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

Accelerated 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

April 8, 2011

Abstract. Given an LLL-basis B of dimension $n = hk$ we accelerate slide-reduction with blocksize k to run under a reasonable assjmption in $\frac{1}{6}\,n^2h\,\log_{1+\varepsilon}\,\alpha$ local SVP-computations in dimension k, where $\alpha \geq \frac{4}{3}$ measures 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 $k/2$ then the number of local SVP-computations for slide-reduction with blocksize k reduces to $\frac{2}{3}h^3(1+\log_{1+\varepsilon}\gamma_{k/2})$. This bound is polynomial for arbitrary bit-length of B, it improves previous bounds considerably. 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. $\lambda_1(\mathcal{L}) = \min_{\mathbf{b}\in\mathcal{L},\mathbf{b}\neq\mathbf{0}}(\mathbf{b}^t\mathbf{b})^{1/2}$ 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 $k \geq 2$ generalising 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 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 $O(nh\cdot\text{size}(B)/\varepsilon)$ 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 all the other workload. [NSV10] show that the bit complexity of LLL-reduction is quasi-linear in size(B). To obtain this quasi-linear bit-complexity 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 $O(nh\cdot\text{size}(B)/\varepsilon)$ bound of [GN08b] in two ways. We concentrate the required conditions for slide-reduced bases in the concept of *almost slide-reduced bases* which enables faster reduction. We study the algorithm for slide-reduction on input bases that are LLL-bases. As LLL-reduction takes a minor part of the workload of slide-reduction this better characterizes the intrinsic workload of slide-reduction. Theorem 1 studies the number of local SVP-computations for slide-reduction with blocksize k of 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 $\frac{1}{6}\,n^2h\,\log_{1+\varepsilon}\,\alpha$. This bound holds for arbitrary bit-length of B. Corollary 1 shows that if the given basis is already slide-reduced for blocksize $k/2$ the number of local SVP-computations for slide-reduction with blocksize k further decreases to $\frac{1}{3}\,\frac{1}{1-2/k}h^3(1+\log_{1+\varepsilon}\gamma_{k/2})$, reducing the number by a factor $2k^{-2}\ln\gamma_{k/2}/\ln\alpha$. For the first time this qualifies the advantage of first performing slide-reduction with half the blocksize.

ISSN 1433-8092

Theorem 2 shows that the bounds proven in [GN08b] on $\|\mathbf{b}_1\|/\lambda_1$ and $\|\mathbf{b}_1\|/(\det \mathcal{L})^{1/n}$ still hold for almost slide-reduced bases even with a minor improvement.

We also accelerate LLL-reduction. Corollary 3 shows, under a reasonable assumption, that accelerated LLL-reduction computes an LLL-basis within $\frac{n^3}{12}\log_2 \mathrm{size}(B)$ local LLL-reductions in dimension 2. The number of local LLL-reductions in dimension 2 is polynomial in n if the bit-length of B is at most exponential in n, i.e., $\mathrm{size}(B) = 2^{n^{O(1)}}$. Lemma 2 shows that every LLL-basis for δ such that $1-\delta \leq 2^{-n-2}2^{-\mathrm{size}(B)}$ satisfies the property $\max_\ell \|\mathbf{b}_\ell^*\|^2/\|\mathbf{b}_{\ell+1}^*\|^2 \leq \frac{4}{3}$ of ideal LLL-bases for $\delta = 1$.

