Electronic Colloquium on Computational Complexity, Revision 7 of Report No. 50 (2011)

Accelerated and Improved Slide- and LLL-Reduction

Claus Peter Schnorr

Fachbereich Informatik und Mathematik,
Goethe-Universität Frankfurt, PSF 111932,
D-60054 Frankfurt am Main, Germany.
schnorr@cs.uni-frankfurt.de

February 9, 2012

Abstract. We accelerate the slide-reduction algorithm of [GN08] with blocksize k to run for a given LLL-basis B of dimension $n = hk$ under reasonable assumptions within $\frac{1}{4}\, n^2 h \log_{1+\varepsilon} \alpha$ local SVP-computations of dimension k, where $\alpha \geq \frac{4}{3}$ is the quality of the given LLL-basis and ε is the quality of slide-reduction. If the given basis B is already slide-reduced for blocksize $k/2$ the $\frac{1}{4}\, n^2 h \log_{1+\varepsilon} \alpha$ bound further decreases to $nh^2(1+\log_{1+\varepsilon} \gamma_{k/2})$, where $\gamma_{k/2}$ is the Hermite constant. These bounds are polynomial in n for arbitrary bit-length of B. Slide-reduced bases for which the approximation factor $\|\mathbf{b}_1\|/\lambda_1$ is nearly maximal can easily be improved. If $\|\mathbf{b}_1\|/\lambda_1 = \gamma_k^{\frac{n-k}{k-1}}$ is maximal we can easily find a shortest lattice vector. We also accelerate LLL-reduction.

Keywords. Block reduction, LLL-reduction, slide reduction.

Introduction. Lattices are discrete subgroups of the $\mathbb{R}^n$. A basis $B = [\mathbf{b}_1, ..., \mathbf{b}_n] \in \mathbb{R}^{m\times n}$ of n linear independent vectors $\mathbf{b}_1, ..., \mathbf{b}_n$ generates the lattice $\mathcal{L}(B) = \{B\mathbf{x} \,|\, \mathbf{x} \in \mathbb{Z}^n\}$ of dimension n. Lattice reduction algorithms transform a given basis into a basis consisting of short vectors. The length of $\mathbf{b} \in \mathbb{R}^m$ is $\|\mathbf{b}\| = (\mathbf{b}^t\mathbf{b})^{1/2}$. $\lambda_1(\mathcal{L}) = \min_{\mathbf{b}\in\mathcal{L}\setminus\mathbf{0}} \|\mathbf{b}\|$ is the minimal length of nonzero $\mathbf{b} \in \mathcal{L}$. The determinant of $\mathcal{L}$ is $\det \mathcal{L} = (\det B^tB)^{1/2}$. The Hermite bound $\lambda_1(\mathcal{L})^2 \leq \gamma_n(\det \mathcal{L})^{2/n}$ holds for all lattices $\mathcal{L}$ of dimension n and the Hermite constant γ_n.

The LLL-algorithm of H.W. Lenstra Jr., A.K. Lenstra and L. Lovász [LLL82] transforms a given basis B in polynomial time into a basis B such that $\|\mathbf{b}_1\| \leq \alpha^{\frac{n-1}{2}} \lambda_1$, where $\alpha > 4/3$. It is important to minimize the proven bound on $\|\mathbf{b}_1\|/\lambda_1$ for polynomial time reduction algorithms and to optimize the polynomial time.

The best known algorithms perform blockwise basis reduction for blocksize $k \geq 2$ generalizing the blocksize 2 of LLL-reduction. Schnorr [S87] introduced blockwise HKZ-reduction. The algorithm of [GHKN06] improves blockwise HKZ-reduction by blockwise primal-dual reduction. So far slide-reduction of [GN08b] yields the smallest proven approximation factor $\|\mathbf{b}_1\|/\lambda_1 \leq ((1+\varepsilon)\gamma_k)^{\frac{n-k}{k-1}}$ of polynomial time reduction algorithms. The algorithm for slide-reduction of [GN08b] performs $O(nh \cdot \mathrm{size}(B)/\varepsilon)$ local SVP-computations, where size(B) is the bit-length of B and ε is the quality of slide-reduction. This bound is polynomial in n if and only if size(B) is polynomial in n. The workload of the local SVP-computations dominates the overall workload. [NSV10] shows that the bit complexity of LLL-reduction is quasi-linear in size(B). The LLL-reduction is performed on the leading bits of the entries of the basis matrix (similar to Lehmer's gcd-algorithm) using fast arithmetic for the multiplication of integers and fast algorithms for matrix multiplication.

Our results. We improve the $O(nh \cdot \mathrm{size}(B)/\varepsilon)$ bound of [GN08b] by choosing the blocks for the next local reduction step as to maximize its progress. We first analyze this strategy in minimizing $\|\mathbf{b}_1\|/(\det \mathcal{L})^{1/n}$ by the concept of *almost slide reduction* and then extend this analysis to minimize $\|\mathbf{b}_1\|/\lambda_1(\mathcal{L})$. Theorem 1 studies the maximal number of local SVP-computations during almost slide-reduction with blocksize k for an input LLL-basis $B \in \mathbb{Z}^{m\times n}$ for δ, α and dimension $n = hk$. It shows under a reasonable assumption that this number is at most $\frac{1}{4}\, n^2 h \log_{1+\varepsilon} \alpha$. This bound is independent of the bit-length of B. Corollary 1 shows that if the given basis is almost slide-reduced for blocksize $k/2$ the number of local SVP-computations for almost slide-reduction with blocksize k further decreases to $nh^2 \frac{1}{1-2/k}(1 + \log_{1+\varepsilon} \gamma_{k/2})$, halving the bound of Theorem 1 for $k = 32$. For the first time this qualifies the advantage of first performing block reduction with half

ISSN 1433-8092

the blocksize. Theorem 4 shows that given a slide-reduced basis for blocksize k and $\varepsilon = 0$ such that $\|\mathbf{b}_1\|/\lambda_1 = \gamma_k^{\frac{n-k}{k-1}}$ is maximal, we can easily find a shortest lattice vector. More generally, this indicates that the closer $\|\mathbf{b}_1\|/\lambda_1$ is to the maximumf for slide-reduced bases of dimension n and blocksize k the easier it is to find a nonzero lattice vector $\mathbf{b}$ that is substantially shorter than $\mathbf{b}_1$. We point to such an algorithm.

We also accelerate LLL-reduction. Corollary 3 shows, under a reasonable assumption, that accelerated LLL-reduction computes an LLL-basis within $n^3 \log_2 \mathrm{size}(B)/3$ local LLL-reductions of dimension 2. This bound is polynomial in n if $\log_2 \mathrm{size}(B) = n^{O(1)}$. Lemma 2 shows that every LLL-basis for δ such that $1 - \delta \le 2^{-4\,\mathrm{size}(B)}$ is an ideal LLL-basis for $\delta = 1$.

