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

August 21, 2011

Abstract. Given an LLL-basis \( B \) of dimension \( n = hk \) we accelerate slide-reduction with blocksize \( k \) to run under a reasonable assumption within \( \frac{1}{k} n^2 h \log_{1+\epsilon} \alpha \) local SVP-computations of dimension \( n \), where \( \alpha \geq \frac{1}{k} \) measures the quality of the given LLL-basis and \( \epsilon \) is the quality of slide-reduction. If the given basis \( B \) is already slide-reduced for blocksize \( k/2 \) the \( \frac{1}{k} n^2 h \log_{1+\epsilon} \alpha \) bound further decreases to \( \frac{2^h}{h^3} (1 + \log_{1+\epsilon} \gamma_k/2) \). This bound is polynomial in \( n \) 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 \( B = [b_1,...,b_n] \in \mathbb{R}^{n \times n} \) of \( n \) linear independent vectors \( b_1,...,b_n \) generates the lattice \( L(B) = \{Bx \mid x \in \mathbb{Z}^n \} \) of dimension \( n \). Lattice reduction algorithms transform a given basis into a basis consisting of short vectors. \( \lambda_1(L) = \min_{b \in L, b \neq 0} \|b\| \) is the minimal length of nonzero \( b \in L \). The determinant of \( L \) is \( \det L = (\det B)^{1/n} \). The Hermite bound \( \lambda_1(L)^2 \leq \gamma_n(\det L)^{2/n} \) holds for all lattices \( L \) of dimension \( n \) and the Hermite constant \( \gamma_n \).

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 \( \hat{B} \) such that \( \|b_1\| \leq \frac{n+1}{n \log \lambda_1} \lambda_1 \), where \( \alpha > 4/3 \). It is important to minimize the proven bound on \( \|b_1\|/\lambda_1 \) 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. Schönherr [S87] introduced blockwise HKZ-reduction. The algorithm of [GHK06] improves blockwise HKZ-reduction by blockwise primal-dual reduction. So far slide-reduction of [GN08b] yields the smallest approximation factor \( \|b_1\|/\lambda_1 \leq ((1 + \epsilon)\gamma_k)^{\frac{1}{2 + \epsilon}} \) of polynomial time reduction algorithms. The algorithm for slide-reduction of [GN08b] performs \( O(nh \cdot \text{size}(B)/\epsilon) \) local SVP-computations, where size\( (B) \) is the bit-length of \( B \) and \( \epsilon \) 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\( (B) \). 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 \( O(nh \cdot \text{size}(B)/\epsilon) \) 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 maximal number of local SVP-computations for slide-reduction with blocksize \( k \) of an input LLL-basis \( B \in \mathbb{Z}^{m \times n} \) for \( \delta, \alpha \) and dimension \( n = hk \). It shows under a reasonable assumption that this number is at most \( \frac{1}{k} n^2 h \log_{1+\epsilon} \alpha \). 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 \( k \) decreases to \( \frac{1}{k} n^2 h \cdot \log_{1+\epsilon} \alpha \) bound by a factor \( 2k^{1-2} \log_{1+\epsilon} \gamma_k/2 \). For the first time this qualifies the advantage
of first performing slide-reduction with half the blocksize. Theorem 2 shows that the bounds proven in [GN08b] on $\|b_i\|/\lambda_1$ and $\|b_i\|/(\det L)^{1/n}$ 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 $\frac{\sqrt{n}}{12} \log_2 \text{size}(B)$ local LLL-reductions of dimension 2. The $\frac{\sqrt{n}}{12} \log_2 \text{size}(B)$ bound is polynomial in $n$ if the bit-length of $B$ is at most exponential in $n$, size($B$) = $2^{\Omega(1)}$. Lemma 2 shows that every LLL-basis for $\delta$ such that $1 - \delta \leq 2^{-n - 2\cdot \text{size}(B)}$ satisfies the property $\max \|b_i\|^2/\|b_{i+1}\|^2 \leq \frac{1}{2}$ of ideal LLL-bases for $\delta = 1$.