Notation. Let $B = QR$, $n = hk$ be the QR-decomposition of $B \in \mathbb{R}^{m\times n}$. Let $R_\ell = [r_{i,j}]_{k\ell-k+1\leq i,j\leq k\ell} \in \mathbb{R}^{k\times k}$ be the submatrix of $R = [r_{i,j}] \in \mathbb{R}^{n\times n}$ for the ℓ-th block, $\mathcal{D}_\ell = (\det R_\ell)^2$, and $R'_\ell = [r_{i,j}]_{k\ell-k+2\leq i,j\leq k\ell+1} \in \mathbb{R}^{k\times k}$ for the ℓ-th block slided by one unit. $R'^*_\ell = (R'_\ell)^*$ is the dual of R'_ℓ. ($R^*_k = U_k R_k^{-t} U_k$ for $R_k \in \mathbb{R}^{k\times k}$, where R_k^{-t} is the inverse transpose of R_k and $U_k \in \{0,1\}^{k\times k}$ is the reversed identity matrix with non-zero entries $u_{i,k-i+1} = 1$ for $i = 1, ..., k$.) Let $\max_{R'_\ell T} r_{k\ell+1,k\ell+1}$ denote the maximum of $\bar{r}_{k\ell+1,k\ell+1}$, $[\bar{r}_{i,j}] := \mathrm{GNF}(R'_\ell T)$ for all $T \in \mathrm{GL}_k(\mathbb{Z})$ with QR-decomposition $R'_\ell T = Q' \cdot \mathrm{GNF}(R'_\ell T)$. Note that $\max_{R'_\ell T} r_{k\ell+1,k\ell+1} = 1/\lambda_1(\mathcal{L}(R'^*_\ell))$. 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, $\frac{1}{4} < \delta \leq 1$ if

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

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

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

Definition 1. [GN08] *An LLL-basis $B = QR \in \mathbb{R}^{m\times n}$, $n = kh$ is* slide-reduced *for $\varepsilon \geq 0$ if*

1. $r_{k\ell-k+1,k\ell-k+1} = \lambda_1(\mathcal{L}(R_\ell))$ *for* $\ell = 1, ..., h$,

2. $\max_{R'_\ell T} r_{k\ell+1,k\ell+1} \leq \sqrt{1+\varepsilon}\cdot r_{k\ell+1,k\ell+1}$ *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. $\|\mathbf{b}_1\| \leq ((1+\varepsilon)\gamma_k)^{\frac{1}{2}\frac{n-1}{k-1}} (\det \mathcal{L})^{1/n}$, **4.** $\|\mathbf{b}_1\| \leq ((1+\varepsilon)\gamma_k)^{\frac{n-k}{k-1}} \lambda_1$.

Almost slide-reduced bases. We call an LLL-basis $B = QR \in \mathbb{R}^{m\times n}$, $n = hk$, *almost slide-reduced* for $\varepsilon \geq 0$ if for some $\ell = \ell_{max}$ that maximizes $\mathcal{D}_\ell/\mathcal{D}_{\ell+1}$,

1. $r_{k\ell-k+1,k\ell-k+1} = \lambda_1(\mathcal{L}(R_\ell))$ for $\ell = 1$ and $\ell = \ell_{max}$,

2. $\max_{R'_\ell T} r_{k\ell+1,k\ell+1} \leq \sqrt{1+\varepsilon}\cdot r_{k\ell+1,k\ell+1}$ holds for $\ell = \ell_{max}$ and $\ell = h-1$.

Theorem 2 shows that the bounds **3, 4** hold for almost slide-reduced bases.

Accelerated slide-reduction (ASR). In each round find some $\ell = \ell_{max}$ that maximizes $\mathcal{D}_\ell/\mathcal{D}_{\ell+1}$. Compute a shortest vector of $\mathcal{L}(R_{\ell+1})$ and transform $R_{\ell+1}$ and B such that $r_{k\ell+1,k\ell+1} = \lambda_1(\mathcal{L}(R_{\ell+1}))$. By an SVP-computation for $\mathcal{L}(R'^*_\ell)$ check that **2** holds for ℓ and if **2** does not hold transform R'_ℓ and B such that **2** holds for $\varepsilon = 0$ (this decreases $\mathcal{D}_\ell$ by a factor $\leq (1+\varepsilon)^{-1}$) otherwise terminate.

On termination continue with this transform on $R_\ell, R_{\ell+1}, B$ for $\ell = \ell_{max}$ and $\ell = h-1$ until **2** holds for both $\ell = \ell_{max}$ and $\ell = h-1$. Finally make sure that **1** holds for $\ell = 1$ and size-reduce B.

