Isodual Reduction of Lattices

Nicholas A. Howgrave-Graham
nhowgravegraham@ntru.com

NTRU Cryptosystems Inc., USA

Abstract

We define a new notion of a reduced lattice, based on a quantity introduced in the LLL paper. We show that lattices reduced in this sense are simultaneously reduced in both their primal and dual. We show that the definition applies naturally to blocks, and therefore gives a new hierarchy of polynomial time algorithms for lattice reduction with fixed blocksize. We compare this hierarchy of algorithms to previous ones. We then explore algorithms to provably minimize the associated mesaure, and also some more efficient heuristics. Finally we comment on the initial investigations of applying our technique to the NTRU family of lattices.

1 Introduction

Although not emphasized in the original LLL paper [14], one can view the LLL algorithm in the following way: given an input basis $\mathcal{B} = \{b_1, b_2, \ldots, b_n\}$ it monotonically reduces the quantity[1]

$$\Psi(b_1, \ldots, b_n) \quad = \quad \prod_{i=1}^{n} |b_i^*|^{n+1-i},$$

such that this quantity cannot be any further reduced (by a constant multiplicative factor of δ) by any consecutive two dimensional row operations.

Here we use the standard notation in that b_i^* are the orthogonal Gram-Schmidt vectors, satisfying $b_i^* = b_i - \sum_{j<i} \mu_{i,j} b_j^*$ where $\mu_{i,j} = \langle b_i, b_j^* \rangle / |b_i^*|^2$.

In subsequent generalizations of the LLL algorithm, the emphasis moved away from reducing the Ψ-measure, and instead concentrated on the following property of an LLL reduced basis: that in each of the two dimensional consecutive projected blocks the first vector has minimal length. Viewed this way, natural extensions of LLL were to use the Korkine-Zolotarev (KZ) notion of reduced lattices [11, 12] on larger blocks [18, 19], or to try a Rankin-type strategy of minimizing half-determinants of larger blocks [18, 5].

We go back to examining the Ψ-measure, and study its properties. Firstly we show that if a basis achieves the minimal Ψ-measure of a lattice then the dual basis achieves the minimal Ψ-measure of the dual of that lattice, and moreover if there is any operation that reduces it in the primal, then there is a corresponding operation that reduces it in the dual.

This builds on the work in [8, 9], where it was shown that if a lattice is LLL-reduced, then its dual is effectively LLL reduced, i.e. no consecutive swaps can reduce the LLL measure in either the primal or the dual.

Definition 1. *A basis $\{b_1, \ldots b_n\}$ of a lattice $\mathcal{L}$ is called Ψ-reduced if in achieves the minimal Ψ-measure over all bases of $\mathcal{L}$. We denote this minimal measure by Ψ_{min}.*

As shown above, we go one step further and call a lattice basis Ψ-reduced if it actually minimizes this measure, and we define a partial ordering on lattice bases with respect to this measure, i.e.

$$\mathcal{B} < \mathcal{C} \quad \text{if} \quad \Psi(\mathcal{B}) < \Psi(\mathcal{C}).$$

[1] This quanity was central to the proof of polynomial-time termination of the algorithm in [14], but not discussed in depth elsewhere.

This is in contrast to the natural ordering on lattices implied by KZ notion and its block extensions, which is based on a lexicographic ordering on the $|b_i^*|$, i.e.

$$\mathcal{B} < \mathcal{C} \quad \text{if} \quad (|b_1|, |b_2^*|, \ldots, |b_{n-1}^*|) <_{\text{lex}} (|c_1^*|, |c_2^*|, \ldots, |c_{n-1}^*|).$$

Neither definition is satisfied by just one basis, e.g. neither say how one should order the identity basis. However the notions of reduction differ even in dimension 3, in that the first vector need not be a smallest vector in a Ψ-reduced lattice. For example the Ψ-measure is minimized by the basis given by the rows of the following matrix whenever $Y > X > 1$ and $XY < 2/\sqrt{3}$. However in this case a KZ-reduced basis would order the $(0, 0, 1)$ vector first.

$$\begin{pmatrix} X & 0 & 0 \\ \frac{X}{2} & \frac{\sqrt{3}Y}{2} & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{1}$$

At this point it is worth justifying why the Ψ-measure is interesting, since we have seen that it does not necessarily make the shortest vector go first, and therefore solve the shortest vector problem (SVP).

Firstly one can justify it because it is an isodual measure - if one had placed the shortest vector first in the example basis 1 then the primal would have been better reduced that the dual with respect to the KZ notion. In many situations one does not wish to have this discrepancy between primal and dual, e.g. the NTRU class of lattices are naturally symplectic [6], and therefore an isodual reduction strategy is a natural one to choose. See [16, 13] for more motivation on isodual lattice reduction: Seysen and LaMacchia also show several ideas for isodual reduction of lattices, but their techniques do not have the provable properties of an LLL-based approach.

However even if one is interested in solving approximate-SVP (appr-SVP) we show that blockwise reducing the Ψ-measure is sometimes preferable in practice to a KZ-based approach, i.e. a greedy strategy of KZ-reducing each block is non-optimal.

We introduce new constants η_i akin to Hermite's family of constants γ_i but with respect to the Ψ-measure rather than the lexicographic ordering. We show that they begin $\eta_2 = \sqrt{4/3}, \eta_3 = 3/2, \ldots$. We leave for further work the determination of the other constants η_n for $n \geq 4$, and an asymptotic bound on their size. The Ψ-measure effectively introduces a whole new field of "sphere packing" (see [3]) with respect to this new measure.

To show the practical ramifications of our results, we apply our results to the NTRU family of lattices.

2 Mathematics and notation

We take a row-oriented view of matrices and allow some flexibity between basis representations and matrix representations, e.g. we call a *matrix* LLL-reduced (resp. Ψ-reduced) if the *rows* of the matrix form an LLL-reduced (resp. Ψ-reduced) *basis*.

For a thorough grounding on lattices see [2, 3], however for our purposes the following will suffice: for a given basis $\mathcal{B} = \{b_1, \ldots, b_n\}$ of $\mathbb{R}^n$ a lattice is defined to be the set of points

$$\mathcal{L} \quad = \quad \left\{ y \in \mathbb{R}^n \;\middle|\; y = \sum_{i=1}^{n} a_i b_i,\ a_i \in \mathbb{Z} \right\}$$

Clearly many bases will generate the same set of lattice points; indeed if we represent a basis $\mathcal{B}$ by a matrix B with rows $\{b_1, \ldots, b_n\}$ then it is exactly the rows of UB for any $U \in GL_n(\mathbb{Z})$ that generate these points.

However it is often convenient to give ourselves even more freedom with matrix representations of lattices in that one can consider bases of isomorphic lattices too.

Definition 2. *Two lattices $\mathcal{L}, \mathcal{L}'$ are called isomorphic if there is a length-preserving bijection $\phi : \mathcal{L} \to \mathcal{L}'$ satisfying $\phi(x + y) = \phi(x) + \phi(y)$.*

In terms of matrix representations this means that if the rows of B form a basis for a lattice $\mathcal{L}$ then the rows of $B' = UBN$ where $U \in GL_n(\mathbb{Z})$ and N is orthonormal, form a basis for an isomorphic lattice $\mathcal{L}'$, even though the rows of B' do not necessarily generate the same *points* of $\mathcal{L}$.

The point of allowing the extra freedom of post-multiplying by an orthonormal matrix is that if (for some reason) one can find an integer vector u such that uB' is small, then $uU^{-1}B$ is also small, i.e. solving lattice problems in an isomorphic lattice can help solve them in the original lattice. It is worth noting that this freedom also allows one to always consider lower triangular lattice bases by forming N from the Gram-Schmidt procedure[2].

Definition 3. *If B_1, B_2 are bases of two isomorphic lattices $\mathcal{L}_1, \mathcal{L}_2$ respectively, and $N = B_1 B_2^{-1}$ is orthornormal (i.e. in the case $U = 1$), then we call the two bases* rotations *of each other.*

Definition 4. *If B_1, B_2 are two bases of a lattice $\mathcal{L}$, and $U = B_1 B_2^{-1}$ is a lower triangular unimodular matrix then we call the two bases* order equivalent.