**Notation.** Let $B = QR$, $n$ be $hk$ be the QR-decomposition of $B \in \mathbb{R}^{m \times n}$, where $R = [r_{i,j}]_{1 \leq i,j \leq n} \in \mathbb{R}^{n \times n}$ is upper triangular with positive diagonal entries $r_{i,i} > 0$ and $Q \in \mathbb{R}^{m \times n}$ is isometric with orthogonal column vectors of length 1. We denote GNF($B$) = $R$. Let $R_\ell = [r_{i,j}]_{k\ell-1 \leq i,j \leq k\ell} \in \mathbb{R}^{k \times k}$ be the submatrix of $R = [r_{i,j}]_{1 \leq i,j \leq n} \in \mathbb{R}^{n \times n}$ for the $\ell$-th block of blocksize $k$, $D_\ell = (\det R_\ell)^2$, and $R_\ell' = [r_{i,j}]_{k\ell-k\ell+2 \leq i,j \leq k\ell+1} \in \mathbb{R}^{k \times k}$ be the $\ell$-th block slid by one unit. $R_\ell' = U_k R_\ell T_k = U_k R_\ell' T_k$ is the inverse transpose of $R_\ell$ and $U_k = \{0,1\}^{k \times k}$ is the reversed identity matrix with non-zero entries $u_{i,k-1} = 1$ for $i = 1, ..., k$. $R_\ell' = (R_\ell')^k$ is the dual of $R_\ell$. Let $k \geq 2$.

Let $\max_{R_\ell' T_{k\ell-k\ell+1}} r_{k\ell-k\ell+1}$ denote the maximum of $r_{k\ell-k\ell+1}$; $\max_{R_\ell' T_{k\ell-k\ell+1}}[i,j] := \text{GNF}(R_\ell' T_{k\ell-k\ell+1})$ for all $T \in \text{GL}_k(\mathbb{Z})$. Note that $\max_{R_\ell' T_{k\ell-k\ell+1}} 1/\lambda_1(L(R_\ell'))$. Let $\pi_i : \mathbb{R}^n \rightarrow \text{span}(b_1,...,b_{i-1})^1$ be the orthogonal projection, and $b_i' := \pi_i(b_i)$ thus $\|b_i\|^2 = \|b_i\|^2$. LLL-bases. LLL82 A basis $B \in \mathbb{R}^{m \times n}$ is LLL-basis for $\delta$, $\frac{1}{2} < \delta \leq 1$, $\alpha = 1/\left(1 - \frac{1}{4}\right)$ if

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

An LLL-basis $B$ for $\delta$ satisfies $\|b_i\|^2/\|b_{i+1}\|^2 \leq \alpha$ for all $\ell = 1, ..., n - 1$ and $\|b_1\| \leq \alpha^{1/2} (\det L)^{1/n}$, $\|b_i\| \leq \alpha^{\ell/2} \lambda_1$.

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

1. $r_{k\ell-k\ell+1,k\ell-k\ell+1} = \lambda_1(L(R_{\ell}'))$ for $\ell = 1, ..., h$,
2. $\max_{R_{\ell}T_{k\ell-k\ell+1}} r_{k\ell-k\ell+1} \leq \sqrt{1 + \varepsilon} \cdot r_{k\ell-k\ell+1}$ holds for $\ell = 1, ..., h - 1$.

$\varepsilon$ slightly relaxes the condition of [GN08] that all bases $R_\ell$ are HKZ-reduced. The following bounds have been proved by GAMA and NGUYEN in [GN08, Theorem 1] for slide-reduced bases:

- $\|b_1\| \leq (\varepsilon/\gamma_k)^{1/2} (\det L)^{1/n}$,
- $\|b_1\| \leq (\varepsilon/\gamma_k)^{1} (\det L)^{1/n}$,
- $\|b_1\| \leq (\varepsilon/\gamma_k)^{1/2} (\det L)^{1/n}$,
- $\|b_1\| \leq (\varepsilon/\gamma_k)^{1} (\det L)^{1/n}$.