Theorem 1. *Accelerated slide-reduction transforms a given LLL-basis $B \in \mathbb{Z}^{m\times n}$ for $\delta \leq 1$, $\alpha = 1/(\delta - 1/4)$, $n = hk$, within $\frac{1}{12}n^2 h \log_{1+\varepsilon}\alpha = n^2 h \frac{1+O(\varepsilon)}{12\cdot\varepsilon}\ln\alpha$ rounds of 2 local SVP-computations either into an almost slide-reduced basis for $\varepsilon > 0$, or else arrives at $\mathcal{D}(B) < 1$, where*

$$\mathcal{D}(B) =_{\mathrm{def}} \prod_{\ell=1}^{h-1} (\mathcal{D}_\ell/\mathcal{D}_{\ell+1})^{h\ell-\ell^2} = (\det \mathcal{L})^{2h} / \prod_{i=1}^{h}\prod_{j=i}^{h} \mathcal{D}_j^2.$$

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

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

Fact. Each round that does not lead to termination results in

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

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

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

rounds either B is almost slide-reduced for ε or else $\mathcal{D}(B) \le 1$. The $\frac{n^2h}{12}\log_{1+\varepsilon}\alpha$ bound includes the rounds on termination. Clearly $\log_{1+\varepsilon}\alpha = \ln\alpha/\ln(1+\varepsilon)$ and $1/\ln(1+\varepsilon) = \frac{1+O(\varepsilon)}{\varepsilon}$. □

Conjecture. We conjecture that $\mathcal{D}(B) < 1$ does not appear for output bases obtained after a maximal number of rounds. 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 $\mathbf{Pr}(\ell) = 6\frac{\ell h-\ell^2}{h^3-h}$. (We have $\sum_{\ell=1}^{h-1}\mathbf{Pr}(\ell) = 1$.) 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 in practice.

Time bound compared to [GN08]. The algorithm for slide-reduction of [GN08] is shown to perform $O(nh\,\mathrm{size}(B)/\varepsilon)$ local SVP-computations, where size(B) is the bit-length of B. The number of rounds of Theorem 1 is polynomial in n even if size(B) is exponential in n.
However, **ASR** can accelerate the [GN08] algorithm at best by a factor $h-1$ because the [GN08] algorithm iterates all rounds for $\ell = 1, ..., h$ which also covers ℓ_{max}, whereas **ASR** iterates all rounds for the current ℓ_{max}. Thus Theorem 1 shows that the [GN08] algorithm performs at most $\frac{n^2h^2}{6}\log_{1+\varepsilon}\alpha$ local SVP-computations if the input basis is an LLL-basis for δ and the algorithm terminates with a basis B such that $\mathcal{D}(B) \ge 1$. Theorem 1 eliminates from the $O(nh\,\mathrm{size}(B)/\varepsilon)$ time bound of [GN08] the bitlength of B and requires only minor conditions on the input and output basis. As size$(B) \approx \sum_{i=1}^n \log_2\|\mathbf{b}_i\|$ our $\frac{n^2h^2}{6}\log_{1+\varepsilon}\alpha$ bound is better than the $O(nh\,\mathrm{size}(B)/\varepsilon)$ bound of [GN08] if $\frac{h}{6}\ln\alpha < \frac{1}{n}\sum_{i=1}^n \log_2\|\mathbf{b}_i\|$. The latter holds in most cases.

Iterative slide-reduction with increasing blocksize. Consider the blocksize $k = 2^j$. We transform the 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.

We bound the number $\#It$ of rounds of the last **ASR**-call with blocksize $k = 2^j$. The input B of this final **ASR**-call satisfies $\mathcal{D}_\ell/\mathcal{D}_{\ell+1} \le ((1+\varepsilon)\gamma_{k/2})^{\frac{k/2}{k/2-1}4}$ as follows from (3) with blocksize $k/2$. Hence $\mathcal{D}(B) \le ((1+\varepsilon)\gamma_{k/2})^{\frac{2k}{k/2-1}\frac{h^3-h}{6}}$.
As each round decreases $\mathcal{D}(B)$ by a factor $(1+\varepsilon)^{-2}$ we see that