It is clear that both of the above notions are equivalence relations on the set of matrices. The *order equivalent* notion is close to the notion of an *effectively* LLL-reduced basis given in [8, 9] in that a basis is effectively LLL-reduced lattice if and only if it is order equivalent to a LLL-reduced lattice.

As with the analysis in [14] we use a constant δ to cope with precision errors and to provide proofs of polynomial-time completion. We assume $1/4 < \delta < 1$ but usually think of δ as very close to 1.

2.1 The properties of Ψ-reduced bases

The Gram-Schmidt vectors b_i^* are invariant under rotations, and multiplication by a lower triangular unimodular matrix, so we have the following trivial lemmas.

Lemma 1. *If $B' = BN$ for some orthonormal matrix N, i.e. B' is a rotation of B, then $\Psi(B) = \Psi(B')$.*

Lemma 2. *If $B' = UB$ for some lower triangular matrix $U \in GL_n(\mathbb{Z})$, then $\Psi(B) = \Psi(B')$.*

Lemma 3. *If $\mathcal{B} = \{b_1, \ldots, b_n\}$ and $\mathcal{B}' = \{b'_1, \ldots, b'_n\}$ are such that $b'_i = b_i$ for all $i \neq j$, and $b'_j = \alpha b_j$ then $\Psi(B') = \alpha^{n+1-j}\Psi(B)$.*

The dual (or polar) lattice, as given in [2], is defined as the following:

Definition 5 (classical)**.** *If $\{b_1, \ldots, b_n\}$ is a basis for a lattice $\mathcal{L}$, then there do exist vectors $\{d_1, \ldots, d_n\}$ such that*

$$d_j \cdot b_i = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}$$

The lattice which is spanned by $\{d_1, \ldots, d_n\}$ is called the dual *lattice of $\mathcal{L}$.*

The following definition of a dual basis will suit our needs better (it fits in better with the present analysis, and the analysis in [6]), and it is clear that the notions of dual lattice and modified-dual lattice are isomorphic.

Definition 6 (modified)**.** *If $\{b_1, \ldots, b_n\}$ is a basis for a lattice $\mathcal{L}$ and b_i has coefficients $(b_i)_1, \ldots (b_i)_n$, then there do exist vectors $\{d_1, \ldots, d_n\}$ such that*

$$\sum_{j=1}^{n} (d_j)_i (b_{n+1-j})_i = \begin{cases} 1 & \text{if } i = n+1-j, \\ 0 & \text{otherwise,} \end{cases}$$

for $1 \leq i \leq n$. The lattice which is spanned by $\{d_1, \ldots, d_n\}$ is called the modified-dual lattice *of $\mathcal{L}$.*

[2]It is worth saying that mathematicians do not always apply this transformation because some non-lower triangular lattice bases naturally have integer entries (as opposed to general real entries), and putting a lattice in lower triangular form can force the use of square roots of rational numbers (or real approximations) in this case.

In terms of matrices, if the rows of B form a basis for a lattice $\mathcal{L}$, then the rows of $D = J(B^{-1})^t J$ form a basis (the *modified-dual basis*) for the modified-dual lattice of $\mathcal{L}$, where J is the n-dimensional identity matrix with its rows reversed (i.e. ones on the anti-diagonal).

Example 1. *To be explicit, we show below a generic lower triangular 4 dimensional primal basis, and its modified-dual basis. If*

$$B = \begin{pmatrix} |b_1| & 0 & 0 & 0 \\ \mu_{2,1}|b_1| & |b_2^*| & 0 & 0 \\ \mu_{3,1}|b_1| & \mu_{3,2}|b_2^*| & |b_3^*| & 0 \\ \mu_{4,1}|b_1| & \mu_{4,2}|b_2^*| & \mu_{4,3}|b_3^*| & |b_4^*| \end{pmatrix}$$

then

$$D = J(B^{-1})^t J = \begin{pmatrix} |b_4^*|^{-1} & 0 & 0 & 0 \\ -\mu_{4,3}|b_4^*|^{-1} & |b_3^*|^{-1} & 0 & 0 \\ (\mu_{3,2}\mu_{4,3} - \mu_{4,2})|b_4^*|^{-1} & -\mu_{3,2}|b_3^*|^{-1} & |b_2^*|^{-1} & 0 \\ \mu'_{4,1}|b_4^*|^{-1} & (\mu_{2,1}\mu_{3,2} - \mu_{3,1})|b_3^*|^{-1} & -\mu_{2,1}|b_2^*|^{-1} & |b_1|^{-1} \end{pmatrix},$$

where $\mu'_{4,1} = \mu_{3,1}\mu_{4,3} + \mu_{2,1}(\mu_{4,2} - \mu_{3,2}\mu_{4,3}) - \mu_{4,1}$.

Lemma 4. *Let B be a basis of a lattice $\mathcal{L}$ of determinant Δ, then*

$$\Psi(B) \quad = \quad \Delta^{n+1}\Psi(JB^{-t}J).$$

Proof. We have that

$$\begin{aligned} \frac{\Psi^2(B)}{\Delta^{n+1}} &= \frac{1}{\Delta^{n+1}} \prod_{i=1}^{n} |b_i^*|^{2(n+1-i)} \\ &= \prod_{i \le n/2} \left(\frac{|b_i^*|}{|b_{n+1-i}^*|} \right)^{n+1-2i} \qquad (2) \\ &= \prod_{i \le n/2} \left(\frac{|d_i^*|}{|d_{n+1-i}^*|} \right)^{n+1-2i} \qquad (3) \\ &= \frac{\Psi^2(JB^{-t}J)}{\Delta^{-(n+1)}} \end{aligned}$$

where equation 3 follows since the modified-dual basis satisfies $|d_i^*| = 1/|b_{n+1-i}^*|$. □

Corollary 1. *If the Ψ-measure is minimized in the primal lattice then it is simultaneously minimized in the dual lattice.*

Corollary 2. *If a unitary transformation U is such that $\Psi(UB) < \Psi(B)$ then the transformation $U' = JU^{-t}J$ is such that $\Psi(U'JB^{-t}J) = \Psi(J(UB)^{-t}J) < \Psi(JB^{-t}J)$, i.e. if U decreases the Ψ-measure in the primal basis B then U' decreases the Ψ-measure in the modified-dual basis $D = JB^{-t}J$.*

The following lemmas give a concise justification for the "swap" formulae used in [14], and generalize the result to 3 dimensions. .

Lemma 5.

$$\Psi^2 \begin{pmatrix} x_{1,1} & x_{1,2} \\ x_{2,1} & 0 \end{pmatrix} \quad = \quad \left(x_{1,1}^2 + x_{1,2}^2\right) \left(x_{1,2}x_{2,1}\right)^2$$

Proof. Just as in the analysis in [14] after a "swap", we may re-triangularize the basis by multiplying on the right by an orthonormal matrix[3]

$$\begin{pmatrix} x_{1,1} & x_{1,2} \\ x_{2,1} & 0 \end{pmatrix} \begin{pmatrix} \frac{x_{1,1}}{\sqrt{x_{1,1}^2+x_{1,2}^2}} & \frac{x_{1,2}}{\sqrt{x_{1,1}^2+x_{1,2}^2}} \\ \frac{x_{1,2}}{\sqrt{x_{1,1}^2+x_{1,2}^2}} & \frac{-x_{1,1}}{\sqrt{x_{1,1}^2+x_{1,2}^2}} \end{pmatrix} = \begin{pmatrix} \sqrt{x_{1,1}^2 + x_{1,2}^2} & 0 \\ \frac{x_{1,1}x_{2,1}}{\sqrt{x_{1,1}^2+x_{1,2}^2}} & \frac{x_{1,2}x_{2,1}}{\sqrt{x_{1,1}^2+x_{1,2}^2}} \end{pmatrix},$$

[3]This tranformation can also be used to justify the update formuale for the $\mu_{i,j}$ and $\mu_{i+1,j}$ for $j > i+1$, but we omit the details.

without changing the Ψ-measure, from which the result is obvious. □

Lemma 6.

$$\begin{aligned}\Psi^2\begin{pmatrix}x_{1,1} & x_{1,2} & x_{1,3}\\ x_{2,1} & x_{2,2} & 0\end{pmatrix} &= \left(x_{1,1}^2+x_{1,2}^2+x_{1,3}^2\right)\left(\left(x_{1,1}x_{2,2}-x_{1,2}x_{2,1}\right)^2+x_{1,3}^2\left(x_{2,1}^2+x_{2,2}^2\right)\right)\\ &= \left(s^2+t^2+x_{1,3}^2\right)\left(t^2+x_{1,3}^2\right)\left(x_{2,1}^2+x_{2,2}^2\right)\\ &= \left(x_{2,1}^2+x_{2,2}^2\right)\Psi^2\begin{pmatrix}s & t & x_{1,3}\\ 1 & 0 & 0\end{pmatrix}\end{aligned}$$

for some orthonormal change of basis $(x_{2,1}, x_{2,2}) \to (s, t)$.