Notation. Let $B = [\mathbf{b}_1, ..., \mathbf{b}_n] \in \mathbb{R}^{m\times n}$ be a basis matrix of rank $n = hk$ and $B = QR$ be its QR-decomposition, where $R = [r_{i,j}]_{1\le i,j\le n} \in \mathbb{R}^{n\times n}$ is upper triangular with positive diagonal entries $r_{i,i} > 0$ and $Q \in \mathbb{R}^{m\times n}$ is isometric with pairwise orthogonal column vectors of length 1. We denote $\mathrm{GNF}(B) = R$. Let $R_\ell = [r_{i,j}]_{k\ell-k+1\le i,j\le k\ell} \in \mathbb{R}^{k\times k}$ be the submatrix of $R = [r_{i,j}] \in \mathbb{R}^{n\times n}$ for the ℓ-th block of blocksize $k \ge 2$, $\mathcal{D}_\ell = (\det R_\ell)^2$. Let $R'_\ell = [r_{i,j}]_{k\ell-k+2\le i,j\le k\ell+1} \in \mathbb{R}^{k\times k}$ denote the ℓ-th block slided by one unit. $R_\ell^\bigstar = U_k R_\ell^{-t} U_k$ is the dual of $R_\ell \in \mathbb{R}^{k\times k}$, where R_ℓ^{-t} is the inverse transpose of R_ℓ and $U_k \in \{0,1\}^{k\times k}$ is the reversed identity matrix with nonzero entries $u_{i,k-i+1} = 1$ for $i = 1, ..., k$. Note that $\mathrm{GNF}(R_\ell^\bigstar) = R_\ell^\bigstar$. $R_\ell'^\bigstar = (R'_\ell)^\bigstar$ is the dual of R'_ℓ.

Let $\max_{R'_\ell T} r_{k\ell+1,k\ell+1}$ denote the maximum of $\bar{r}_{k\ell+1,k\ell+1}$, $[\bar{r}_{i,j}]_{k\ell-k+2\le l,j\le k\ell+1} := \mathrm{GNF}(R'_\ell T)$ over all $T \in \mathrm{GL}_k(\mathbb{Z})$. Note that $\max_{R'_\ell T} r_{k\ell+1,k\ell+1} = 1/\lambda_1(\mathcal{L}(R_\ell'^\bigstar))$. Let $\pi_i : \mathbb{R}^n \to \mathrm{span}(\mathbf{b}_1, ..., \mathbf{b}_{i-1})^\perp$ be the orthogonal projection, and $\mathbf{b}_i^* := \pi_i(\mathbf{b}_i)$ thus $\|\mathbf{b}_i^*\| = r_{i,i}$.

LLL-bases. [LLL82] A basis $B = QR \in \mathbb{R}^{m\times n}$ is LLL-basis for δ, $\frac{1}{4} < \delta \le 1$, $\alpha = 1/(\delta - 1/4)$ if

- $|r_{i,j}| \le \frac{1}{2}\, r_{i,i}$ holds for all $j > i$,
- $\delta r_{i,i}^2 \le r_{i,i+1}^2 + r_{i+1,i+1}^2$ holds for $i = 1, ..., n-1$.

An LLL-basis B for δ satisfies $\|\mathbf{b}_\ell^*\|^2/\|\mathbf{b}_{\ell+1}^*\|^2 \le \alpha$ for all $\ell = 1, ..., n-1$ and

$$\|\mathbf{b}_1\| \le \alpha^{\frac{n-1}{4}} (\det \mathcal{L})^{1/n}, \qquad \|\mathbf{b}_1\| \le \alpha^{\frac{n-1}{2}} \lambda_1.$$

Definition 1. [GN08] *A basis* $B = QR \in \mathbb{R}^{m\times n}$, $n = hk$ *is* slide-reduced *for* $\varepsilon \ge 0$ *and* $k \ge 2$ *if*

1. $\|\mathbf{b}_{k\ell+1}^*\| = r_{k\ell+1,k\ell+1} = \lambda_1(\mathcal{L}(R_{\ell+1}))$ *for* $\ell = 0, ..., h-1$,

2. $\max_{R'_\ell T} r_{k\ell+1,k\ell+1} \le \sqrt{1+\varepsilon} \cdot \|\mathbf{b}_{k\ell+1}^*\|$ *holds for* $\ell = 1, ..., h-1$.

1 slightly relaxes the condition of [GN08] that all bases R_ℓ are HKZ-reduced. The following bounds have been proved by Gama and Nguyen in [GN08, Theorem 1] for slide-reduced bases:

3. $\|\mathbf{b}_1\| \le ((1+\varepsilon)\gamma_k)^{\frac{1}{2}\frac{n-1}{k-1}} (\det \mathcal{L})^{1/n}$, **4.** $\|\mathbf{b}_1\| \le ((1+\varepsilon)\gamma_k)^{\frac{n-k}{k-1}} \lambda_1$.

Almost slide-reduced (asr-) bases. We call a basis $B = QR \in \mathbb{R}^{m\times n}$, $n = hk$, an asr-basis for $\varepsilon \ge 0$ and blocksize k if clause **2** of Def. 1 holds for some $\ell = \ell_{max}$ that maximizes $\mathcal{D}_\ell/\mathcal{D}_{\ell+1}$ and clause **1** of Def. 1 holds for $R_1, R_\ell, R_{\ell+1}$.
Theorem 2 shows that a slightly stronger inequality **3.** holds for all asr-bases.

Accelerated almost slide reduction (ASR)
`INPUT` LLL-basis $B = QR \in \mathbb{Z}^{m\times n}$, $R = [r_{i,j}] \in \mathbb{R}^{n\times n}$, $n = hk$, $0 < \varepsilon \le 1$, $k \ge 2$
`LOOP` Choose some $\ell = \ell_{max}$ that maximizes $\mathcal{D}_\ell/\mathcal{D}_{\ell+1}$. By SVP-computations on $\mathcal{L}(R_\ell)$, $\mathcal{L}(R_{\ell+1})$ transform $R_\ell, R_{\ell+1}$ and B such that **1** of Def. 1 holds for $R_\ell, R_{\ell+1}$.
By an SVP-computation on $R_\ell'^\bigstar$ verify whether **2** holds for ℓ and the input ε.
`IF` **2** does not hold `THEN` transform R'_ℓ and B such that **2** holds for $\varepsilon = 0$
`ELSE` transform R_1 and B such that $\|\mathbf{b}_1\| = \lambda_1(\mathcal{L}(R_1))$ and terminate. `end loop`
`OUTPUT` the resulting asr-basis B.

We can replace the 3 SVP-computations per round on $\mathcal{L}(R_\ell), \mathcal{L}(R_{\ell+1}), \mathcal{L}(R_\ell'^\bigstar)$ by the stronger and faster two SVP-computations on $\mathcal{L}(R_{\ell+1})$, $\mathcal{L}(R_\ell^{+\bigstar})$, where $R_\ell^+ = [r_{i,j}]_{\ell k-k<i,j\le \ell k+1} \in \mathbb{R}^{(k+1)\times(k+1)}$. Alternatively we can perform two SVP-computations on $\mathcal{L}(R_\ell^\bigstar), \mathcal{L}(R_{\ell+1}'^+)$ per round, where $R_{\ell+1}'^+ := [r_{i,j}]_{\ell k\le i,j\le \ell k+k} \in \mathbb{R}^{(k+1)\times(k+1)}$.

