol{b}_i'\|^2
\end{aligned}$$

□

Applying this lemma recursively yields

$$\|\boldsymbol{b}_i\|^2 \leq \tfrac{4}{3} \|\boldsymbol{b}_i'\|^2 \leq \left(\tfrac{4}{3}\right)^2 \|\boldsymbol{b}_i^{(2)}\|^2 \leq \left(\tfrac{4}{3}\right)^3 \|\boldsymbol{b}_i^{(3)}\|^2 \leq \cdots \leq \left(\tfrac{4}{3}\right)^{i-1} \|\boldsymbol{b}_i^*\|^2 ,$$

and it follows

$$\prod_{i=1}^{d} \|\boldsymbol{b}_i\|^2 \leq \prod_{i=1}^{d} \left(\tfrac{4}{3}\right)^{i-1} \|\boldsymbol{b}_i^*\|^2 = \left(\tfrac{4}{3}\right)^{\sum_{i=0}^{d-1} i} \operatorname{vol}(\mathcal{L})^2 = \left(\tfrac{4}{3}\right)^{d(d-1)/2} \operatorname{vol}(\mathcal{L})^2,$$

where $\prod_{i=1}^{d} \|\boldsymbol{b}_i^*\| = \operatorname{vol}(\mathcal{L})$ because the Gram-Schmidt change-of-basis matrix has determinant 1 and the $\boldsymbol{b}_i^*$ are orthogonal. Taking the square root yields the promised orthogonality defect bound

$$\prod_{i=1}^{d} \|\boldsymbol{b}_i\| \leq \left(\tfrac{4}{3}\right)^{d(d-1)/4} \operatorname{vol}(\mathcal{L}).$$

Also, from $\|\boldsymbol{b}_1\| \leq \|\boldsymbol{b}_i\|$ we have $\|\boldsymbol{b}_1\|^d \leq \prod_{i=1}^{d} \|\boldsymbol{b}_i\|$, so taking the dth root yields

$$\|\boldsymbol{b}_1\| \leq \left(\tfrac{4}{3}\right)^{(d-1)/4} \operatorname{vol}(\mathcal{L})^{1/d},$$

which is actually the same bound satisfied by the reduction in Hermite's first letter.

It is unknown if Hermite's basis reduction can be computed in polynomial time in d or not.

7 Optimal-LLL Reduction

The lack of a provable polynomial time algorithm for Hermite basis reduction suggests we should weaken the reduction conditions even farther, and indeed the optimal-LLL reduction is a natural weakening of Hermite's reduction.

Definition. *A basis $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_d$ of $\mathcal{L}$ is optimal-LLL reduced if*

- $\|\boldsymbol{b}_1\| \leq \|\boldsymbol{b}_2\|$
- $\boldsymbol{b}'_2, \ldots, \boldsymbol{b}'_d$ *is a optimal-LLL reduced basis of* $\mathcal{L}'$
- $\boldsymbol{b}_2, \ldots, \boldsymbol{b}_d$ *are lifted from* $\mathcal{L}'$ *minimally:* $|\mu_{i,1}| \leq \frac{1}{2}$ *for* $2 \leq i \leq d$

As usual, we would like to be able to find a bound for the orthogonality defect for optimal-LLL reduced bases. The lemma $\|\boldsymbol{b}_i\|^2 \leq \frac{4}{3}\|\boldsymbol{b}'_i\|^2$ which was used in the Hermite case no longer holds, but as it turns out we can still show exactly the same orthogonality defect bound! To start off we use a different lemma.

Lemma. *If $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_d$ is an optimal-LLL reduced basis then*

$$\|\boldsymbol{b}_i^*\|^2 \leq \tfrac{4}{3}\|\boldsymbol{b}_{i+1}^*\|^2 .$$

Proof. Using condition 1 recursively, we get

$$\begin{aligned}
\|\boldsymbol{b}_i^*\| &\leq \|\boldsymbol{b}_{i+1}^{(i-1)}\| \\
&= \|\boldsymbol{b}_{i+1}^* + \mu_{i+1,i}\boldsymbol{b}_i^*\| \\
\|\boldsymbol{b}_i^*\|^2 &\leq \|\boldsymbol{b}_{i+1}^*\|^2 + \mu_{i+1,i}^2\|\boldsymbol{b}_i^*\|^2 \\
\|\boldsymbol{b}_i^*\|^2 &\leq \|\boldsymbol{b}_{i+1}^*\|^2 + \tfrac{1}{4}\|\boldsymbol{b}_i^*\|^2 \\
\tfrac{3}{4}\|\boldsymbol{b}_i^*\|^2 &\leq \|\boldsymbol{b}_{i+1}^*\|^2 \\
\|\boldsymbol{b}_i^*\|^2 &\leq \tfrac{4}{3}\|\boldsymbol{b}_{i+1}^*\|^2
\end{aligned}$$