$$\#It \le \tfrac{1}{2}\log_{1+\varepsilon}\mathcal{D}(B) \le \tfrac{k}{k/2-1}\tfrac{h^3-h}{6}\log_{1+\varepsilon}((1+\varepsilon)\gamma_{k/2}) = \tfrac{h^3-h}{1-2/k}\tfrac{1+O(\varepsilon)}{3\cdot\varepsilon}\ln\gamma_{k/2}$$

provided that $\mathcal{D}(B) \ge 1$ holds on termination. Here $\log_{1+\varepsilon}\gamma_{k/2} = \ln\gamma_{k/2}/\ln(1+\varepsilon) = \frac{1+O(\varepsilon)}{\varepsilon}\gamma_{k/2}$. For $k = 4$, resp. $k = 8$ this is less than a 0.603, resp. 0.201 fraction of the number of rounds $\frac{n^2h}{12}\log_{1+\varepsilon}\alpha$ of Theorem 1, where the input is an LLL-basis for δ, α. The final **ASR**-call dominates the workload of all other calls together, including the workload for the LLL-reduction of the input basis. We see that iterative slide-reduction for $k = 2^j$ requires only an $O(k^{-2}\ln\gamma_{k/2})$-fraction of the workload of the direct **ASR**-call as in Theorem 1. In particular we have proved

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 $\frac{1}{3}\frac{h^3-h}{(1-2/k)}\log_{1+\varepsilon}((1+\varepsilon)\gamma_{k/2})$ rounds of two local SVP-computations either an almost slide-reduced basis for blocksize k and ε or else arrives at $\mathcal{D}(B) < 1$.*

Theorem 2. *The bounds* **3, 4** *hold for every almost slide-reduced basis $B \in \mathbb{Z}^{m\times n}$ and the exponent of $(1+\varepsilon)$ in* **3, 4** *can roughly be halved, multiplying it by $\frac{1+1/k}{2}$.*

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

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

holds for $\ell = \ell_{max}$ and $\ell = h-1$, where $\mathcal{D}'_\ell := (\det R'_\ell)^2$. Moreover, the Hermite bound for R_ℓ yields

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

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

$$r_{k\ell-k+1,k\ell-k+1} \le ((1+\varepsilon)\gamma_k)^{\frac{k}{k-1}} r_{k\ell+1,k\ell+1} \quad \text{for } \ell = \ell_{max} \text{ and } \ell = h-1. \tag{2}$$

Next we prove

$$\mathcal{D}_\ell/\mathcal{D}_{\ell+1} \le ((1+\varepsilon)^{\frac{1+1/k}{2}} \gamma_k)^{\frac{2k^2}{k-1}} \quad \text{for } \ell = 0, ..., h-1. \tag{3}$$

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

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

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

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 $\ell = 1, ..., h-1$.

3. The Hermite bound for R_1 and (3) imply for $\ell = 1, ..., h$ 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

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

This proves and improves **3** to (without using that **2** holds for $\ell = h-1$.)

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

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

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

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

$$\le \gamma_k ((1+\varepsilon)^{\frac{1+1/k}{2}} \gamma_k)^{\frac{2kh-4k+2}{k-1}} (1+\varepsilon) \gamma_k r^2_{n-k+1,n-k+1}. \qquad \text{(by } \mathbf{2} \text{ for } \ell = h-1)$$

(we also used that $r^{-2}_{n-k+1,n-k+1} = \lambda_1^2(\mathcal{L}(R'^*_{h-1})) \le \gamma_k / D'_{h-1}$ holds by the Hermite bound for R'^*_{h-1}.)

$$< ((1+\varepsilon)^{\frac{1+1/k}{2}} \gamma_k)^{2\frac{n-k}{k-1}} r^2_{n-k+1,n-k+1}.$$

W.l.o.g $\pi_{n-k+1}(\mathbf{b}) \neq \mathbf{0}$ holds for some $\mathbf{b} \in \mathcal{L}$ with $\|\mathbf{b}\| = \lambda_1$, otherwise we remove the last k vectors of the basis. Hence $r_{n-k+1,n-k+1} \le \|\pi_{n-k+1}(\mathbf{b})\| \le \lambda_1$. The latter inequalities yield the claim