Theorem 1. **ASR** *transforms a given LLL-basis $B \in \mathbb{Z}^{m\times n}$ for $\delta \le 1$, $\alpha = 1/(\delta - 1/4)$, $n = hk$, within $\frac{1}{12}n^2 h \log_{1+\varepsilon}\alpha$ rounds (passes of the* **loop***) of three local SVP-computations of dimension k either into an almost slide-reduced basis for ε and blocksize k, or else arrives at $\mathcal{D}(B) < 1$, where*

$$\mathcal{D}(B) =_{\mathrm{def}} \prod_{\ell=1}^{h-1}(\mathcal{D}_\ell/\mathcal{D}_{\ell+1})^{h\ell-\ell^2} = \mathcal{D}_1^{h-1}\mathcal{D}_2^{h-3}\cdots\mathcal{D}_\ell^{h-2\ell+1}\cdots\mathcal{D}_{h-1}^{-h+3}\mathcal{D}_h^{-h+1}.$$

Proof. We use the novel version $\mathcal{D}(B)$ of the Lovász invariant to measure B's reducedness. Note that $h^2/4 - (\ell - h/2)^2 = h\ell - \ell^2$ is symmetric to $\ell = h/2$ with maximal point $\ell = \lceil h/2 \rfloor = \lceil h/2 - 1/2\rceil$. The input LLL-basis $B^{(in)}$ for $\delta \le 1$ satisfies for $\alpha = 1/(\delta - 1/4)$ that $\mathcal{D}_\ell/\mathcal{D}_{\ell+1} \le \alpha^{k^2}$ and thus

$$\mathcal{D}(B^{(in)}) \le \alpha^{k^2 s} \quad \text{for} \quad s := \textstyle\sum_{\ell=1}^{h-1} h\ell - \ell^2 = \frac{h^3-h}{6}.$$

Fact. Every non-terminal round with ℓ decreases $\mathcal{D}_\ell$ and $\mathcal{D}(B)$ as

$$\mathcal{D}_\ell^{new} \le \mathcal{D}_\ell/(1+\varepsilon) \qquad \mathcal{D}(B^{new}) \le \mathcal{D}(B)/(1+\varepsilon)^2.$$

This is because the round changes merely the factor $\prod\limits_{t=\ell-1,\ell,\ell+1}(\mathcal{D}_t/\mathcal{D}_{t+1})^{t(h-t)} = (\mathcal{D}_\ell\mathcal{D}_{\ell+1})^{h-2\ell-1}\,\mathcal{D}_\ell^2$ of $\mathcal{D}(B)$, where $\mathcal{D}_\ell\mathcal{D}_{\ell+1}$ does not change. Hence, after at most

$$\tfrac{1}{2}\log_{1+\varepsilon}\mathcal{D}(B^{(in)}) \le \tfrac{1}{2}\log_{1+\varepsilon}(\alpha^{k^2 s}) = \tfrac{1}{2}k^2\tfrac{h^3-h}{6}\log_{1+\varepsilon}\alpha < \tfrac{n^2h}{12}\log_{1+\varepsilon}\alpha$$

rounds either B is asr-basis for ε or else $\mathcal{D}(B) < 1$. Our bound on the number of rounds does not count the terminal round which does not decrease $\mathcal{D}$. □

Remarks. 1. We conjecture that the time bound of Theorem 1 even holds if on termination $\mathcal{D}(B) < 1$. This might be provable by the dynamical system method of [HPS11]. Anyway, $\mathcal{D}(B) < 1$ is very unlikely. If $\mathcal{D}(B) < 1$ then $\mathbf{E}[\ln(\mathcal{D}_\ell/\mathcal{D}_{\ell+1})] < 0$ holds for the expectation $\mathbf{E}$ for random ℓ with $\mathbf{Pr}(\ell) =_{\mathrm{def}} 6\frac{\ell h-\ell^2}{h^3-h^2-h}$. (Note that $\sum_{\ell=1}^{h-1}\mathbf{Pr}(\ell) = 1$.) In this sense $\mathcal{D}_\ell < \mathcal{D}_{\ell+1}$ would hold "on the average" if $\mathcal{D}(B) < 1$, whereas such $\mathcal{D}_\ell, \mathcal{D}_{\ell+1}$ are extremely unlikely.
2. On the other hand, if the output basis of **ASR** satisfies on average that $\|\mathbf{b}_\ell^*\|^2/\|\mathbf{b}_{\ell+1}^*\|^2 \ge \alpha^{1/t}$ then the number of rounds decreases to at most $(1-1/t)\frac{n^2h}{12}\log_{1+\varepsilon}\alpha$.

Theorem 2. *Every asr-basis $B \in \mathbb{Z}^{m\times n}$ for ε, k satisfies $\|\mathbf{b}_1\| \le \left((1+\varepsilon)^{\frac{1+1/k}{2}}\gamma_k\right)^{\frac{1}{2}\frac{n-1}{k-1}}(\det\mathcal{L})^{1/n}$.*

Proof. We see from clause **2** of Def. 1 and the Hermite bound on $\lambda_1(\mathcal{L}(R'_\ell)^\bigstar) \le 1/r_{k\ell+1,k\ell+1}$ that

$$\mathcal{D}'_\ell/r^2_{k\ell+1,k\ell+1} \le ((1+\varepsilon)\gamma_k)^k\, r^{2k-2}_{k\ell+1,k\ell+1} \tag{1}$$

holds for $\ell = \ell_{max}$, where $\mathcal{D}'_\ell := (\det R'_\ell)^2$. Moreover, the Hermite bound for R_ℓ shows that

$$r^{2k-2}_{k\ell-k+1,k\ell-k+1} \le \gamma_k^k\,\mathcal{D}_\ell/r^2_{k\ell-k+1,k\ell-k+1}.$$

Combining these two inequalities with $\mathcal{D}'_\ell/r^2_{k\ell+1,k\ell+1} = \mathcal{D}_\ell/r^2_{k\ell-k+1,k\ell-k+1}$ yields for $\ell = \ell_{max}$:

$$r_{k\ell-k+1,k\ell-k+1} \le ((1+\varepsilon)\gamma_k)^{\frac{k}{k-1}}\, r_{k\ell+1,k\ell+1}. \tag{2}$$

Next we prove

$$\mathcal{D}_\ell/\mathcal{D}_{\ell+1} \le ((1+\varepsilon)^{\frac{1+1/k}{2}}\gamma_k)^{\frac{2k^2}{k-1}} \quad \text{for } \ell = 1,\dots,h-1. \tag{3}$$

Proof. As (1) holds for $\ell = \ell_{max}$ and **1** holds for $R_{\ell+1}$ the Hermite bound on $\lambda_1(\mathcal{L}(R_{\ell+1}))$ yields

$$\mathcal{D}'_\ell \le (1+\varepsilon)^k\gamma_k^k r^{2k}_{k\ell+1,k\ell+1} \le (1+\varepsilon)^k\gamma_k^{2k}\mathcal{D}_{\ell+1}.$$

Hence (2) yields for $\ell = \ell_{max}$

$$\mathcal{D}_\ell = r^2_{k\ell-k+1,k\ell-k+1}\mathcal{D}'_\ell/r^2_{k\ell+1,k\ell+1} \le ((1+\varepsilon)\gamma_k)^{\frac{2k}{k-1}}\mathcal{D}'_\ell. \tag{4}$$

Combining the two previous inequalities yields for $\ell = \ell_{max}$

$$\mathcal{D}_\ell \le ((1+\varepsilon)\,\gamma_k)^{\frac{2k}{k-1}}(1+\varepsilon)^k\gamma_k^{2k}\mathcal{D}_{\ell+1} = ((1+\varepsilon)^{\frac{1+1/k}{2}}\gamma_k)^{\frac{2k^2}{k-1}}\mathcal{D}_{\ell+1}.$$