Proof. Let

$$N = \frac{1}{\sqrt{x_{2,1}^2+x_{2,2}^2}}\begin{pmatrix}x_{2,1} & x_{2,2} & 0\\ x_{2,2} & -x_{2,1} & 0\\ 0 & 0 & 1\end{pmatrix}$$

and let N' be the top left $(2)\times(2)$ orthonormal submatrix of N, then

$$\begin{aligned}\Psi^2\begin{pmatrix}x_{1,1} & x_{1,2} & x_{1,3}\\ x_{2,1} & x_{2,2} & 0\end{pmatrix} &= \Psi^2\left(\begin{pmatrix}x_{1,1} & x_{1,2} & x_{1,3}\\ x_{2,1} & x_{2,2} & 0\end{pmatrix}N\right)\\ &= \Psi^2\begin{pmatrix}\frac{x_{1,1}x_{2,1}+x_{1,2}x_{2,2}}{\sqrt{x_{2,1}^2+x_{2,2}^2}} & \frac{x_{1,1}x_{2,2}-x_{1,2}x_{2,1}}{\sqrt{x_{2,1}^2+x_{2,2}^2}} & x_{1,3}\\ \sqrt{x_{2,1}^2+x_{2,2}^2} & 0 & 0\end{pmatrix}\\ &= \Psi^2\begin{pmatrix}\frac{x_{1,1}x_{2,1}+x_{1,2}x_{2,2}}{\sqrt{x_{2,1}^2+x_{2,2}^2}} & \sqrt{\frac{\left(x_{1,1}x_{2,2}-x_{1,2}x_{2,1}\right)^2}{x_{2,1}^2+x_{2,2}^2}+x_{1,3}^2}\\ \sqrt{x_{2,1}^2+x_{2,2}^2} & 0\end{pmatrix}\\ &= \left(x_{1,1}^2+x_{1,2}^2+x_{1,3}^2\right)\left(\left(x_{1,1}x_{2,2}-x_{1,2}x_{2,1}\right)^2+x_{1,3}\left(x_{2,1}^2+x_{2,2}^2\right)\right)\\ &= \left(s^2+t^2+x_{1,3}^2\right)\left(t^2+x_{1,3}^2\right)\left(x_{2,1}^2+x_{2,2}^2\right) \qquad (4)\end{aligned}$$

where $(s, t) = (x_{1,2}, x_{2,2})N'$. □

Since lemma 6 shows that Ψ^2 is the product of convex functions, we have the following convexity result.

Corollary 3. *If*

$$\Psi^2\begin{pmatrix}x_{1,1} & x_{1,2} & x_{1,3}\\ x_{2,1} & x_{2,2} & 0\end{pmatrix} \le W, \text{ and } \Psi^2\begin{pmatrix}x'_{1,1} & x'_{1,2} & x_{1,3}\\ x_{2,1} & x_{2,2} & 0\end{pmatrix} \le W,$$

then line between $(x_{1,1}, x_{1,2})$ *and* $(x'_{1,1}, x'_{1,2})$ *is also so bounded, i.e. for any* $0 \le \alpha \le 1$

$$\Psi^2\begin{pmatrix}x_{1,1}+\alpha(x'_{1,1}-x_{1,1}) & x_{1,2}+\alpha(x'_{1,2}-x_{1,2}) & x_{1,3}\\ x_{2,1} & x_{2,2} & 0\end{pmatrix} \le W,$$

2.2 The constants η_n

Lemma 7. *For a lattice* $\mathcal{L}$ *of dimension* n *and discriminant* Δ*, let* $\Psi_{min}(\mathcal{L})$ *denote the minimal* Ψ*-measure taken over all bases* $\mathcal{B}$ *of* $\mathcal{L}$*, then*

$$\frac{\Psi_{min}^2(\mathcal{L})}{\Delta^{n+1}} \le \left(\frac{4}{3\delta}\right)^{n(n-1)(n+1)/12}$$

Proof. Let $\Delta_m = \prod_{i=1}^{m} |b_i^*|$. Any LLL-reduced basis of $\mathcal{L}$ has $|b_m^*| \geq (3\delta/4)^{(m-1)/4}\Delta_m^{1/m}$, and $|b_i^*| \geq (3\delta/4)^{(i-m)/2}|b_m^*|$ for $i > m$, from which we deduce

$$\begin{aligned}
\Delta &= \Delta_m \prod_{i=m+1}^{n} |b_i^*| \\
&\geq \Delta_m \left(\left(\frac{3\delta}{4}\right)^{(m-1)/4} \Delta_m^{1/m} \right)^{n-m} \left(\frac{3\delta}{4}\right)^{(n-m)(n-m+1)/4} \\
&= \Delta_m^{n/m} \left(\frac{3\delta}{4}\right)^{n(n-m)/4}
\end{aligned}$$

so

$$\Delta_m \leq \left(\frac{4}{3\delta}\right)^{m(n-m)/4} \Delta^{m/n}.$$

In which case

$$\begin{aligned}
\frac{\Psi^2}{\Delta^{n+1}} &= \frac{1}{\Delta^{n+1}} \left(\prod_{m=1}^{n} \Delta_m \right)^2 \\
&\leq \left(\prod_{m=1}^{n} \left(\frac{4}{3\delta}\right)^{m(n-m)/4} \right)^2 \\
&= \left(\frac{4}{3\delta}\right)^{n(n-1)(n+1)/12}
\end{aligned}$$

□

Lemma 7 shows that the quantity $\Psi_{\min}^2(\mathcal{L})/\Delta^{n+1}$ is upper bounded for every lattice $\mathcal{L}$, however some lattices may have a larger value of $\Psi_{\min}^2(\mathcal{L})/\Delta^{n+1}$ than others. We define the following constants over all n-dimensional lattices:

$$\eta_n = \max_{\mathcal{L}} \left\{ \frac{\Psi_{\min}^2(\mathcal{L})}{\Delta^{n+1}} \right\}.$$

These constants allow one to bound the Ψ-measure in terms of the determinant, e.g. in the two dimensional case we know that for every lattice $\mathcal{L}$ there exists a vector b_1 such that $|b_1|^2 \leq \eta_2\Delta$, and in the three dimensional case we know that for every lattice $\mathcal{L}$ there exists a pair of vectors b_1, b_2 such that $|b_1|^4|b_2^*|^2 \leq \eta_3\Delta^2$, etc.

This can be looked on as an alternative definition of the density of a lattice, as opposed to the traditional $|v_1|/\Delta^{1/n}$, which gives rise to Hermite's constants γ_n. In the two dimensional case we have $\eta_2 = \gamma_2 = \sqrt{4/3}$, but in $n > 2$ dimensions the two notions differ. We prove that $\eta_3 = 3/2$ below, but leave the determination of further constants, and their asymptotic analysis for further work.

Theorem 1. *With η_n defined as above, then $\eta_3 = 3/2$.*

Proof. We will show that if $|b_3^*|^2 = (2/3)|b_1|^2$ then there are just two values for $|b_2^*|^2$ such that the basis is Ψ-reduced bases, and if $|b_3^*| < \sqrt{2/3}|b_1|$, there are none. These critical lattices have $\Psi^2/\Delta^2 = |b_1|^2/|b_3^*|^2 = 3/2$, which will prove that $\eta_3 = 3/2$.