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

We have roughly halved the exponent of $(1+\varepsilon)$ in **3** and **4** multiplying it by at most $\frac{1+1/k}{2}$. □

Time bounds for extremely small ε. We measure the reducedness of a basis B by the integer m defined by

$$2^{2^{m-1}} < \max_\ell(\mathcal{D}_\ell/\mathcal{D}_{\ell+1}) \, \gamma_k^{-\frac{2k^2}{k-1}} \le 2^{2^m}. \tag{6}$$

This integer m exists if and only if $\max_\ell(\mathcal{D}_\ell/\mathcal{D}_{\ell+1}) > \gamma_k^{\frac{2k^2}{k-1}}$

Next we show that every round of **ASR** with initial value m decreases $\mathcal{D}(B)$ by a factor $2^{-2^{m-1}}$. The transform of $R_\ell, R_{\ell+1}, B$ for $\ell = \ell_{max}$ results in (2), (3) holding f or $\varepsilon = 0$, i.e., $\mathcal{D}^{new}_\ell/\mathcal{D}^{new}_{\ell+1} \le \gamma_k^{\frac{2k^2}{k-1}}$.

Multiplying this inequality with $2^{2^{m-1}} \gamma_k^{\frac{2k^2}{k-1}} < \mathcal{D}^{old}_\ell/\mathcal{D}^{old}_{\ell+1}$ and $\mathcal{D}^{new}_\ell \mathcal{D}^{new}_{\ell+1} = \mathcal{D}^{old}_\ell \mathcal{D}^{old}_{\ell+1}$ yields

$$2^{2^{m-2}}\mathcal{D}_\ell^{new} \le \mathcal{D}_\ell^{old} \qquad \text{hence} \qquad \mathcal{D}(B^{new}) \le \mathcal{D}(B^{old})\, 2^{-2^{m-1}}. \tag{7}$$

We denote $M_0 := \max(\|\mathbf{b}_1\|^2, ..., \|\mathbf{b}_n\|^2)$ for the input basis B.

Lemma 1. *If B is almost slide-reduced for $\varepsilon < \frac{k-1}{6k^2}/(2^n M_0)$ then* $\max_\ell(\mathcal{D}_\ell/\mathcal{D}_{\ell+1}) \le \gamma_k^{\frac{2k^2}{k-1}}$.

Proof. Let $\varepsilon > 0$ be minimal such that B is almost slide-reduced for ε. It follows from the proof of Theorem 1 that $\mathcal{D}_\ell/\mathcal{D}_{\ell+1} = ((1+\varepsilon)\gamma_k)^{\frac{2k^2}{k-1}}$ holds for some ℓ. Then (6) implies $(1+\varepsilon)^{\frac{k^2}{k-1}} \le 2^{2^m}$, thus

$$\varepsilon < \tfrac{k-1}{k^2}\, 2^m. \tag{8}$$

If $B = QR$ is not almost slide-reduced for some $0 < \varepsilon' < \varepsilon$ then any nearly maximal such ε' satisfies

$$\max_{R'_\ell T} r_{k\ell+1,k\ell+1} \approx (1+\varepsilon')r_{k\ell+1,k\ell+1} \quad \text{for some } \ell.$$

It follows from [LLL82, (1.28)] for the integer matrix B that $r_{k\ell+1,k\ell+1}M_0^n \ge 1$ and thus

$$\varepsilon' \gtrsim (\max_{R'_\ell T} r_{k\ell+1,k\ell+1} - r_{k\ell+1,k\ell+1})/r_{k\ell+1,k\ell+1} \ge 1/M_0^n.$$

This contradicts (8) if $\frac{k-1}{k^2}\, 2^m < 1/M_0^n$, and thus excludes that $-m > n\log_2 M_0$.