Moreover if (3) holds for ℓ_{max} it clearly holds for all $\ell = 1,\dots,h-1$.
3. **1** of Def.1 for R_1 and (3) imply for $\ell = 1,\dots,h$ that

$$\|\mathbf{b}_1\|^2 \le \gamma_k\mathcal{D}_1^{1/k} \le \gamma_k((1+\varepsilon)^{\frac{1+1/k}{2}}\gamma_k)^{\frac{2k(\ell-1)}{k-1}}\mathcal{D}_\ell^{1/k}. \tag{5}$$

The product of these h inequalities for $\ell = 1, ..., h$ yields

$$\|\mathbf{b}_1\|^{2h} \le \gamma_k^h ((1+\varepsilon)^{\frac{1+1/k}{2}} \gamma_k)^{\frac{kh(h-1)}{k-1}} (\det \mathcal{L})^{2/k}.$$

Hence the claim $\quad \|\mathbf{b}_1\|^2/(\det \mathcal{L})^{2/n} \le \gamma_k \big((1+\varepsilon)^{\frac{1+1/k}{2}} \gamma_k\big)^{\frac{n-k}{k-1}} \le \big((1+\varepsilon)^{\frac{1+1/k}{2}} \gamma_k\big)^{\frac{n-1}{k-1}}$. □

Strong asr-bases. We call an asr-basis $B \in \mathbb{R}^{m\times hk}$ strong if **2** of Def. 1 holds for $\ell = h-1$ and **1** of Def. 1 holds for R_{h-1} and R_h.

Most likely, we obtain a strong asr-basis from any asr-basis by $O(k \ln k/\varepsilon)$ **ASR**-rounds with $\ell = h-1$ and $\ell = \ell_{max}$ that can possibly change B. This takes at most $\frac{k^2}{k-1}(1 + \log_{1+\varepsilon} \gamma_k)$ **ASR**-rounds with $\ell = h-1$ because $\mathcal{D}_{h-1}/\mathcal{D}_h \le ((1+\varepsilon)\gamma_k)^{\frac{2k^2}{k-1}}$ holds for any asr-basis and each round with $\ell = h-1$ decreases $\mathcal{D}_{h-1}/\mathcal{D}_h$ by a factor $(1+\varepsilon)^{-2}$. Similarly we can transform an asr-basis B into a slide-reduced basis by iterating **ASR**-rounds that can possibly change B. Most likely this takes only $O(n \ln k/\varepsilon)$ **ASR**-rounds, much fewer than to transform an LLL-basis into an asr-basis.

Theorem 3. *Every strong asr-basis $B = [\mathbf{b}_1, ..., \mathbf{b}_n]$ for $\varepsilon \ge 0, k \ge 2$, $n = hk$ satisfies*

$$\|\mathbf{b}_1\| \le (1+\varepsilon)^{\frac{1+1/k}{2}} \gamma_k)^{\frac{n-k}{k-1}} \lambda_1$$

provided that some $\mathbf{b} \in \mathcal{L}(B) \setminus \mathcal{L}(\mathbf{b}_1, ..., \mathbf{b}_{n-k})$ satisfies $\|\mathbf{b}\| = \lambda_1$.

Proof. (5) for $\ell = h-1$ shows that $\qquad \|\mathbf{b}_1\|^2 \le \gamma_k \big((1+\varepsilon)^{\frac{1+1/k}{2}} \gamma_k\big)^{\frac{2kh-4k}{k-1}} \mathcal{D}_{h-1}^{1/k}$.

Clearly **2** for $\ell = h-1$ implies (2) and (4) for $\ell = h-1$, and thus we get

$$\|\mathbf{b}_1\|^2 \le \gamma_k \big((1+\varepsilon)^{\frac{1+1/k}{2}} \gamma_k\big)^{\frac{2kh-4k}{k-1}} \big((1+\varepsilon)\gamma_k\big)^{\frac{2}{k-1}} {\mathcal{D}'_{h-1}}^{1/k} \qquad \text{(by (4) for } \ell = h-1)$$

$$\le \gamma_k \big((1+\varepsilon)^{\frac{1+1/k}{2}} \gamma_k\big)^{\frac{2kh-4k}{k-1}} \big((1+\varepsilon)\,\gamma_k\big)^{\frac{2}{k-1}+1} r^2_{n-k+1,n-k+1}$$

(by **1, 2** for $\ell = h-1$ and the Hermite bound for $R'^{\bigstar}_{h-1}$ we have ${\mathcal{D}'_{h-1}}^{1/k} \le (1+\varepsilon)\gamma_k\, r^2_{n-k+1,n-k+1}$)

$$\le \big((1+\varepsilon)^{\frac{1+1/k}{2}} \gamma_k\big)^{2\frac{n-k}{k-1}} r^2_{n-k+1,n-k+1}. \qquad \text{(since } 1 + \tfrac{2}{k-1} < \tfrac{2k}{k-1} \text{ for } k \ge 2)$$

The theorem assumes that $\|\mathbf{b}\| = \lambda_1$ holds for some $\mathbf{b} \in \mathcal{L} \setminus \mathcal{L}([\mathbf{b}_1, ..., \mathbf{b}_{n-k}])$. Hence $r_{n-k+1,n-k+1} \le \|\pi_{n-k+1}(\mathbf{b})\| \le \lambda_1$. The latter inequalities yield the claim.

We have decreased the exponent 1 of $(1+\varepsilon)$ in **3** and **4** to $\frac{1+1/k}{2} \approx 1/2$ for large k. □

Iterative almost slide-reduction with increasing blocksize. Consider the blocksize $k = 2^j$. We transform a given LLL-basis $B \in \mathbb{Z}^{m\times n}$ for δ, α, $n = hk$ iteratively as folllows:

FOR $i = 1, ..., j$ DO transform B by calling **ASR** with blocksize 2^i and ε.

The final **ASR**-call with blocksize $k = 2^j$ dominates the overall workload of all **ASR**-calls of the iteration, including the workload for the LLL-reduction of the input basis, due to the dominating workload of local SVP-computations in dimension k.

We bound the number $\#It$ of rounds of the last **ASR**-call with blocksize $k = 2^j$. Importantly, the input B of this final **ASR**-call satisfies $\quad \mathcal{D}_\ell/\mathcal{D}_{\ell+1} \le ((1+\varepsilon)\gamma_{k/2})^{\frac{2k^2}{k/2-1}} \quad$ as follows from (3) with blocksize $k/2$ and $\frac{1+2/k}{2} \le 1$ for $k \ge 2$. In fact we have that $\mathcal{D}_\ell/\mathcal{D}_{\ell+1} \le \max_\ell(\mathcal{D}_{\ell,k/2}/\mathcal{D}_{\ell+1,k/2})^4$, where $\mathcal{D}_{\ell,k/2} = (\det R_{\ell,k/2})^2$ for the ℓ-th block $R_{\ell,k/2}$ of blocksize $k/2$ of the input basis B. Hence

$$\mathcal{D}(B) \le ((1+\varepsilon)\gamma_{k/2})^{\frac{2k^2}{k/2-1}\frac{h^3-h}{6}}$$

holds for the input B. As each round prior to termination decreases $\mathcal{D}(B)$ by a factor $(1+\varepsilon)^{-2}$ the number $\#It$ of rounds of the last **ASR**-call is bounded as

$$\#It \le \tfrac{1}{2} \log_{1+\varepsilon} \mathcal{D}(B) \le \tfrac{k^2}{k/2-1} \tfrac{h^3-h^2-h}{6} \log_{1+\varepsilon}((1+\varepsilon)\gamma_{k/2})$$
$$< \tfrac{1}{3} \tfrac{nh^2}{1-2/k} \log_{1+\varepsilon}((1+\varepsilon)\gamma_{k/2}),$$

provided that $\mathcal{D}(B) \ge 1$ holds on termination. This proves

Corollary 1. *Given an almost slide-reduced-basis $B \in \mathbb{Z}^{m\times n}$ for $\varepsilon > 0$ and blocksize $k/2$, $n = hk$,* **ASR** *finds within $\frac{1}{3}\frac{nh^2}{1-2/k}\log_{1+\varepsilon}((1+\varepsilon)\gamma_{k/2})$ rounds of three local SVP-computations an asr-basis of blocksize k and ε unless it terminates with $\mathcal{D}(B) < 1$.*