Suppose $|b_3^*|^2 = (2/3)|b_1|^2$, then for the basis to be LLL-reduced we must have that[4]

$$\frac{3}{4} \leq \frac{|b_2^*|^2}{|b_1|^2} \leq \frac{8}{9}, \quad |b_2| \geq |b_1|, \quad |\mu_{2,1}| \leq 1/2.$$

[4]Actually this region may be reduced for the proof if we use the fact that the Ψ-measure is isodual, since either a lattice or its dual will satisfy $|b_2^*| \leq (2/3)^{1/4}|b_1|$. We consider te full range in the proof to explicitly show the dual solution.

This area is shown in figure 1(a).

Without loss of generality we can assume the projection of b_3 on to the space generated by b_1, b_2 falls within the Delaunay cell around the origin, since there is always some linear combination of b_1, b_2 to make b_3 project in to the Delaunay cell around the origin (and such linear operations do not change the Ψ-measure).

Let $a = \mu_{2,1}|b_1|, b = |b_2^*|, x = \mu_{3,1}|b_1|, y = \mu_{3,2}|b_2^*|$, then in two-dimensions the vertices of the fundamental Delaunay cell[5] are given by:

$$\begin{array}{ccc} ((a+1)/3, b/3), & ((2-a)/3, -b/3), & ((1-2a)/3, -2b/3), \\ (-(a+1)/3, -b/3), & ((a-2)/3, b/3), & ((2a-1)/3, 2b/3). \end{array}$$

We will show that if $|b_3^*|^2 = (2/3)|b_1|^2$, and none[6] of the following 3 unimodular transformations[7] decreases the Ψ-measure, then there are only two possible Ψ-reduced lattices in the case that $\mu_{2,1} > 0$. We note the case $\mu_{2,1} < 0$ can be handled similarly by changing the second row of U_3 to $(1, 1, 0)$.

$$U_1 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, U_2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, U_3 = \begin{pmatrix} 0 & 0 & 1 \\ -1 & 1 & 0 \end{pmatrix}.$$

In figure 2 we plot the possible the possible projections of b_3 such that $\Psi^2(U_i B) = |b_1|^4 |b_2^*|^2$ for three basis with $|b_2^*|^2 = 2/3, 59/72, 8/9$ and fixing $|b_2| = 1$. It is scaled such that $|b_1| = 1$. Lemma 6 shows that these "egg-shapes" are just rotations and scalings of each other.

Let $x = \mu_{3,1}|b_1|, y = \mu_{3,2}|b_2^*|$, then these equations are given by:

$$\begin{aligned} \Psi^2 \begin{pmatrix} x & y & \sqrt{2/3} \\ 1 & 0 & 0 \end{pmatrix} &= \left(x^2 + y^2 + 2/3\right)\left(y^2 + 2/3\right) \\ &\leq b^2 \end{aligned} \tag{5}$$

$$\begin{aligned} \Psi^2 \begin{pmatrix} x & y & \sqrt{2/3} \\ a & b & 0 \end{pmatrix} &= \left(x^2 + y^2 + (2/3)\right)\left((bx - ay)^2 + (2/3)\left(a^2 + b^2\right)\right) \\ &\leq b^2 \end{aligned} \tag{6}$$

$$\begin{aligned} \Psi^2 \begin{pmatrix} x & y & \sqrt{2/3} \\ a-1 & b & 0 \end{pmatrix} &= \left(x^2 + y^2 + 2/3\right)\left((bx - (a-1)y)^2 + (2/3)\left((a-1)^2 + b^2\right)\right) \\ &\leq b^2 \end{aligned} \tag{7}$$

To show that these equations cover the fundamental Delaunay cell, we will treat the areas, A_i, of the Delaunay cell shown in figure 1 seperately. Let $F = \{(a, b) \mid a^2 + b^2 \geq 1, a^2 \leq 1/2, b^2 \leq 8/9, a > 0, b > 0\}$, and let $F' = \{(a, b) \in F \mid a^2 + b^2 = 1\}$. We note the cases $(a < 0, b < 0)$, $(a < 0, b > 0)$, $a > 0, b < 0)$ can be handled similarly in what follows, but it aids exposition to concentrate on just one of these at a time.

Covering A_1 We show that for every $(a, b) \in F$, if $(x, y) \in A_1$ then (x, y) also satisfies either equation 5 or equation 6. Let $A_1' = \{(x, y) \in A_1 \mid y \leq bx/(a+1)\}$ and $A_1'' = \{(x, y) \in A_1 \mid y/x \geq bx/(a+1)\}$.

Clearly the points $(x_0, y_0) = (0, 0)$ and $(x_1, y_1) = (1/2, 0)$ satisfy equation 5 for any $(a, b) \in F$, since $b^2 \geq 3/4$. To see that the point $(x_2, y_2) = ((a+1)/3, b/3)$ also satisfies equation 5 we plot the function

$$f_1(a, b) = \left(\left(\frac{a+1}{3}\right)^2 + \left(\frac{b}{3}\right)^2 + \frac{2}{3}\right)\left(\left(\frac{b}{3}\right)^2 + \frac{2}{3}\right) - b^2$$

[5]These vertices are the centroids of the the triangles in figure 1, and the faces of the Delaunay cell are therefore given by segments of the centroids.

[6]We note that in general the fact that these transformations do not decrease the Ψ-measure is not sufficient to show that a basis is Ψ-reduced, e.g. consider the basis $((1, 0, 0), (0, 1, 0), (0, 0.5, 0.95))$.

[7]The Ψ-measure is only dependent on the first two vectors, so we only show these, and note that these changes of basis can clearly be extended to $(3) \times (3)$ unimodular transformations.

for all $(a,b) \in F$ in figure 3(a). It is clear (e.g. by considering partial derivates or simply studying the plot) that this function is bounded by 0 for all $(a,b) \in F$ and achieves 0 only at the point $(a,b) = (1/2, \sqrt{3/4})$. Thus (x_2, y_2) satisfies equation 5, and by convexity (see corollary 3) we know all the points within the triangle of vertices $\{(x_0,y_0),(x_1,y_1),(x_2,y_2)\}$ also satisfy equation 5, i.e. all $(x,y) \in A_1'$.

Now we show that for every $(a,b) \in F$, if $(x,y) \in A_1''$ then (x,y) must satisfy equation 6. It follows from lemma 3 that

$$\Psi^2 \begin{pmatrix} x & y & \sqrt{2/3} \\ a & b & 0 \end{pmatrix} \leq b^2 \quad \Leftrightarrow \quad \Psi^2 \begin{pmatrix} x & y & \sqrt{2/3} \\ \alpha a & \alpha b & 0 \end{pmatrix} \leq (\alpha b)^2,$$

so we may restrict ourselves to considering $(a,b) \in F'$.

The rotational symmetry allows us to confirm

$$\begin{aligned}
\Psi^2 \begin{pmatrix} \frac{a+1}{3} & \frac{b}{3} & \sqrt{2/3} \\ a & b & 0 \end{pmatrix} &= \Psi^2 \left(\begin{pmatrix} \frac{a+1}{3} & \frac{b}{3} & \sqrt{2/3} \\ a & b & 0 \end{pmatrix} \begin{pmatrix} a & b & 0 \\ b & -a & 0 \\ 0 & 0 & 1 \end{pmatrix} \right) = \Psi^2 \begin{pmatrix} \frac{a+1}{3} & \frac{b}{3} & \sqrt{2/3} \\ 1 & 0 & 0 \end{pmatrix} \leq b^2, \\
\Psi^2 \begin{pmatrix} \frac{a}{2} & \frac{b}{2} & \sqrt{2/3} \\ a & b & 0 \end{pmatrix} &= \Psi^2 \left(\begin{pmatrix} \frac{a}{2} & \frac{b}{2} & \sqrt{2/3} \\ a & b & 0 \end{pmatrix} \begin{pmatrix} a & b & 0 \\ b & -a & 0 \\ 0 & 0 & 1 \end{pmatrix} \right) = \Psi^2 \begin{pmatrix} \frac{1}{2} & 0 & \sqrt{2/3} \\ 1 & 0 & 0 \end{pmatrix} \leq b^2,
\end{aligned}$$

for all $(a,b) \in F'$. Again we use a convexity argument to conclude that for every $(a,b) \in F$ and $(x,y) \in A_1''$ equation 6 is satisfied.