(3) and (6) imply $2^{2^{m-1}} < (1+\varepsilon)^{\frac{2k^2}{k-1}}$, and thus $\qquad 2^{m-1} < \frac{2k^2}{k-1}\log_2(1+\varepsilon) < \frac{2k^2}{k-1}\frac{\varepsilon}{\ln 2}$.

Hence $-m > n\log_2 M_0$ which is impossible. This implies by (6) that $\max_\ell \mathcal{D}_\ell/\mathcal{D}_{\ell+1} \le \gamma_k^{\frac{2k^2}{k-1}}$. □

Next we bound the number $\#It_m$ of rounds until the current m either decreases to $m-1$ or arrives at $\mathcal{D}(B) < 1$. During this reduction the m defined by (6) implies that (7) holds for each round. Moreover, initially $\max_\ell \mathcal{D}_\ell/\mathcal{D}_{\ell+1} \le \gamma_k^{\frac{2k^2}{k-1}} 2^{2^m}$. This shows for the initial and final bases for the reduction of m to $m-1$:

$$\begin{aligned}\#It_m &\le \log_2(\mathcal{D}(B^{(in)})/\mathcal{D}(B^{(fin)}))/2^{m-1}\\ &\le \tfrac{h^3-h}{3}(2^m/2^{m-1} + 2^{-m+1}\tfrac{2k^2}{k-1}\log_2\gamma_k).\end{aligned}$$

Thus within $O(nh^2\log_2 k)$ rounds **ASR** either decreases $m \ge 0$ to $m-1$ or arrives at $\mathcal{D}(B) < 1$.

Open problem. Can **ASR** perform for $m \ll 0$ more than $O(nh^2\log_2 k)$ rounds until either the current m decreases to $m-1$ or that $\mathcal{D}(B) < 1$? We can exclude this by the following rule of

Early Termination (ET). Terminate as soon as $\mathcal{D}(B) < \gamma_k^{\frac{2k^2}{k-1}\frac{h^3-h}{6}}$.

$\mathcal{D}(B) < \gamma_k^{\frac{2k^2}{k-1}\frac{h^3-h}{6}}$ implies that $\mathbf{E}[\ln(\mathcal{D}_\ell/\mathcal{D}_{\ell+1})] < \frac{2k^2}{k-1}\ln\gamma_k$ holds for random ℓ, where $\mathbf{Pr}(\ell) = 6\frac{\ell h = \ell^2}{h^3-h}$. In this sense (3), (4) and **3** hold for $\varepsilon = 0$ "on the average".

Corollary 2. ASR *terminates under* **ET** *for arbitrary $\varepsilon \ge 0$ in $\frac{h^3-h}{3}(m + |m_0|)$ rounds, where m, m_0 are the m-value of the input and final basis. Moreover $|m_0| \le n\log_2 M_0$.*

Proof. Consider $\#It_m$ the number of rounds until the current m decreases to $m-1$. During this reduction the m of (6) satisfies $\max_\ell \mathcal{D}_\ell/\mathcal{D}_{\ell+1} > 2^{2^{m-1}}\gamma_k^{\frac{2k^2}{k-1}}$. This implies by (7) and **ET** for the initial and final bases for the reduction of m to $m-1$:

$$\#It_m \le \log_2(\mathcal{D}(B^{(in)})/\mathcal{D}(B^{(fin)}))/2^{m-1} \le \log_2(2^{2^m\frac{h^3-h}{6}})/2^{m-1} = \tfrac{h^3-h}{3}.$$

Thus within $\frac{h^3-h}{3}$ rounds **ASR** either decreases m to $m-1$ or arrives at $\mathcal{D}(B) < \gamma_k^{\frac{2k^2}{k-1}\frac{h^3-h}{3}}$.

Hence **ASR** terminates within $\frac{h^3-h}{3}(m + |m_0|)$ rounds, where $|m_0| \le n\log_2 M_0$ holds by the proof of Lemma 1. □

Accelerated LLL-reduction (ALR). We accelerate LLL-reduction by performing either Gauß-reductions or LLL-swaps on $\mathbf{b}_\ell, \mathbf{b}_{\ell+1}$ for an ℓ that maximizes the resulting reduction progress.