This shows that the upper bound on the number of rounds of **ASR** with blocksize k and ε of Theorem 1 decreases for $\varepsilon \le 0.01$ and $\alpha \approx 4/3$ by a factor

$$4/((1-2/k)k)\ln\alpha/\ln((1+\varepsilon)\gamma_{k/2}) \approx 4(k-2)^{-1}\ln\gamma_{k/2}/\ln(4/3)$$

if the input basis B is an asr-basis with blocksize $k/2$. For $k = 32$ this is less than half the bound from Theorem 1, where the input is an LLL-basis for δ, α. Here we assume that $\gamma_{16} \approx 2\sqrt{2}$. Moreover, within only half of these rounds **ASR** achieves $\mathcal{D}(\mathbf{B}) \le \big((1+\varepsilon)\gamma_k\big)^{\frac{2k^2}{k-1}\frac{h^3-h}{6}}$, a bound on the final $\mathbf{B}$ that follows from (3). Interestingly, this bound on $\mathcal{D}(\mathbf{B})$ is sharp on the average.

Fast slide-reduction for extremely small ε. Instead of running **ASR** with a very small ε and some k on an input LLL-basis it is faster to first run **ASR** for some $\varepsilon' > \varepsilon$ and $k' > k$ such that

$$((1+\varepsilon)\gamma_k)^{k'-1} > ((1+\varepsilon')\gamma_{k'})^{k-1}. \tag{6}$$

Then perform on this asr-basis **ASR**-rounds for ε, k for such ℓ that the **ASR**-round can possibly change B, and terminate when B can no more change. (6) implies that the upper bound **3** on $\|\mathbf{b}_1\|/(\det\mathcal{L})^{1/n}$ is smaller for an asr-basis with ε', k' than for an asr-basis with ε, k. This suggests that there are most likely only a few **ASR**-rounds for ε, k.

.

Lemma 1. *Any asr-basis $B = [\mathbf{b}_1, ..., \mathbf{b}_n] \in \mathbb{Z}^{m\times n}$ for $\varepsilon < 1/M_0^{2n}$, $M_0 := \max(\|\mathbf{b}_1\|^2, ..., \|\mathbf{b}_n\|^2)$, is asr-basis for $\varepsilon = 0$.*

Proof. Let $\varepsilon > 0$ be minimal such that B is asr-basis for ε, k. We see from the proof of (3) that the inequality **2** of Def. 1 holds with equality for some $\ell = \ell_{max}$. Consider an artificial **ASR**-round performed on B with $\ell = \ell_{max}$ resulting in $r^{new}_{k\ell+1,k\ell+1} = \max_{R'^T_\ell} r_{k\ell+1,k\ell+1}$. Let $\mathbf{D}_\ell := (\det[\mathbf{b}_1, ..., \mathbf{b}_{k\ell}])^2 \in \mathbb{Z}$ denote the value before and $\mathbf{D}^{new}_\ell$ after this round. Then $\mathbf{D}^{new}_\ell < \mathbf{D}_\ell$ because $\det R_\ell$ decreases in that round. Importantly, the values $(r_{k\ell+1,k\ell+1})^2\mathbf{D}_\ell, (r^{new}_{k\ell+1,k\ell+1})^2\mathbf{D}^{new}_\ell$ before and after this round are integers – this claim is analogous to [LLL82,(1.28)]. As **2** of Def. 1 holds with equalty we have $(r^{new}_{k\ell+1,k\ell+1})^2 = (1+\varepsilon)\,(r_{k\ell+1,k\ell+1})^2$ and thus

$$\varepsilon,\ (r_{k\ell+1,k\ell+1})^2,\ (r^{new}_{k\ell+1,k\ell+1})^2 \in \mathbb{Z}/(\mathbf{D}_\ell\mathbf{D}^{new}_\ell).$$

Hence $\varepsilon \ge 1/(\mathbf{D}_\ell\mathbf{D}^{new}_\ell) \ge 1/M_0^{2n-2k}$ since $\mathbf{D}^{new}_\ell < \mathbf{D}_\ell \le M_0^{k\ell} \le M_0^{n-k}$. Therefore, the minimality of ε implies that either $\varepsilon = 0$ or $\varepsilon > 1/M_0^{2n}$. This proves the claim. □

Improving worst case slide-reduced bases. We characterize slide-reduced bases for k and $\varepsilon = 0$ for which $\|\mathbf{b}_1\|/\lambda_1$ is maximal. A shortest lattice vector can easily be found for such a basis.

Theorem 4. *Let the basis $R = \mathrm{GNF}(R) = [\mathbf{b}_1, ..., \mathbf{b}_n] \in \mathbb{R}^{n\times n}$, $n = hk$ be slide-reduced for k and $\varepsilon = 0$. If $\|\mathbf{b}_1\|/\lambda_1 = \gamma_k^{\frac{n-k}{k-1}}$ then there exists $\mathbf{b}_{min} \in 0^{n-k}\mathbb{R}^k \cap \mathcal{L}(R)$ with $\|\mathbf{b}_{min}\| = \lambda_1$. Any such $\mathbf{b}_{min}$ can be found from its projection $\pi_{n-k+1}(\mathbf{b}_{min})$ in $O(n^2)$ arithmetic steps.*

Proof. Let $R = [r_{i,j}] \in \mathbb{R}^{n\times n}$ then $\pi_{n-k+1}\,\mathcal{L}(R) = \mathcal{L}([[r_{i,j}]_{n-k<i,j\le n})$ is a lattice of dimension k. By (2)the slide-reduced R satisfies

$$r_{k\ell-k+1,k\ell-k+1} \le \gamma_k^{\frac{1}{k-1}} r_{k\ell+1,k\ell+1} \quad \text{for } \ell = 1, ..., h-1.$$