□

From $\boldsymbol{b}_i = \boldsymbol{b}_i^* + \sum_{j=1}^{i-1} \mu_{i,j} \boldsymbol{b}_j^*$ and the orthogonality of the $\boldsymbol{b}_j^*$ we have:

$$\begin{aligned}
\|\boldsymbol{b}_i\|^2 &= \|\boldsymbol{b}_i^*\|^2 + \sum_{j=1}^{i-1} \mu_{i,j}^2 \|\boldsymbol{b}_j^*\|^2 \\
&\leq \|\boldsymbol{b}_i^*\|^2 + \sum_{j=1}^{i-1} \tfrac{1}{4} \left(\tfrac{4}{3}\right)^{i-j} \|\boldsymbol{b}_i^*\|^2 \\
&= \|\boldsymbol{b}_i^*\|^2 + \|\boldsymbol{b}_i^*\|^2 \sum_{j=1}^{i-1} \tfrac{1}{4} \left(\tfrac{4}{3}\right)^{j} \\
&= \|\boldsymbol{b}_i^*\|^2 \left(1 + \left(\tfrac{4}{3}\right)^{i-1} - 1\right) \\
&= \left(\tfrac{4}{3}\right)^{i-1} \|\boldsymbol{b}_i^*\|^2
\end{aligned}$$

And $\prod_{i=1}^{d} \|\boldsymbol{b}_i\| \leq \left(\frac{4}{3}\right)^{d(d-1)/4} \mathrm{vol}(\mathcal{L})$ follows, as in the Hermite case. Also, repeatedly using the lemma yields

$$\|\boldsymbol{b}_1\|^2 \leq \|\boldsymbol{b}_1^*\|^2 \leq \tfrac{4}{3} \|\boldsymbol{b}_2^*\|^2 \leq \left(\tfrac{4}{3}\right)^2 \|\boldsymbol{b}_3^*\|^2 \leq \cdots \leq \left(\tfrac{4}{3}\right)^{d-1} \|\boldsymbol{b}_d^*\|^2$$

so $\prod_{i=1}^{d} \|\boldsymbol{b}_1\|^2 \leq \prod_{i=1}^{d} \left(\frac{4}{3}\right)^{i-1} \|\boldsymbol{b}_i^*\|^2 = \left(\frac{4}{3}\right)^{d(d-1)/2} \mathrm{vol}(\mathcal{L})^2$ and like in the Hermite case we still have the bound $\|\boldsymbol{b}_1\| \leq \left(\frac{4}{3}\right)^{(d-1)/4} \mathrm{vol}(\mathcal{L})^{1/d}$.

Also like in the Hermite case, it is unknown if optimal-LLL basis reduction can be computed in polynomial time in d or not.

8 LLL Reduction

Finally we are ready to introduce the LLL basis reduction, as a slight relaxation of the optimal-LLL reduction just discussed. Now we allow a little slack room for $\boldsymbol{b}_2$ to be smaller than $\boldsymbol{b}_1$; the exact amount of slack can be controlled with a quality parameter $c \in (1, 4)$. The closer c is to 1, the better the reduction will be (and the longer it will take). A choice of $c = 1$ corresponds to the optimal-LLL reduction. The original paper by Lenstra, Lenstra and Lovász [2] effectively uses $c = \frac{4}{3}$.

Definition. *A basis $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_d$ of $\mathcal{L}$ is LLL reduced with quality parameter $c \in (1, 4)$ if*

- $\|\boldsymbol{b}_1\| \leq \sqrt{c}\,\|\boldsymbol{b}_2\|$
- $\boldsymbol{b}'_2, \ldots, \boldsymbol{b}'_d$ *is an LLL reduced basis (with quality parameter c) of $\mathcal{L}'$*
- $\boldsymbol{b}_2, \ldots, \boldsymbol{b}_d$ *are lifted from $\mathcal{L}'$ minimally: $|\mu_{i,1}| \leq \frac{1}{2}$ for $2 \leq i \leq d$*

To find a bound on the orthogonality defect we proceed much like before, except that in this case the results aren't quite as nice. Define $C = \frac{4c}{4-c}$ and note that $C > \frac{4}{3}$ for $c > 1$. Roughly speaking, $\frac{4}{3}$ in our previous results will be replaced by C in the LLL-specific results.