Covering A_2 We show that for every $(a,b) \in F$, if $(x,y) \in A_2$ then (x,y) also satisfies either equation 5 or equation 7. Let $A_2' = \{(x,y) \in A_2 \mid y \geq -bx/(2-a)\}$ and $A_2'' = \{(x,y) \in A_2 \mid y \leq -bx/(2-a)\}$.

We have already shown that the points $(x_1,y_1) = (0,0)$ and $(x_1,y_1) = (1/2,0)$ satisfy equation 5. To see that the point $(x_3,y_3) = ((2-a)/3, -b/3)$ also satisfies equation 5 we plot the function

$$f_2(a,b) = \left(\left(\frac{2-a}{3} \right)^2 + \left(\frac{b}{3} \right)^2 + \frac{2}{3} \right) \left(\left(\frac{b}{3} \right)^2 + \frac{2}{3} \right) - b^2$$

for all $(a,b) \in F$ in figure 3(b). It is clear (e.g. by considering partial derivates or simply studying the plot) that this function is bounded by 0 for all $(a,b) \in F$ and achieves 0 only at the point $(a,b) = (1/2, \sqrt{3/4})$. Thus (x_3,y_3) satisfies equation 5, and by convexity (see corollary 3) we know all the points within the triangle of vertices $\{(x_0,y_0),(x_1,y_1),(x_3,y_3)\}$ also satisfy equation 5, i.e. all $(x,y) \in A_2'$.

The region A_2'' is slightly more complicated than previous areas in that it is partially covered by equation 5 and partially covered by equation 7.

We have seen that the point (x_3,y_3) satisfies equation 5, and we will show that

1. the point $(x_4,y_4) = ((1-a)/2, -b/2)$ satisfies equation 7 for all $(a,b) \in F$,
2. there is a point $(\hat{x},\hat{y})$ on the face of the Delaunay cell between (x_3,y_3) and (x_4,y_4) that satisfies both equation 5 and equation 7 for all $a,b \in F$.

By convexity this will enable us to prove that all $(x,y) \in A_2''$ are satisfied by equation 5 or equation 7 for all $(a,b) \in F$.

The function $f_3(a,b) = \Psi^2(((1-a)/2, -b/2, \sqrt{2/3}), (a-1,b,0)) - b^2$ is plotted in figure 3(c). Again it can be seen that this function is bounded by 0 and only achieves 0 at $(a,b) = (1/3, \sqrt{8/9})$. Thus the point (x_4,y_4) must satisfy equation 7 for all $(a,b) \in F$.

We now define the point $(\hat{x},\hat{y})$: notice that equation 5 and equation 7 cross whenever

$$b^2x^2 + 2b(1-a)xy + a(a-2)y^2 + (2/3)(a(a-2)+b^2) = 0. \tag{8}$$

This is a hyperbolic equation, and dividing by y^2 and letting $x/y \to \infty$ we see that it has asymptotes at $y = bx/(a-1\pm 1)$. We define the point $(\hat{x},\hat{y})$ to be the point at which the hyperbola crosses the relevant

edge of the Delaunay cell, i.e. the line $y = (b/(a+1))(x-1)$, which can be seen to be explicitly given by[8]

$$(\hat{x}, \hat{y}) \quad = \quad \left(\frac{(a+1)(-2b + \sqrt{2a(2-a) - b^2}) + 3b}{3b}, \frac{-2b + \sqrt{2a(2-a) - b^2}}{3} \right). \tag{9}$$

This point is shown in figure 1(c), and the function $f_4(a,b) = \Psi^2((\hat{x}, \hat{y}, 2/3), (1,0,0)) - b^2$ is shown in figure 3(d). Once again the function can be seen to be bounded by 0, but in this case it achieves 0 at the two points $(a,b) = (1/2, \sqrt{3/4})$ and $(a,b) = (1/3, \sqrt{8/9})$. Regardless, we have shown the point $(\hat{x}, \hat{y})$ satisfies both equation 5 and equation 7, and hence all of A_2 is covered.

Covering A_3 The covering of A_3 by equation 6 and equation 7 follows from previous results and the symmetry of the problem. As before we may restrict ourselves to $(a,b) \in F'$ to minimize the area covered by equation 6 in which case A_3 is a reflection of A_2 in the line $y = -bx/(1-a)$, i.e. we can describe all points

$$A_2 \quad = \quad \{(x', y') \quad | (x', y') = (x, y)N, (x, y) \in A_3 \ \}$$

where

$$N = \begin{pmatrix} \frac{(1-a)^2 - b^2}{2(1-a)} & -b \\ -b & \frac{b^2 - (1-a)^2}{2(1-a)} \end{pmatrix}.$$

Lemma 1 and lemma 3 then allow us to confirm

$$\begin{aligned} \Psi^2 \begin{pmatrix} x & y & \sqrt{2/3} \\ a & b & 0 \end{pmatrix} &= \Psi^2 \left(\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} x & y & \sqrt{2/3} \\ a & b & 0 \end{pmatrix} \begin{pmatrix} \frac{(1-a)^2 - b^2}{2(1-a)} & -b & 0 \\ -b & \frac{b^2 - (1-a)^2}{2(1-a)} & 0 \\ 0 & 0 & 1 \end{pmatrix} \right) \\ &= \Psi^2 \begin{pmatrix} x' & y' & \sqrt{2/3} \\ 1 & 0 & 0 \end{pmatrix} \\ &\leq b^2, \end{aligned}$$

and

$$\begin{aligned} \Psi^2 \begin{pmatrix} x & y & \sqrt{2/3} \\ a-1 & b & 0 \end{pmatrix} &= \Psi^2 \left(\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x & y & \sqrt{2/3} \\ a-1 & b & 0 \end{pmatrix} \begin{pmatrix} \frac{(1-a)^2 - b^2}{2(1-a)} & -b & 0 \\ -b & \frac{b^2 - (1-a)^2}{2(1-a)} & 0 \\ 0 & 0 & 1 \end{pmatrix} \right) \\ &= \Psi^2 \begin{pmatrix} x' & y' & \sqrt{2/3} \\ a-1 & b & 0 \end{pmatrix} \\ &\leq b^2, \end{aligned}$$

where $(x', y') = (x, y)N$, and the bounds come from the corresponding bounds in A_2.

Final note We note the left one of the lattices in figure 2 is the regular tetrahedron, and is clearly Ψ-reduced from it's symmetry; the right lattice is the dual of the regular tetrahedron and is therefore also Ψ-reduced. The middle lattice cannot be Ψ-reduced for any choice of $\mu_{3,1}, \mu_{3,2}$.

We also note that by lemma 3 that if $|b_3^*| = \alpha |b_1|$ for some $\alpha < \sqrt{2/3}$ then all the Ψ-measures considered above decrease independently of $|b_2^*|$, so the areas A_1, A_2 and A_3 are fully covered in this case, i.e. there are no Ψ-reduced lattices with $\alpha < \sqrt{2/3}$.

□

[8]Note that the hyperbola actually crosses the line twice, but we are only interested in the instance given.