Almost slide-reduced bases. We call an LLL-basis $B = QR \in \mathbb{R}^{m \times n}$, $n = hk$, almost slide-reduced for $\varepsilon \geq 0$ and blocksize $k$ if for some $\ell = \ell_{\text{max}}$ that maximizes $D_\ell/D_{\ell+1}$ we have that

1. $r_{k\ell-k\ell+1,k\ell-k\ell+1} = \lambda_1(L(R_{\ell}'))$ for $\ell = 1$ and $\ell = \ell_{\text{max}}$,
2. $\max_{R_{\ell}T_{k\ell-k\ell+1}} r_{k\ell-k\ell+1} \leq \sqrt{1 + \varepsilon} \cdot r_{k\ell-k\ell+1}$ holds for $\ell = \ell_{\text{max}}$ and $\ell = h - 1$.

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

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

On termination continue with this transform on $R_\ell$, $R_{\ell+1}$, $B$ for $\ell = \ell_{\text{max}}$ and $\ell = h - 1$ until 2 holds for both $\ell = \ell_{\text{max}}$ 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 $\delta \leq 1$, $\alpha = 1/\left(6 - 1/4\right)$, $n = hk$, with $\frac{\sqrt{n}}{12} n^2 \text{size}(B) \leq \alpha n^2 h \log_2(\alpha)$. In $\alpha$ rounds of 2 local SVP-computations either into an almost slide-reduced basis for $\varepsilon > 0$ and blocksize $k$, or else arrives at $D(B) < 1$, where

$D(B) = \det \left( \prod_{\ell=1}^k (D_{\ell}/D_{\ell+1})^{\delta_{\ell-\ell}} \right)^{1/2} = (\det L)^{1/h} \prod_{\ell=1}^h D_{\ell}$. 

2
Proof. We use the novel version $D(B)$ 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 $\ell = [h/2] = [h/2 - 1/2]$

The input LLL-basis $B^{(m)}$ for $\delta \leq 1$ satisfies for $\alpha = 1/(\delta - 1/4)$ that $D_i/D_{i+1} \leq \alpha k^2$ and thus $D(B^{(m)}) \leq \alpha k^2$. As $\sum_{\ell=1}^{h-1} h\ell - \ell^2 = \frac{h^3 - h^2 - h}{6}$.

Fact. Each round on $\ell = \ell_{max}$ that does not lead to termination results in

$$D_{new}^\ell \leq D_{i}/(1 + \varepsilon) \leq D(B)/(1 + \varepsilon)^2.$$

This is because the round changes merely the factor $D_{t-1}/D_{t+1} = (D_i D_{t+1})^{D_{(h-t)}} = (D_i D_{t+1})^h \leq D(B)$. We use the novel version $D(B)$ of Def. 1 and the Hermite bound on $\gamma_{k/2}$.

Conjecture. We conjecture that $D(B) < 1$ does not appear for output bases obtained after a maximal number of rounds. If $D(B) < 1$ then $E[\ln(D_i/D_{i+1})] < 0$ holds for the expectation $E$ for random $\ell$ with $\Pr(t) = \frac{6\gamma_k}{k^3 - 3k - 2}\frac{k}{k}$. We have $\sum_{t=1}^{1/2} \Pr(t) = 1$. In this sense $D_i < D_{i+1}$ would hold “on the average” if $D(B) < 1$, whereas such $D_i$, $D_{i+1}$ are extremely unlikely in practice.

Time bound compared to [GN08]. The algorithm for slide-reduction of [GN08] has been shown to perform $O(nh \text{size}(B)/\varepsilon)$ 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 $n$.

Note that ASR can accelerate the [GN08] algorithm at best by a factor $h$ because the [GN08] algorithm corrects $\ell_{max}$ by iterating all rounds for $\ell = 1, ..., h$, whereas ASR iterates exclusively on the current $\ell_{max}$. Theorem 1 decreases the $O(nh \text{size}(B)/\varepsilon)$ bound of [GN08] to $\frac{n^2h}{\varepsilon} \log_{1+\varepsilon} \alpha$ and requires only minor conditions on the input and output basis. In general it decreases the $nh \text{size}(B)/\varepsilon$ bound of [GN08] by the factor $\frac{1}{\varepsilon} \ln \alpha/\text{size}(B) = \Theta(1/(6 \max \log \|b_{i}\|))$.