Therefore $\|\mathbf{b}_1\|/\lambda_1 = \gamma_k^{\frac{n-k}{k-1}}$ implies $\|\mathbf{b}_{min}\| = r_{n-k+1,n-k+1}$. Hence $\pi_{n-k+1}(\mathbf{b}_{min})$ is a shortest nonzero vector of $\pi_{n-k+1}\,\mathcal{L}(R)$ of length $r_{n-k+1,n-k+1}$. Therefore $\mathbf{b}_{min} \in 0^{n-k}\mathbb{R}^k \cap \mathcal{L}(R)$. Let $\mathbf{b}_{min} = \sum_{i=1}^n t_i\mathbf{b}_i$. Then, given $\sum_{i=n-k+1}^n t_i\mathbf{b}_i$ we find $t_{n-k}, ..., t_1 \in \mathbb{Z}$ from the equations

$$t_j r_{j,j} + \cdots + t_{n-k} r_{j,n-k} + \sum +i = m-k+1^n t_i r_{j,i} = 0$$

for $j = n-k, ..., 1$. This proves the Theorem. □

Note that we find all $\mathbf{b}_{min} \in 0^{n-k}\mathbb{R}^k \cap \mathcal{L}(R)$ by enumerating the shortest vectors of $\pi_{n-k+1}\,\mathcal{L}(R)$ and trying to extend them to some $\mathbf{b}_{min} \in 0^{n-k}\mathbb{R}^k \cap \mathcal{L}(R)$. In particular, uf the shortest vector $\pm\mathbf{b}$ of $\pi_{n-k+1}\,\mathcal{L}(R)$ is unique, which is most likely the case, then we find $\mathbf{b}_{min} \in 0^{n-k}\mathbb{R}^k \cap \mathcal{L}(R)$ by an **SVP**-computation of dimension k in $O(n^2)$ arithmetic steps that compute $t+1, ..., y_{n-k} \in \mathbb{Z}$.

Conclusion. Given a slide-reduced basis $R \in \mathbb{R}^{n\times n}$ with blocksize k and $\varepsilon = 0$ for which $\|\mathbf{b}_1\|/\lambda_1$ is maximal we can easily find a shortest vector of $\mathcal{L} * R)$. More generally, this suggests that the closer $\|\mathbf{b}_1\|/\lambda_1$ is to the maximumf or slide-reduced bases of dimension n and blocksize k the easier it is to find a nonzero lattice vector $\mathbf{b}$ that is substantially shorter than $\mathbf{b}_1$.

Such short $\mathbf{b}$ can be found by random sampling reduction [S03]. This method transforms a given basis$R = \mathrm{GNF}(R) = [r_{i,j}] = [\mathbf{b}_1, ..., \mathbf{b}_n] \in \mathbb{R}^{n\times n}$ by checking for sufficiently many integer combinations $\bar{\mathbf{b}} = \sum_{i=n}^{n} t_i \mathbf{b}_i$ whether size-reduction of $\bar{\mathbf{b}}$ versus $\mathbf{b}_1, ...\mathbf{b}_{n-u-1}$ yields a vector $\mathbf{b}$ that is shorter than $\mathbf{b}_1$. By Theorem 1 of [S03] this method finds under reasonable assumptions a basis such that $\|\mathbf{b}_1\|/\lambda_1 \le (k/6)^{\frac{n}{2k}}$ within time $O(n^2(k/6)^{k/4})$. Random sampling reduction of [S03] seems to outperform slide-reduction which produces a basis such that $\|\mathbf{b}_1\|/\lambda_1 \le ((1+\varepsilon)\gamma_k)^{\frac{n-k}{k-1}}$ in time $O(n^2 k^{\frac{k}{2e}(1+o(1))})$. Random sample reduction of [S03] is complementary to slide-reduction in that it largely improves slide-reduced bases for which $\|\mathbf{b}_1\|/\lambda_1$ is maximal. It makes sense to alternate the two reduction methods iteratively as the two methods rely on independent principles.

Improving worst case LLL-bases. We translate Theorem 4 to LLL-bases with $\delta = 1$. These bases are slide-reduced for $k = 2$ and $\varepsilon = 0$ and thus $\|\mathbf{b}_1\|^2 \le (\frac{4}{3})^{n-2}\lambda_1^2$ holds by Theorem 3 since $\gamma_3^2 = \frac{4}{3}$. If $\|\mathbf{b}_1\|^2 = (\frac{4}{3})^{n-2}\lambda_1^2$ then by Theorem 4 a shortest lattice vector can be found by size-reducing a combination of the last two basis vectors:

Theorem 5. *Let $R = \mathrm{GNF}(R) \in \mathbb{R}^{n\times n}$ be an LLL-basis for $\delta = 1$. If $\|\mathbf{b}_1\|^2 = (\frac{4}{3})^{n-2}\lambda_1^2$, i.e., $\|\mathbf{b}_1\|/\lambda_1$ is maximal, then there exists $\mathbf{b}_{min} = (0, ..., 0, \pm r_{n-1,n-1}, r_{n,n})^t \in \mathcal{L}(R)$ of length $\|\mathbf{b}_{min}\| = \lambda_1$ and such $\mathbf{b}_{min}$ can be found in $O(n^2)$ arithmetic steps.*

Accelerating LLL-reduction (ALR). We accelerate LLL-reduction by performing either local Gauß-reductions, i.e., LLL-reductions with $\delta = 1$, or LLL-swaps on $\mathbf{b}_\ell, \mathbf{b}_{\ell+1}$ for an ℓ that maximizes $\|\mathbf{b}_\ell\|/\|\pi_\ell(\mathbf{b}_{\ell+1})\|$ and thus promises maximal reduction progress.

We value the reduction of the basis B satisfying $\max_\ell \|\mathbf{b}_\ell^*\|^2/\|\mathbf{b}_{\ell+1}^*\|^2 > \frac{4}{3}$ the integer μ defined by

$$2^{2^{\mu-1}} < \max_\ell \|\mathbf{b}_\ell^*\|^2/\|\mathbf{b}_{\ell+1}^*\|^2/\tfrac{4}{3} \le 2^{2^\mu}. \tag{7}$$

ALR iterates the following loop:

`WHILE` the loop changes B `DO`
`IF` $\mu \ge 0$ `THEN` for an ℓ that maximizes $\|\mathbf{b}_\ell^*\|/\|\mathbf{b}_{\ell+1}^*\|$ LLL-reduce $\pi_\ell(\mathbf{b}_\ell), \pi_\ell(\mathbf{b}_{\ell+1})$ with $\delta = 1$. (this is a Gauß-reduction of $\pi_\ell(\mathbf{b}_\ell), \pi_\ell(\mathbf{b}_{\ell+1})$)
`ELSE` choose an ℓ that after the size-reduction $\mathbf{b}_{\ell+1} := \mathbf{b}_{\ell+1} - \lceil r_{\ell,\ell+1}/r_{\ell,\ell}\rfloor \mathbf{b}_\ell$ maximizes $\|\mathbf{b}_\ell^*\|^2/\|\pi_\ell(\mathbf{b}_{\ell+1})\|^2$. If $\|\pi_\ell(\mathbf{b}_{\ell+1})\|^2 \le \delta\|\mathbf{b}_\ell^*\|^2$ swap $\mathbf{b}_\ell$, $\mathbf{b}_{\ell+1}$ and size-reduce $\mathbf{b}_\ell$, $\mathbf{b}_{\ell+1}$ against $\mathbf{b}_1, ..., \mathbf{b}_{\ell-1}$. `end while`
`termination` size-reduce the basis B to satisfy $|r_{i,j}| \le \frac{1}{2} r_{i,i}$ for all $j > i$.