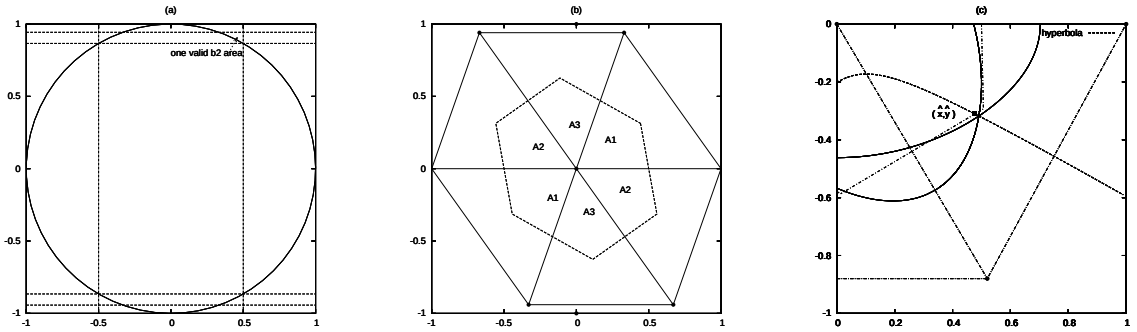
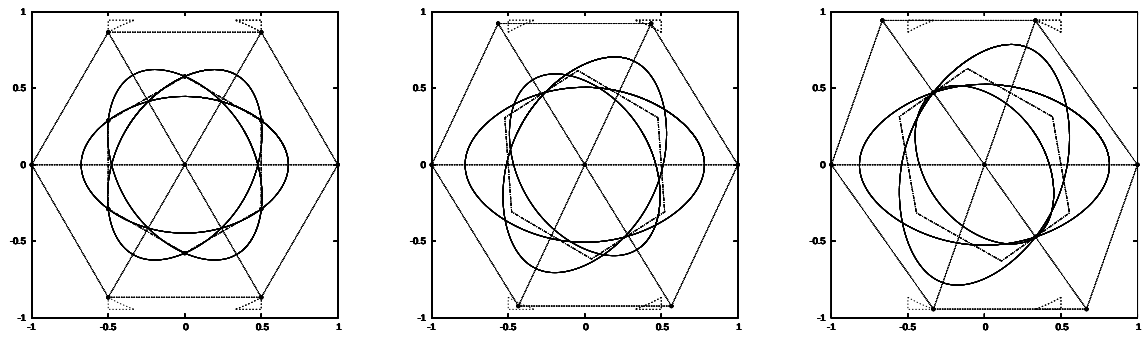


Figure 1: Left: the area in which the b_2 vector must lie. Middle: the fundamental Delaunay cell for $\mu_{2,1} = 1/3$, $|b_2| = |b_1|$. Right: diagram showing the intersection of equation 5 and equation 7, and the intersection of the hyperbolic equation 8 and the relevant face of the Delaunay cell



$$\begin{pmatrix} 1 & 0 & 0 \\ \frac{1}{2} & \frac{\sqrt{3}}{2} & 0 \\ \frac{1}{2} & \frac{1}{\sqrt{12}} & \sqrt{\frac{2}{3}} \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 & 0 \\ 0.424 & 0.923 & 0 \\ \mu_{3,1} & 0.923\mu_{3,2} & \sqrt{\frac{2}{3}} \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 & 0 \\ \frac{1}{3} & \frac{\sqrt{8}}{3} & 0 \\ -\frac{1}{3} & \frac{\sqrt{2}}{3} & \sqrt{\frac{2}{3}} \end{pmatrix}$$

Figure 2: The shapes and bases of the two critical 3-dimensional bases (left and right), scaled such that $|b_1| = 1$. The middle basis is not Ψ-reduced for any choice of $\mu_{3,1}, \mu_{3,2}$.

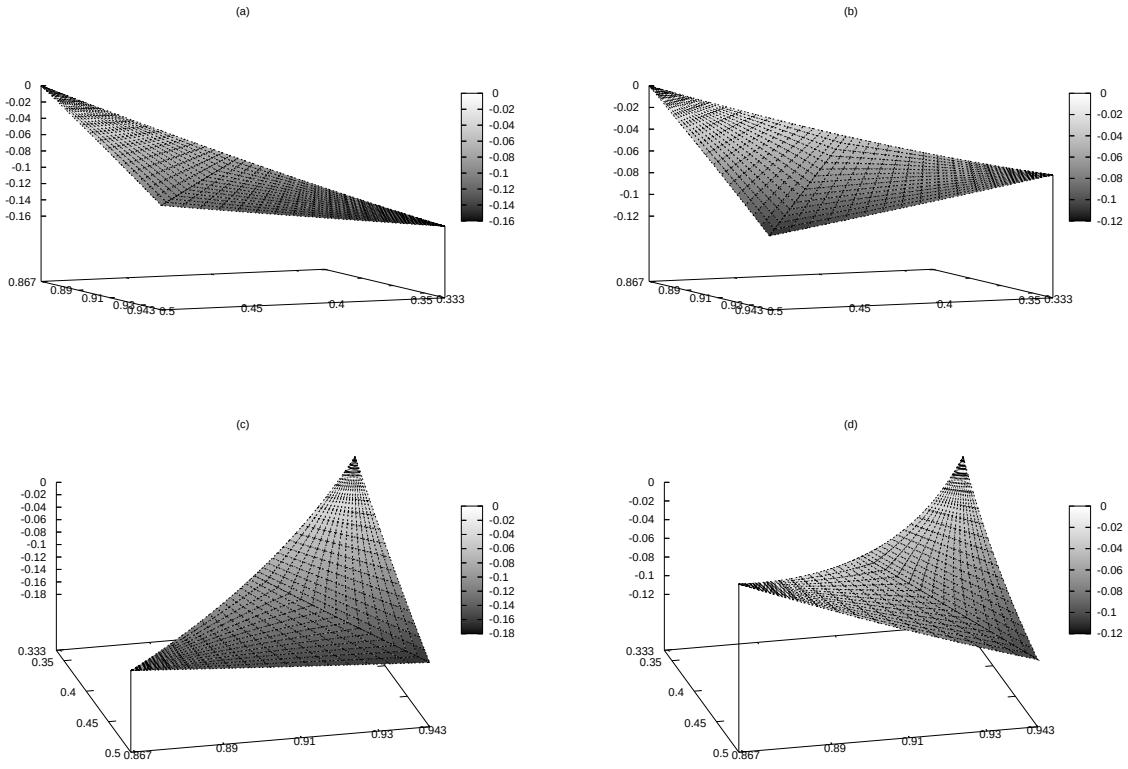


Figure 3: Surface plots of Ψ-measures of various bases

2.3 Properties of Ψ_m-reduced bases

We may extend the notion of a Ψ-reduced basis to blocks, as done in [18].

Definition 7. *For $1 \leq k \leq n-m+1$ we define the k'th m-block sub-basis of a lattice basis $\{b_1, \ldots, b_n\}$ to be the m-dimensional lattice basis gotten by projecting $\{b_k, \ldots, b_{k+m-1}\}$ in to the space orthogonal to $\{b_1, \ldots, b_{k-1}\}$.*

Definition 8. *A n-dimensional basis is called Ψ_m-reduced if every m-block sub-basis is Ψ-reduced.*

We first show that the notion of blocks fits well with duality. The proof follows some simple lemmas.

Theorem 2. *The modified-dual basis of the k'th m-block sub-basis of $\{b_1, \ldots, b_n\}$ is* a rotation *of the $(n-m+2-k)$'th m-block sub-basis of the modified-dual basis $\{d_1, \ldots, d_n\}$.*

Lemma 8. *If $M \in M_n(\mathbb{R})$ is lower triangular, then the inverse of the k'th m-block sub-matrix is the k'th m-block sub-matrix of the inverse of M.*

Proof. The m-block sub-matrices of M are simply the $(n-m+1)$ lower triangular $(m) \times (m)$ matrices along the diagonal of M. Simply from the fact that $MM^{-1} = 1$ and that M is lower triangular we know that the inverse of these blocks are the corresponding blocks in M^{-1}. □

Lemma 9. *If B is lower triangular, then the modified-dual matrix of the k'th m-block sub-matrix of B is the $(n-m+2-k)$'th m-block sub-basis of the modified-dual matrix $D = JB^{-t}J$.*

Proof. We consider starting with the lower triangular matrix B and k'th m-block sub-matrix $B^{(k)}$ with indices located between (k,k) and $(k+m-1, k+m-1)$. Lemma 8 shows that $\left(B^{(k)}\right)^{-1}$ is located between indices (k,k) and $(k+m-1, k+m-1)$ of B^{-1}, and thus $\left(B^{(k)}\right)^{-t}$ is located between indices (k,k) and $(k+m-1, k+m-1)$ of B^{-t}. It follows that $J\left(B^{(k)}\right)^{-t}J$ is located between indices $(n+2-k-m, n_2-k-m)$ and $(n+1-k, n+1-k)$ of $JB^{-t}J$. □

Proof. **of theorem 2**

Lemma 9 proves the result in the case that B is lower triangular. If B is not lower triangular we may rewrite it as $B = TN$ where T is lower triangular and N is orthonormal. The m-blocks of B are then *rotations* of the m-blocks of T.