Iterative slide-reduction with increasing blocksize. Consider the blocksize $k = 2^l$. We transform the given LLL-basis $B \in \mathbb{Z}^{m \times n}$ for $\delta, \alpha, n = h k$ iteratively as follows:

For $i = 1, ..., j$ DO transform $B$ by calling ASR with blocksize $2^l$ and $\varepsilon$.

We bound the number of calls of the last ASR-call with blocksize $k = 2^l$. The input $B$ of this final ASR-call satisfies $D_i/D_{i+1} \leq (1 + \varepsilon)\gamma_{k/2}$ as follows from (3) with blocksize $k/2$ and $\frac{1 + 2h}{h} \leq 1$ for $k \geq 2$. Hence $D(B) \leq (1 + \varepsilon)\gamma_{k/2}$.

As each round decreases $D(B)$ by a factor $(1 + \varepsilon)^{-2}$ we see that

$$\#Ii \leq \frac{1}{2} \log_{1+\varepsilon} D(B) \leq \frac{k^3 - k^2 - k}{6} \log_{1+\varepsilon} ((1 + \varepsilon)\gamma_{k/2}) = \frac{1}{2} \frac{k^3 - k^2 - k}{h} \log_{1+\varepsilon} \gamma_{k/2}$$

provided that $D(B) \geq 1$ 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. a $0.201$ -fraction of the $\frac{1}{2} \log_{1+\varepsilon} \gamma_{k/2}$ bound of Theorem 1, where the input is an LLL-basis for $\delta, \alpha$. The final ASR-call dominates the overall workload of all ASR-calls, including the workload for the LLL-reduction of the input basis. We see that iterative slide-reduction for $k = 2^l$ 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 this proves

Corollary 1. Given an almost slide-reduced basis $B \in \mathbb{Z}^{m \times n}$ for $\varepsilon > 0$ and blocksize $k/2$, $n = h k$, ASR finds within $\frac{1}{2} \frac{k^3 - k^2 - k}{h(2 - 2\varepsilon)} \log_{1+\varepsilon} ((1 + \varepsilon)\gamma_{k/2})$ rounds of two local SVP-computations either an almost slide-reduced basis for blocksize $k$ and $\varepsilon$ or else arrives at $D(B) < 1$.

Theorem 2. The bounds $3, 4$ hold for every almost slide-reduced basis $B \in \mathbb{Z}^{m \times n}$ and $(1 + \varepsilon)$ in 3, 4 can be reduced to $(1 + \varepsilon)^{1/2}$. Proof. We see from clause 2 of Def. 1 and the Hermite bound on $\lambda_1(L(R_0^t)^*) < 1/\gamma_{n/t+1,k,t+1}$ that...
\[ D'_\ell /r_{2\ell+1,k\ell+1}^2 \leq ((1 + \varepsilon)\gamma_k)^k r_{2(k-1)}^2_{k\ell+1,k\ell+1} \]  
holds for \( \ell = \ell_{\text{max}} \) and \( \ell = h - 1 \), where \( D'_\ell := (\det R'_\ell)^2 \). Moreover, the Hermite bound for \( R_\ell \) yields
\[ r_{k\ell-k+1,k\ell-k+1}^{2(k-1)} \leq \gamma_k D'_\ell /r_{2(k-1),k\ell-k+1}^2. \]

Combining these two inequalities with \[ D'_\ell /r_{2\ell+1,k\ell+1}^2 = D'_\ell /r_{2\ell+1,k\ell+1}^2 \] yields
\[ r_{k\ell-k+1,k\ell-k+1} \leq ((1 + \varepsilon)\gamma_k)^{\frac{1}{2k}} r_{k\ell+1,k\ell+1} \] for \( \ell = \ell_{\text{max}} \) and \( \ell = h - 1 \). (2)