Theorem 6. *Given an LLL-basis $B \in \mathbb{Z}^{m\times n}$ for $\delta' < 1$, $\alpha' = 1/(\delta' - 1/4)$* **ALR** *with δ such that $1 > \delta > \max(\delta', \frac{1}{2})$ terminates within $\frac{n^3}{12}\log_{1/\delta}\alpha'$ rounds of local Gauß-reductions, resp. LLL-swaps at an LLL-basis for δ, unless it arrives at $\mathcal{D}(B) := \prod_{\ell=1}^{n-1}(\|\mathbf{b}_\ell^*\|^2/\|\mathbf{b}_{\ell+1}^*\|^2)^{n\ell-\ell^2} < 1$.*

Theorem 6 proves that the number of rounds of **ALR** is $O(n^3)$ for input LLL-bases of arbitrary quality δ, α, a bound that is independent of size(B), whereas the number of rounds for the original LLL-algorithm [LLL82] is merely polynomial in size(B).

Proof. We use $\mathcal{D}(B)$ for blocksize 1, $\mathcal{D}(B) := \prod_{\ell=1}^{n-1}(\|\mathbf{b}_\ell^*\|^2/\|\mathbf{b}_{\ell+1}^*\|^2)^{\ell(n-\ell)}$. Each round decreases $\|\mathbf{b}_\ell^*\|^2$ by a factor δ, and both $\|\mathbf{b}_\ell^*\|^2/\|\mathbf{b}_{\ell+1}^*\|^2$, $\mathcal{D}(B)$ by a factor δ^2. Then the number of rounds until either an LLL-basis for δ appears or else $\mathcal{D}(B) \le 1$ is at most

$$\tfrac{1}{2}\log_{1/\delta}\mathcal{D}(B) \le \tfrac{1}{2}\log_{1/\delta}(\alpha')^{\frac{n^3-n}{6}} \le \tfrac{n^3}{12}\log_{1/\delta}\alpha'. \qquad \square$$

The workload per round. If each round completely size-reduces $\mathbf{b}_\ell, \mathbf{b}_{\ell+1}$ against $\mathbf{b}_1, ..., \mathbf{b}_{\ell-1}$ it requires $O(n^2)$ arithmetic steps. If we only size-reduce $\mathbf{b}_{\ell+1}$ against $\mathbf{b}_\ell$ then a round costs merely $O(n)$ arithmetic steps but the length of the integers might explode. This explosion can be prevented at low costs by doing size-redction in segments, see [S06], [KS01]. Note that the bit complexity of the round can be made quasi-linear in size(B) by the method of [NSV10]: perform the arithmetic steps of the round on the leading bits of the entries of the basis matrix using fast integer arithmetic.

Corollary 2. *The μ-value (7) of the input basis satisfies $\mu \le \log_2 n + \log_2\log_2 M_0$, let $c \in \mathbb{Z}$ $c \ge 0$ be constant. Within $\frac{2n^3}{3}(\mu + 2^c)$ rounds* **ALR** *either decreases the initial μ to $\mu \le -c$ or else arrives at $\mathcal{D}(B) < 1$. This number of rounds is polynomial in n if $\log_2\log_2 M_0 \le n^{O(1)}$.*

Proof. As initially $\frac{4}{3}\,2^{2^{\mu-1}} \le \max_\ell \|\mathbf{b}_\ell^*\|^2/\|\mathbf{b}_{\ell+1}^*\|^2 \le \frac{4}{3}\,2^{2^\mu}$ Each round of **ALR** with $\ell = \ell_{max}$ decreases $\|\mathbf{b}_\ell^*\|^2/\|\mathbf{b}_{\ell+1}^*\|^2$ by a factor $2^{-2^{\mu-1}}$, where μ is the initial value of the round. Following the fact in the proof of Theorem 1 this decreases $\mathcal{D}(B) =_{def} \prod_{\ell=1}^{n-1}(\|\mathbf{b}_\ell^*\|^2/\|\mathbf{b}_{\ell+1}^*\|^2)^{n\ell-\ell^2}$ for $k=1$ as $\mathcal{D}(B^{new})/\mathcal{D}(B^{old}) \le 2^{-2^{\mu-1}}$. This bounds the number $\#It_\mu$ of **ALR**-rounds for the reduction of μ to $\mu - 1$ to

$$\#It_\mu \le \tfrac{n^3-n}{3}(2^\mu + \log_2\tfrac{4}{3})/2^{\mu-1}$$

unless **ALR** arrives at $\mathcal{D}(B) < 1$. Similarly **ALR** decreases the μ of the input-basis within at most

$$\tfrac{n^3}{3}(2(\mu+c) + \log_2\tfrac{4}{3}\sum_{i=-c}^{\mu}2^{-i+1}) < \tfrac{2n^3}{3}(\mu + c + 2^{c+1}\log_2\tfrac{4}{3}) < \tfrac{2n^3}{3}(\mu + \cdot 2^c)$$

rounds to $-|c|$ unless it arrives at $\mathcal{D}(B) < 1$.

The bound $\mu \le \log_2 n + \log_2\log_2 M_0$ follows from (7) and $\|\mathbf{b}_{\ell+1}^*\|^2 \ge 1/M_0^{2n}$. $\square$

LLL-reduction for extremely small $1-\delta$. It follows from Cor. 2 that LLL-reduction with $\delta = 1$ is in polynomial time $n^{O(1)}$ if $\log_2 \text{size}(B) = n^{O(1)}$. For this first compute an LLL-basis for $\delta = 3/4$, transform it into a strong asr-basis for $k = 3$ and $\varepsilon = 0.07$. As $\gamma_2^2 > 1.07\,\gamma_3$ the proven bound for $\|\mathbf{b}_1\|/(\det\mathcal{L})^{1/n}$ is smaller for this asr-basis then for an LLL-basis with $\delta = 1$. Transform the asr-basis by iterating **ALR**-rounds with $\varepsilon = 0$ that can possibly change B. The work load of the latter **ALR**-roads should be negligible compared to the previous reductions.

Next we study LLL-reduction for extremely small $1-\delta$ by block reduction of dimension 2.

Lemma 2. *Every LLL-basis $B = [\mathbf{b}_1, ..., \mathbf{b}_n]$ for $\delta > 1 - 1/M_0^{2n}$, $M_0 := \max(\|\mathbf{b}_1\|^2, ..., \|\mathbf{b}_n\|^2)$, is LLL-basis for $\delta = 1$ and thus $\max_\ell \|\mathbf{b}_\ell^*\|^2/\|\mathbf{b}_{\ell+1}^*\|^2 \le \frac{4}{3}$.*

Proof. Follow the proof of Lemma 1 for $\varepsilon = 1-\delta$. Let δ be maximal such that B is LLL-basis for δ. Consider the effect of an artificial **ALR**-round with $\ell = \ell_{max}$ that maximizes $r_{\ell,\ell}^2/r_{\ell+1,\ell+1}^2$ performed on the LLL-basis B for $\delta < 1$ and resulting in $(r_{\ell,\ell}^{new})^2 = \delta r_{\ell,\ell}^2$. This holds as δ is maximal such that B is LLL-basis for δ. Then

$$\mathbf{D}_\ell = (\det[\mathbf{b}_1, ..., \mathbf{b}_\ell])^2 \in \mathbb{Z}, \quad r_{\ell,\ell}^2\mathbf{D}_{\ell-1}, \ (r_{\ell,\ell}^{new})^2\,\mathbf{D}_{\ell-1}^{new} \in \mathbb{Z}$$

$1-\delta \ge 1/(\mathbf{D}_{\ell-1}\mathbf{D}_{\ell-1}^{new}) > 1/M_0^{2n-2}$, and thus $1-\delta < 1/M_0^{2n}$ implies $\delta = 1$. $\square$

Comparison with previous algorithms for LLL-reduction. The original LLL for $\delta = \frac{3}{4}$ [LLL82] has bit-complexity $O(n^{5+\varepsilon}(\log_2 M_0)^{2+\varepsilon})$ performing $O(n^2\log_{1/\delta}M_0)$ rounds, each round size-reduces some $\mathbf{b}_\ell$ in n^2 arithmetic steps on integers of bit-length $n\log_2 M_0$; ε in the exponent comes from the fast FFT-multiplication of integers. The $n\log_2 M_0$ bit-length of integers has been reduced to $n + \log_2 M_0$ by orthogonalizing the basis in floating point arithmetic. The LLL-time can be reduced by 10 - 15 % by successively increasing δ from $3/4, 7/8, 15/16, 31/32, 63/64$ to 0.99.