By lemma 9 the m-blocks of T are also modified-dual matrices of the m-blocks of $JT^{-t}J = J\left(BN^{-1}\right)^{-t}J = JB^{-t}J(JN^tJ)$, i.e. the m-blocks of T are *rotations* of the modified-dual matrix $D = JB^{-t}J$. □

Corollary 4. *If a matrix B is Ψ_m-reduced, then the modified-dual matrix $D = JB^{-t}J$ is also Ψ_m-reduced.*

Proof. This follows immediately from theorem 2 and lemma 1. □

Example 2. *A worst case LLL-reduced basis is given by*

$$\begin{pmatrix} 1 & & & & & \\ 1/2 & \sqrt{3/4} & & & & \\ 0 & \sqrt{3/16} & 3/4 & & & \\ 0 & 0 & 3/8 & \sqrt{27/64} & & \\ & & & & \ddots & \\ & & & & & (3/4)^{(n-1)/2} \end{pmatrix}.$$

A worst case Ψ_3-reduced basis is given by

$$\begin{pmatrix} 1 & & & & & & \\ 1/2 & \sqrt{3/4} & & & & & \\ 1/2 & \sqrt{1/12} & \sqrt{2/3} & & & & \\ & -\sqrt{1/12} & \sqrt{1/6} & \sqrt{1/2} & & & \\ & & \sqrt{1/6} & \sqrt{1/18} & 2/3 & & \\ & & & & & \ddots & \\ & & & & & & (2/3)^{(n-1)/4} \end{pmatrix}.$$

Thus an LLL-reduced basis might have $|b_n^*| = (3/4)^{(n-1)/2} \approx 0.866^{n-1}$ *whereas a* Ψ_3*-reduced basis has a minimal* $|b_n^*| = (2/3)^{(n-1)/4} \approx 0.904^{n-1}$.

It is interesting to observe how the dual and primal critical lattices merge in the worst case Ψ_3*-reduced basis (this is the root lattice* $D4$*).*

3 Algorithms

3.1 Minimizing the Ψ-measure in dimension 3

Lemma 10. *An LLL-reduced basis* $\mathcal{B} = \{b_1, b_2, b_3\}$ *is* Ψ*-reduced if*

$$|b_2^*|^2 \quad > \quad \sqrt{\frac{4}{3}}|b_1|^2.$$

Proof. We consider all unimodular transformation matrices U which map from the LLL-reduced basis $\{b_1, b_2, b_3\}$ to another LLL-reduced basis $\{c_1, c_2, c_3\}$. We will show that for all such transformations $|c_1|^4|c_2^*|^2 \geq |b_1|^4|b_2^*|^2$, so $\mathcal{B}$ must be Ψ-reduced.

If the first row of U is of the form $(\star, 0, 0)$ then $|c_1|^2 \geq |b_1|^2$ and since $\mathcal{B}$ is LLL-reduced we know $|c_2^*|^2 \geq |b_2^*|^2$, thus $|c_1|^4|c_2^*|^2 \geq |b_1|^4|b_2^*|^2$. Otherwise if the first row of U has any other form we know $|c_1|^2 \geq |b_2^*|^2$, and $|c_2^*|^2 \geq (3/4)|c_1|^2$ so $|c_1|^4|c_2^*|^2 \geq (3/4)|b_2^*|^6 \geq |b_1|^4|b_2^*|^2$. □

Lemma 11. *If* $\mathcal{B}$ *is LLL-reduced but not* Ψ*-reduced then the* Ψ*-reduced basis* $\mathcal{C}$ *is such that*

$$|c_1|^2 \quad < \quad \sqrt{\frac{4}{3}}|b_1|^2.$$

Proof. Since $\mathcal{B}$ is not Ψ-reduced we can combine lemma 10 with the formula for $\Psi(\mathcal{C}) < \Psi(\mathcal{B})$:

$$\frac{3}{4}|c_1|^6 < |c_1|^4|c_2^*|^2 < |b_1|^4|b_2^*|^2 < \sqrt{\frac{4}{3}}|b_1|^6$$

□

Lemma 10 and lemma 11 motivate algorithm 1 given below.

Algorithm 1 Ψ-reducing a 3-dimensional lattice

```
LLL-reduce the input basis to form a basis {b1, b2, b3}
if |b2*|^2 > sqrt(4/3)|b1|^2 then
   return {b1, b2, b3}
else
   for each vector c1, |c1|^2 < sqrt(4/3)|b1|^2 do
      Complete c1 to a basis {c1, c2, c3}
      LLL-reduce {c1, c2, c3} {this just involves LLL reducing {c2, c3}}
      if Ψ(C) < Ψ(B) then
         Set {b1, b2, b3} ← {c1, c2, c3}
      end if
   end for
   return {b1, b2, b3}
end if
```

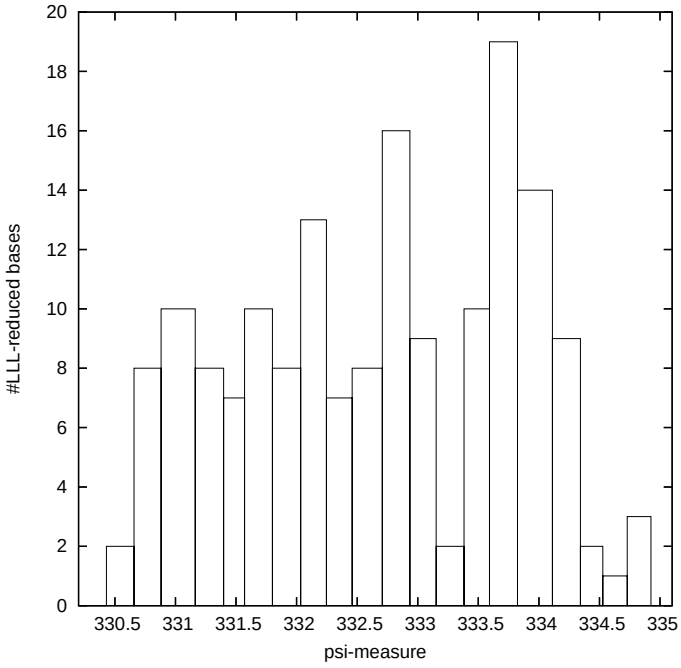


Figure 4: Range of the Ψ-measure for all LLL reduced lattices of M_9

3.2 Enumerating LLL-reduced bases in arbitrary dimension

Kannan's algorithm [10] is a way to enumerate all the small vectors in a lattice. By using the provable bounds on the first vector for LLL-reduced bases one can recursively use this algorithm to enumerate all possible LLL-reduced bases. The tree-search can be pruned whenever the initial choices made do not form an LLL-reduced basis. If we are just interested in Ψ-reduced bases then we may prune if the initial choices are not Ψ-reduced. This gives a provable, but costly method of finding a Ψ-reduced basis in arbitrary dimension.

We do not study the complexity analysis of this algorithm here, but state that for dimension less than 10 the technique is reasonably efficient (less than an hour on a 2.21GHz machine with 1GB of RAM using the NTL library in Cygwin on a Windows XP machine). The range of values of the Ψ-measure, for a lattice[9] of dimension 9 are given in figure 4. It is interesting to observe that the Ψ-measure is relatively uniform. In this example the least value of Ψ-measure corresponded to both the Ψ-reduced basis, and KZ-reduced basis.

3.3 Heuristics for reducing the Ψ-measure in arbitrary dimension

Naively examining the Ψ measure might lead us to noticing that $|b_1|$ is raised to the largest power, so we may try to reduce $|b_1|$, and then with that choice for smallest vector we may aim to reduce $|b_2^*|$, etc. This would end up using an SVP-oracle in the same way as the KZ notion of reduction to reduce the Ψ-measure. For a given blocksize β one could then do an algorithm similar to LLL. Although this approach may work reasonably in practice, the example 1 shows that it does not truly *minimize* the Ψ-measure, even in dimension 3. We call this the *KZ-approach*.