Lemma. *If $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_d$ is an LLL reduced basis then*

$$\|\boldsymbol{b}_i^*\|^2 \leq C\,\|\boldsymbol{b}_{i+1}^*\|^2 .$$

Proof. Using condition 1 recursively, we get

$$\begin{aligned}
\|\boldsymbol{b}_i^*\| &\leq \sqrt{c}\,\|\boldsymbol{b}_{i+1}^{(i-1)}\| \\
&= \sqrt{c}\,\|\boldsymbol{b}_{i+1}^* + \mu_{i+1,i}\boldsymbol{b}_i^*\| \\
\|\boldsymbol{b}_i^*\|^2 &\leq c\,\|\boldsymbol{b}_{i+1}^*\|^2 + c\mu_{i+1,i}^2\,\|\boldsymbol{b}_i^*\|^2 \\
\|\boldsymbol{b}_i^*\|^2 &\leq c\,\|\boldsymbol{b}_{i+1}^*\|^2 + c\tfrac{1}{4}\,\|\boldsymbol{b}_i^*\|^2 \\
\tfrac{4-c}{4}\,\|\boldsymbol{b}_i^*\|^2 &\leq c\,\|\boldsymbol{b}_{i+1}^*\|^2 \\
\|\boldsymbol{b}_i^*\|^2 &\leq \tfrac{4c}{4-c}\,\|\boldsymbol{b}_{i+1}^*\|^2
\end{aligned}$$

□

From $\boldsymbol{b}_i = \boldsymbol{b}_i^* + \sum_{j=1}^{i-1} \mu_{i,j} \boldsymbol{b}_j^*$ and the orthogonality of the $\boldsymbol{b}_j^*$ we have:

$$\begin{aligned}
\|\boldsymbol{b}_i\|^2 &= \|\boldsymbol{b}_i^*\|^2 + \sum_{j=1}^{i-1} \mu_{i,j}^2 \|\boldsymbol{b}_j^*\|^2 \\
&\leq \|\boldsymbol{b}_i^*\|^2 + \sum_{j=1}^{i-1} \tfrac{1}{4} C^{i-j} \|\boldsymbol{b}_i^*\|^2 \\
&= \|\boldsymbol{b}_i^*\|^2 + \|\boldsymbol{b}_i^*\|^2 \sum_{j=1}^{i-1} \tfrac{1}{4} C^j \\
&= \|\boldsymbol{b}_i^*\|^2 \left(\tfrac{c}{5c-4}\left(C^{i-1} - 1\right) + 1\right) \\
&\leq C^{i-1} \|\boldsymbol{b}_i^*\|^2
\end{aligned}$$

since $\frac{c}{5c-4} < 1$. It follows

$$\prod_{i=1}^{d} \|\boldsymbol{b}_i\|^2 \leq \prod_{i=1}^{d} C^{i-1} \|\boldsymbol{b}_i^*\|^2 = C^{d(d-1)/2} \operatorname{vol}(\mathcal{L})^2$$

$$\prod_{i=1}^{d} \|\boldsymbol{b}_i\| \leq C^{d(d-1)/4} \operatorname{vol}(\mathcal{L})$$

Similarly, repeatedly using the lemma yields

$$\|\boldsymbol{b}_1\|^2 \leq C^{i-1} \|\boldsymbol{b}_i^*\|^2 \tag{4}$$

$$\prod_{i=1}^{d} \|\boldsymbol{b}_1\|^2 \leq \prod_{i=1}^{d} C^{i-1} \|\boldsymbol{b}_i^*\|^2 = C^{d(d-1)/2} \operatorname{vol}(\mathcal{L})^2$$

$$\|\boldsymbol{b}_1\| \leq C^{(d-1)/4} \operatorname{vol}(\mathcal{L})^{1/d}$$

Also, if $\boldsymbol{x} = \sum_{i=1}^{k} r_i \boldsymbol{b}_i$ is the shortest nonzero vector in $\mathcal{L}$, with $r_i \in \mathbb{Z}$

and $r_k \neq 0$, we use the Gram-Schmidt change-of-basis to write, for some s_i,

$$\begin{aligned}
\boldsymbol{x} &= r_k \boldsymbol{b}_k^* + \sum_{i=1}^{k-1} s_i \boldsymbol{b}_i^* \\
\|\boldsymbol{x}\|^2 &= r_k^2 \|\boldsymbol{b}_k^*\|^2 + \sum_{i=1}^{k-1} s_i^2 \|\boldsymbol{b}_i^*\|^2 \\
&\geq \|\boldsymbol{b}_k^*\|^2 \qquad \text{since } r_k^2 \geq 1 \\
C^{k-1} \|\boldsymbol{x}\|^2 &\geq C^{k-1} \|\boldsymbol{b}_k^*\|^2 \\
&\geq \|\boldsymbol{b}_1\|^2 \qquad \text{by (4)}
\end{aligned}$$

So the first vector in an LLL-reduced basis contains an approximation to the shortest nonzero vector, off by a factor of at most C^{d-1}.