To minimize the workload of size-reduction **ALR** should be organized according to segment reduction of [KS01], [S06] doing most of the size-reductions locally on segments of k basis vectors. The bit-complexity of Gauß-reduction of $\pi_\ell(\mathbf{b}_\ell), \pi_\ell(\mathbf{b}_{\ell+1})$ is quasi-linear in the bit-length of

$\mathbf{b}_\ell, \mathbf{b}_{\ell+1}$ [NSV10]. Therefore we do not split up this LLL-reduction into LLL-swaps. Gauß-reduction of $\pi_\ell(\mathbf{b}_\ell), \pi_\ell(\mathbf{b}_{\ell+1})$ for $\ell = \ell_{max}$ decreases $\mathcal{D}(B)$ by the factor $2^{-2^{\mu}-1}$ while LLL-swaps guarantee only a decrease by the factor $\frac{3}{4}$.

A result that is very close to Cor. 2 and Cor. 3 has been proved independently in Lemma 12 of [HPS11]: $\max_\ell \|\mathbf{b}_\ell^*\|^2/\|\mathbf{b}_{\ell+1}^*\|^2 \leq \frac{4}{3} + \varepsilon$ can be achieved in polynomial time $n^{O(1)}\mathrm{size}(B)^{1+o(1)}$ for arbitrary $\varepsilon > 0$ by block reduction of dimension 2.

Early Termination (ET). Terminate as soon as $\mathcal{D}(B) < (\frac{4}{3})^{\frac{n^3-n}{6}}$.

$\mathcal{D}(B) < \frac{4}{3})^{\frac{n^3-n}{6}}$ implies that $\mathbf{E}[\ln(\|\mathbf{b}_\ell^*\|^2/\|\mathbf{b}_{\ell+1}^*\|^2)] < \ln(4/3)$ holds for random ℓ and $\mathbf{Pr}(\ell) = 6\,\frac{\ell h = \ell^2}{h^3-h^2-h}$. In this sense the output basis approximates "on the average" the logarithm of the inequality $\|\mathbf{b}_1\|/(\det\mathcal{L})^{1/n} \leq (\frac{4}{3})^{\frac{n-1}{4}}$ that holds for ideal LLL-bases with $\delta = 1$.

Corollary 3. **ALR** *terminates under* **ET** *in* $n^3(\mu + |\mu_0|)/3$ *rounds, where* μ, μ_0 *are the* μ*-values of the input and output basis. Moreover* $|\mu_0| \leq n \log_2 M_0$ *and* $\mu \leq \log_2 n + \log_2\log_2 M_0$.

Proof. Consider the number $\#It_\mu$ of rounds until either the current μ decreases to $\mu - 1$ or else $\mathcal{D}(B)$ becomes less than $(4/3)^{\frac{n^3-n}{6}}$. As in the proof of Corollary 2 each round with μ results in Gauß-reduction under π_ℓ if $\mu \geq 0$, resp. an LLL-swap if $\mu < 0$, results in

$$\|\mathbf{b}_\ell^{*new}\|^2 < \|\mathbf{b}_\ell^{*old}\|^2 2^{-2^{\mu}-2} \qquad \text{hence} \qquad \mathcal{D}(B^{new}) < \mathcal{D}(B^{old})2^{-2^{\mu}-1}.$$

Under **ET** this shows as in the proof of Cor. 1 that

$$\#It_\mu < \log_2(\mathcal{D}(B^{(in)})/(\mathcal{D}(B^{(fin)}))/2^{\mu-1} \leq (2^{\mu}\tfrac{n^3-n}{6})/2^{\mu-1} = \tfrac{n^3-n}{3}.$$

Hence μ decreases to $\mu - 1$ under **ET** in less than $\frac{n^3-n}{3}$ rounds. The proof of Lemma 1 shows that $|m_0| \leq n\log_2 M_0$. □

Open problem. Does **ALR** realize $\max_\ell \|\mathbf{b}_\ell\|^2/\|\mathbf{b}_{\ell+1}\|^2 \leq \frac{4}{3}$ in a polynomial number of rounds ? Can **ALR** perform for $\mu \ll 0$ without **ET** more than $O(n^3)$ rounds until either the current μ decreases to $\mu - 1$ or that $\mathcal{D}(B) \leq 1$? We can exclude this for $\mu \geq 0$ and under **ET** also for $\mu < 0$.

References

[GHKN] *N. Gama, N. Howgrave-Graham, H. Koy and P, Q. Nguyen*, Rankin's constant and blockwise lattice reduction. In Proc. of CRYPTO'06, LNCS 4117, Springer, pp. 112–130, 2006.

[GN08] *N. Gama and P. Nguyen*, Finding Short Lattice Vectors within Mordell's Inequality, In Proc. of the ACM Symposium on Theory of Computing **STOC'08**, pp. 208–216, 2008.

[GN08b] *N. Gama and P.Q. Nguyen*, Predicting lattice reduction, in Proc. EUROCRYPT 2008, LNCS 4965, Springer-Verlag, pp. 31–51, 2008.

[HPS11] *G. Hanrot, X. Pujol and D. Stehlé*, Terminating BKZ, Cryptology ePrint Archive, Report 198, 2011, personal communication 21.2.2011, final version in Proc. CRYPTO'11, LNCS 6841, Springer-Verlag, 2011.

[KS01] *H. Koy and C.P. Schnorr* Segment LLL-reduction of lattice bases, In *Proceedings of the 2001 Cryptography and Lattice Conference (CACL'01)*, LNCS 2146, Springer-Verlag, pp. 67-80, 2001.

[LLL82] *H.W. Lenstra Jr., A.K. Lenstra and L. Lovász*, Factoring polynomials with rational coefficients, Mathematische Annalen 261, pp. 515–534, 1982.

[NSV10] *A. Novocia, D. Stehlé and G. Villard* An LLL-reduction algorithm with quasilinear time complexity. Technical Report, version 1, Nov. 2010.

[S87] *C.P. Schnorr*, A hierarchy of polynomial time lattice basis reduction algorithms. *Theoret. Comput. Sci.*, **53**, pp. 201–224, 1987.

[S03] *C.P. Schnorr*, Lattice reduction by sampling and birthday methods. Proc. STACS 2003: 20th Annual Symposium on Theoretical Aspects of Computer Science, LNCS 2007, Springer-Verlag, pp. 146–156, 2003. //www.mi.informatik.uni-frankfurt.de

[S06] *C.P. Schnorr*, Fast LLL-type lattice reduction, *Information and Computation* 204, pp. 1–25, 2006.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de