However, even limiting ourselves to an SVP-oracle we can do better than this, by considering equation 2. In this formulation of Ψ we see explicitly that maximizing $|b_n^*|$ is "more important" that minimizing $|b_2^*|$, in that it has a higher power associated with it.

Prior work has shown one can maximize $|b_n^*|$ by minimizing $|d_1|$ in the dual lattice[9, 8], thus one can just use an SVP algorithm [10, 1].

[9]The particular basis M_9 was extracted from sub-block a well-reduced NTRU lattice; it is anticipated that it is a "typical" BKZ-reduced 9-dimensional basis.

Thus one strategy might be to minimize $|b_1^*|$, maximize $|b_n^*|$, minimize $|b_2^*|$, maximize $|b_{n-1}^*|$, etc. While this heuristic seems reasonable, the example basis 1 again shows that it fails to achieve the minimal Ψ-measure, even in dimension 3. We call this the *balanced approach*, although we do note it is not exactly balanced since it has a slight preference for mimimizing b_1 over maximizing b_n^*, rather than the ratio $|b_1|/|b_n^*|$.

This idea can be combined with exhaustive search, in that one may several candidate vectors for small b_1, and then for each of these find several candidate large b_n^*, and recurse on the technique. If we only recurse for to a depth for which exhaustive search is reasonable, and then use the balanced approach to estimate the Ψ-measure for the middle[10], this can lead to an effective technique. We call this the *balanced approach with search*.

4 The hierarchy of polynomial-time algorithms

Essentially this is exactly the algorithm given in [14], i.e. for each consecutive block try to minimize the Ψ-measure. If one cannot reduce the Ψ-measure of a block then consider the next one, however if one can reduce it by some constant factor (e.g. 0.99), then do so, and step back to the first block that has changed as a result of the linear transformation applied. The Ψ-measure monotonically decreases by a constant factor, so the algorithm must terminate in polynomial time for a fixed blocksize.

5 Experimental results

Experiments are currently being run. We examine the NTRU lattice, with the 80-bit security parameters.

We use the BKZ implementation in the NTL library [20] as a KZ-oracle for arbitrary dimension m (the blocksize). When finer control over Kannan's algorithm is needed we use our own implementation. The BKZ implementation in the NTL library [20] has very good performance on NTRU lattices [7] up to blocksize around 20, after which performance degrades substantially.

After blocksize 25 it becomes preferable to use the balanced approach given in section 3.3. However, fascinatingly, the balanced approach fails to make any progress after blocksize around 30, i.e. putting the smallest vector first (in the primal, then dual, etc.) does not lead to a smaller Ψ-measure. In this case we use balanced approach with search (typically with checking $3^4 = 81$ combinations of the first two vectors, and the last two). The balanced approach typically makes a small amount of progress (i.e. the Ψ-measure is slighlty reduced), but the complexity of this approach is prohibitive. Further analysis is currently being conducted.

6 A further generalization

We note that the KZ-reduced notion and the Ψ-reduced notion can be mixed in that one can define an ordering on lattices by lexicographic ordering on the Ψ-measure of the sub-basis of a fixed blocksize.

We also note that there are other possible isodual notions of a reduced basis, e.g. lexicographically minimizing $|b_1|/|b_n^*|$, $|b_2|/|b_{n-1}^*|$, ... We note that this is the same as our notion in the case $n = 3$. The problem with this definition is that a proof of polynomial time termination is non-trivial for $n > 3$, even though the method may work well in practice.

7 Acknowledgements

I would like to thank Daniele Micciancio and Phong Nguyen for early conversations about this work, and Cong Ling for detailed comments on this manuscript.

[10] We would apply the balanced approach with search recursively to the middle, but we need an initial estimate to know which middle to consider.

8 Conclusions and open questions

This work opens a number of interesting questions. A first interesting question is to work out the asymptotics of η_n akin to the known asymptotics of Hermite's constants. Then it would be interesting to work out a few more of the η_n constants, and give best guesses for larger n. It would be fascinating to see if/when the critical lattices for γ_n and η_n differ.

On the algorithmic side it seems it is likely that there are far more efficient, provable techniques for reducing the Ψ-measure in blocksize $4, 5, 6 \ldots$, rather than enumerating all the LLL-reduced(or Ψ-reduced) bases as described in section 3.2. It would be very interesting if there is a reasonaly efficient strategy in arbitrary dimension.

References

[1] M. Ajtai, R. Kumar and D. Sivakumar, *A sieve algorithm for the shortest lattice vector problem,* Proc. 33rd ACM Symp. on Theory of Comput., Crete, Greece, July 6-8, 2001, 601–610.

[2] J. W. S. Cassels *An introduction to the geometry of numbers*, Springer-Verlag, Reprint of the 1st ed. Berlin Heidelberg New York 1959. Corr. 2nd printing 1971, 1997, VIII

[3] J. H. Conway, N. J. A. Sloane, *Sphere Packings, Lattices and Groups*. Grundlehren der mathematischen Wissenschaften 290, 1993

[4] D. Coppersmith, *Finding a Small Root of a Univariate Modular Equation*. Proc. Eurocrypt 1996, pp. 155–165.

[5] N. Gama, N. Howgrave-Graham, H. Koy, P. Q. Nguyen *Rankin's constant and blockwise lattice reduction*, Proc. of CRYPTO '06, LNCS vol. 4117.

[6] N. Gama, N. Howgrave-Graham, P. Q. Nguyen *Symplectic Lattice Reduction and NTRU*, Proc. of CRYPTO '06, LNCS vol. 4117.

[7] J. Hoffstein, J. Pipher, J. H. Silverman *NTRU: A Ring-Based Public Key Cryptosystem*, in Algorithmic Number Theory (ANTS III), Portland, OR, June 1998, J.P. Buhler (ed.), Lecture Notes in Computer Science 1423, Springer-Verlag, Berlin, 1998, 267-288.

[8] N. Howgrave-Graham, *Finding Small Roots of Univariate Modular Equations Revisited*, IMA Int. Conf. 1997, pp. 131–142.

[9] N. Howgrave-Graham, *Computational mathematics inspired by RSA*, Ph. D. Thesis, University of Bath, 1999.

[10] R. Kannan, *Improved algorithms for integer programming and related lattice problems*, In Proc. 15th symposium on the Theory of Computation (STOC 1983), pp. 99-108. ACM Press, 1983.

[11] A. Korkin, G. Zolotarev, *Sur les formes quadratiques*, Math. Ann 6, 366-389, 1873.

[12] A. Korkin, G. Zolotarev, *Sur les formes quadratiques*, Math. Ann 11, 242-292, 1877.

[13] B. La Macchia *Basis Reduction Algorithms and Subset Sum Problems*, Ph. D. Thesis, MIT, 1991.

[14] A. K. Lenstra, H. W. Lenstra, L. Lovasz *Factoring Polynomials with Rational Coefficients*, Mathematische Annalen, vol. 261, n. 4, 1982, pp. 515–534

[15] H. Minkowski, *Diskontinuitsbereich fur arithmetic Aquivalenz*, J. reine Angew. 129, pp. 220–224.

[16] M. Seysen, *Simultaneous reduction of a lattice basis and its reciprocal basis*, Combinatorica 13(3), pp. 363–376, 1993.

[17] C. P. Schnorr *Lattice Reduction by Random Sampling and Birthday Methods*, STACS 2003, LNCS 2607, Springer-Verlag, pp. 145–156

[18] C. P. Schnorr *A Hierarchy of Polynomial Time Lattice Basis Reduction Algorithms*, Theoretical Computer Science, Vol. 53, pp. 201–224, 1987.

[19] C. P. Schnorr, M. Euchner *Lattice Basis Reduction: Improved Practical Algorithms and Solving Subset Sum Problems*, Mathematical Programming, Vol. 66, pp. 181–191, 1994.

[20] V. Shoup *NTL: A Library for doing Number Theory*, Version 5.4, `http://www.shoup.net/ntl`