Now perhaps the most important fact in this report is this: The 'obvious' algorithm for computing an LLL reduced basis runs in polynomial time in the lattice dimension d. We note the algorithm suggested by the definition:

Algorithm 2 LLLReduce, the recursive version

Input: A basis $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_d$ of a lattice $\mathcal{L}$
Output: An LLL reduced basis (with quality parameter c) of $\mathcal{L}$

1: **if** $d = 1$ **then return** $(\boldsymbol{b}_1)$
2: **repeat**
3: **if** $\|\boldsymbol{b}_1\| > \sqrt{c}\,\|\boldsymbol{b}_2\|$ **then** swap $\boldsymbol{b}_1$ and $\boldsymbol{b}_2$
4: $(\boldsymbol{b}_2, \ldots, \boldsymbol{b}_d) := \text{lift}_{\boldsymbol{b}_1}(\text{LLLReduce}(\boldsymbol{b}'_2, \ldots, \boldsymbol{b}'_d))$
5: **until** $\|\boldsymbol{b}_1\| \leq \sqrt{c}\,\|\boldsymbol{b}_2\|$
6: **return** $(\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_d)$

Where the lift function returns $\boldsymbol{b}_i$ which satisfy the third condition $|\mu_{i,1}| \leq \frac{1}{2}$ for $2 \leq i \leq d$. In practice to avoid recursion overhead LLL should be implemented iteratively, as usually presented.

Finally, we show that the total number of swaps (including those in recursive calls) needed until an LLL reduced basis is found is polynomial in d.

As noted before, $\prod_{i=1}^{d} \|\boldsymbol{b}_i^*\| = \text{vol}(\mathcal{L})$ and therefore is constant throughout the algorithm. Also the volume of the lattice projected orthogonally to $\boldsymbol{b}_1$ and $\boldsymbol{b}_2$ does not change when $\boldsymbol{b}_1$ and $\boldsymbol{b}_2$ are swapped. But the volume of the

lattice projected orthogonally to $\boldsymbol{b}_1$ may change when $\boldsymbol{b}_1$ and $\boldsymbol{b}_2$ are swapped. So if we define

$$d_k = \prod_{i=1}^{k} \|\boldsymbol{b}_i^*\|^2 = \frac{\mathrm{vol}(\mathcal{L})^2}{\mathrm{vol}(\mathcal{L}^{(k)})^2}$$

then the only time d_k may change is when we perform a swap at a recursive depth of k. In fact, if we do perform a swap it is because

$$\|\boldsymbol{b}_k^*\|^2 > c\,\|\boldsymbol{b}_{k+1}^{(k-1)}\|^2,$$

so by replacing $\boldsymbol{b}_k^{(k-1)}$ with $\boldsymbol{b}_{k+1}^{(k-1)}$ we have $d_k > c d_k^{\mathrm{new}}$, i.e., we decrease d_k by a factor of c.

Now define $D = \prod_{i=1}^{d} d_i$. Any swap we perform at a recursion depth of k decreases d_k by a factor of c and does not change the other d_i, so every time a swap is performed D decreases by a factor of c. Further, $D \in \mathbb{Z}^+$ because $d_i \in \mathbb{Z}$ as $\mathrm{vol}(\mathcal{L}) \in \mathbb{Z}^+$ and $\mathrm{vol}(\mathcal{L}^{(i)})^2 \mid \mathrm{vol}(\mathcal{L})^2$. Therefore the total number of swaps the algorithm can perform is at most $\log_c(D) = O(d^2 \log(\max \|\boldsymbol{b}_i\|))$, since

$$D = \prod_{i=1}^{d} \|\boldsymbol{b}_i^*\|^{2(d-i+1)} \leq \prod_{i=1}^{d} \|\boldsymbol{b}_i\|^{2(d-i+1)} \leq \max \|\boldsymbol{b}_i\|^{d(d+1)}.$$

However, to prove a polynomial bit complexity it is still necessary to bound the size of the rational numbers used during the algorithm as done in [2].

References

[1] Miklós Ajtai. SVP in L_2 is NP-hard. *STOC '98*, 1998.

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

[3] P. Nguyen and D. Stehlé. An LLL algorithm with quadratic complexity. *To appear in SIAM Journal on Computing*, 2009.

[4] P. Nguyen, D. Stehlé. Low-Dimensional Lattice Basis Reduction Revisited. *To appear in ACM Transactions on Algorithms*, 2009.

[5] H. Yao, G. W. Womell. Lattice-Reduction-Aided Detectors for MIMO Communication Systems. *Proceedings of IEEE Globecom 2002*, Taipei, Taiwan, November 2002.

[6] P. Van Em de Boas. Another NP-complete partition problem and the complexity of computing short vectors in lattice. *Tech. Report 81-04*, Department of Mathematics, University of Amsterdam, 1980.