We associate to a basis B satisfying $\max_\ell \|\mathbf{b}_\ell^*\|^2/\|\mathbf{b}_{\ell+1}^*\|^2 > \frac{4}{3}$ the integer m defined by

$$2^{2^{m-1}} < \max_\ell \|\mathbf{b}_\ell^*\|^2/\|\mathbf{b}_{\ell+1}^*\|^2/\tfrac{4}{3} \le 2^{2^m}. \tag{9}$$

If $m \ge 0$ we transform in the current round $\mathbf{b}_\ell, \mathbf{b}_{\ell+1}$ for an ℓ that maximizes $\|\mathbf{b}_\ell^*\|^2/\|\mathbf{b}_{\ell+1}^*\|^2$ by Gauß-reducing the basis $\pi_\ell(\mathbf{b}_\ell), \pi_\ell(\mathbf{b}_{\ell+1})$ of dimension 2. (Gauß-reducing the basis $\pi_\ell(\mathbf{b}_\ell), \pi_\ell(\mathbf{b}_{\ell+1})$ means to LLL-reduce $\pi_\ell(\mathbf{b}_\ell), \pi_\ell(\mathbf{b}_{\ell+1})$ with $\delta = 1$.) This decreases $\|\mathbf{b}_\ell^*\|^2$ by a factor less than $2^{-2^m} < \frac{1}{2}$.

If $m < 0$ or m does not exist, we transform in the current round $\mathbf{b}_\ell, \mathbf{b}_{\ell+1}$ for an ℓ that maximizes $\|\mathbf{b}_\ell^*\|^2/\|\pi_\ell(\mathbf{b}_{\ell+1}^*)\|^2$ after size-reducing $\mathbf{b}_{\ell+1}$ against $\mathbf{b}_\ell$ by setting $\mathbf{b}_{\ell+1} := \mathbf{b}_{\ell+1} - \lceil r_{\ell,\ell+1}/r_{\ell/\ell} \rfloor \mathbf{b}_\ell$. If $\|\pi_\ell(\mathbf{b}_{\ell+1}^*)\|^2 \le \delta \|\mathbf{b}_\ell^*\|^2$ we swap $\mathbf{b}_\ell$, $\mathbf{b}_{\ell+1}$ and otherwise terminate.

On termination we size-reduce the basis B.

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

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 explodes. This explosion can be prevented at low costs by doing size-redction in segments, see [S06], [KS01].

Lemma 2. *If B is LLL-basis for δ and $1 - \delta < 2^{-n-2}/M_0$ then $\max_\ell \|\mathbf{b}_\ell^*\|^2/\|\mathbf{b}_{\ell+1}^*\|^2 \le \frac{4}{3}$.*

Proof. The LLL-basis B satisfies $\|\mathbf{b}_\ell^*\|^2 \le \frac{1}{\delta - 1/4} \|\mathbf{b}_{\ell+1}^*\|^2$. Therefore (9) implies $2^{2^{m-1}} < \frac{1}{\delta-1/4} \frac{3}{4}$. Setting $\delta = 1 - \varepsilon$ this shows that

$$\begin{aligned} 2^{m-1} &< \log_2 \tfrac{3}{4\delta-1} < \log_2 \tfrac{1}{1-\frac{4}{3}\varepsilon} = \ln(1 - \tfrac{4}{3}\varepsilon)/\ln 2 \\ &< -1.45\, \tfrac{4}{3}\varepsilon < 2^{-n-1}/M_0. \end{aligned}$$

This implies $m < -n \log_2 M_0$ which is impossible (by the proof of Lemma 1). This shows that m is undefined and thus $\max_\ell \|\mathbf{b}_\ell^*\|^2/|\mathbf{b}_{\ell+1}^*\|^2 \le \frac{4}{3}$. $\square$

Corollary 3. *Let m be the m-value of the input basis and $c \in \mathbb{Z}$ $c \ge 0$ be constant. Within $\frac{n^3}{12}(m + 2.22 \cdot 2^c)$ rounds* **ALR** *either decreases the initial m to $m \le -c$ or else arrives at $\mathcal{D}(B) < 1$. Moreover $m \le \log_2 n + \log_2 \log_2 M_0$.*

Surprisingly, the number of rounds in Cor. 3 is polynomial in n if $\log_2 \log_2 M_0 \le n^{O(1)}$.

Proof. We have shown that **ASR** with $k = 2$ either decreases within at most

$$\tfrac{(n/2)^3}{3} \,(2^m/2^{m-1} + 2^{-m+1} 8 \log_2 \sqrt{4/3})$$

rounds either the current m to $m - 1$ or arrives at $\mathcal{D}(B) < 1$. Therefore **ALR** either decreases the m of the input-basis within at most

$$\tfrac{n^3}{24}(2m + 2^4 \log_2 \sqrt{4/3} \textstyle\sum_{i=-c}^m 2^{-i}) < \tfrac{n^3}{12}(m + 2^{c+4} \log_2 \sqrt{4/3}) < \tfrac{n^3}{12}(m + 2.22 \cdot 2^c)$$

rounds to $m = -|c|$ or else arrives at $\mathcal{D}(B) < 1$

The bound $m \le \log_2 n + \log_2 \log_2 M_0$ follows from (9) and $\|\mathbf{b}_{\ell+1}^*\|^2 \ge 1/M_0^n$. $\square$

Comparison with previous algorithms for LLL-reduction. The LLL was originally proved [LLL82] to be of 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 large bit-length of integers $n \log_2 M_0$ has been reduced to $n + \log_2 M_0$ by orthogonalizing the basis in floating point arithmetic.

The number of rounds in Cor. 3 is independent of M_0. This is because**ALR** maximizes the reduction progress per round. 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 $\pi_\ell(b_\ell), \pi_\ell(b_{\ell+1})$ is quasi-linear in size(B) [NSV10]. Therefore we do not split up this Gauss-reduction into LLL-swaps. If the current m is large then Gauß-reduction of $\pi_\ell(b_\ell), \pi_\ell(b_{\ell+1})$ for $\ell = \ell_{max}$ decreases $\mathcal{D}(B)$ be the factor 2^{-m} while LLL-swaps guarantee only a decrease by the factor $\frac{3}{4}$.

The algorithm for LLL-reduction with fixed complexity iterates all possible LLL-swaps of $\mathbf{b}_\ell, \mathbf{b}_{\ell+1}$ for $\ell = 1, ..., n-1$. If this algorithm would not just do LLL-swaps but Gauss-reductions of $\pi_\ell(\mathbf{b}_\ell), \pi_\ell(\mathbf{b}_{\ell+1})$ for all ℓ its number of rounds would be at most $n-1$ times the number of rounds $\frac{n^3}{12}\log_{1/\delta}\alpha'$ of **ALR**.

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 $\mathbf{Pr}(\ell) = 6\,\frac{\ell h = \ell^2}{h^3-h}$. 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 4. **ALR** *terminates under* **ET** *in* $n^3(m+|m_0|)/3$ *rounds, where* m, m_0 *are the m-values of the input and output basis. Moreover* $|m_0| \leq n\log_2 M_0$ *and* $m \leq \log_2 n + \log_2\log_2 M_0$.

Proof. Consider the number $\#It_m$ of rounds until either the current m decreases to $m-1$ 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 m results in Gauß-reduction under π_ℓ if $m \geq 0$, resp. an LLL-swap if $m < 0$, results in

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

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

$$\#It_m < \log_2(\mathcal{D}(B^{(in)})/(\mathcal{D}(B^{(fin)}))/2^{m-1} \leq (2^m\,\frac{n^3-n}{6})/2^{m-1} = \frac{n^3-n}{3}.$$

Hence m decreases to $m-1$ 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 $m \ll 0$ without **ET** more than $O(n^3)$ rounds until either the current m decreases to $m-1$ or that $\mathcal{D}(B) \leq 1$? We can exclude this for $m \geq 0$ and under **ET** also for $m < 0$.

References

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

[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.

[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.

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

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

ECCC ISSN 1433-8092

http://eccc.hpi-web.de