Next we prove
\[ D_\ell /D_{\ell+1} \leq ((1 + \varepsilon)\frac{1+\ell}{4} \gamma_k)^{\frac{1}{2k}} \] for \( \ell = 0, \ldots, h - 1 \). (3)

**Proof.** As (1) holds for \( \ell = \ell_{\text{max}} \) and (1) holds for \( \ell + 1 \) the Hermite bound on \( \lambda_1(\mathcal{L}(R_{\ell+1})) \) yields
\[ D'_\ell \leq (1 + \varepsilon)^{\frac{k-1}{2k}} r_{k\ell+1,k\ell+1} \leq (1 + \varepsilon)^{\frac{1}{2k}} \gamma_k D_\ell. \]

Hence (2) yields
\[ D_\ell = r_{2k\ell-k+1,k\ell+1} D'_\ell /r_{2k\ell-k+1,k\ell+1} \leq ((1 + \varepsilon)\gamma_k)^{\frac{1}{2k}} D'_\ell. \]

Combining the two previous inequalities yields for \( \ell = \ell_{\text{max}} \)
\[ D_\ell \leq ((1 + \varepsilon)\gamma_k)^{\frac{1}{2k}} (1 + \varepsilon)^{\frac{k-1}{2k}} D_{\ell+1} = ((1 + \varepsilon)^{\frac{1}{2k}} \gamma_k)^{\frac{1}{2k}} D_{\ell+1}. \]

Moreover if (3) holds for \( \ell_{\text{max}} \) it clearly holds for all \( \ell = 1, \ldots, h - 1 \).

3. The Hermite bound for \( R_1 \) and (3) imply for \( \ell = 1, \ldots, h \) that
\[ \|b_1\|^2 \leq \gamma_k D_1^{1/k} \leq \gamma_k((1 + \varepsilon)\frac{1+1/k}{2} \gamma_k)^{\frac{2k-1}{k}} D_1^{1/k}. \]

The product of these \( h \) inequalities for \( \ell = 1, \ldots, h \) yields
\[ \|b_1\|^{2h} \leq \gamma_k^h((1 + \varepsilon)^{\frac{1+1/h}{2}} \gamma_k)^{\frac{k(h-1)}{2h}} (\det \mathcal{L})^2/k. \]

This proves and improves 3 to ( without using that 2 holds for \( \ell = h - 1 \) )
\[ \|b_1\|^2/(\det \mathcal{L})^2/\gamma \leq \gamma_k((1 + \varepsilon)^{\frac{1+1/h}{2}} \gamma_k)^{\frac{k(h-1)}{2h}} = (1 + \varepsilon)^{\frac{1+1/h}{2}} \frac{\gamma_k - 1}{\gamma_k}. \]

4. (5) for \( \ell = h - 1 \) shows that
\[ \|b_1\|^2 \leq \gamma_k((1 + \varepsilon)^{\frac{1+1/k}{2}} \gamma_k)^{\frac{2k(k-2)}{k-1}} D_1^{1/k}. \]

Clearly 2 for \( \ell = h - 1 \) implies (2) and (4) for \( \ell = h - 1 \), and thus we get
\[ \|b_1\|^2 \leq \gamma_k((1 + \varepsilon)^{\frac{1+1/k}{2}} \gamma_k)^{\frac{2k(k-2)}{k-1}} (D_1^{1/k})^{\frac{1}{k}} \] (by (4) for \( \ell = h - 1 \))
\[ \leq \gamma_k((1 + \varepsilon)^{\frac{1+1/k}{2}} \gamma_k)^{\frac{2k(k-2)}{k-1}} (1 + \varepsilon)^{\frac{1+1/k}{2}} \gamma_k r_{n-k+1,n-k+1}^{2k/k} \] (by 2 for \( \ell = h - 1 \)).

(we also used that \( r_{n-k+1,n-k+1} \) \( \lambda_1(\mathcal{L}(R'_n^{\times 1})) \leq \gamma_k / D_1^{1/k} \) holds by the Hermite bound for \( R'_n^{\times 1} \)).

With \( \varepsilon \neq 0 \) holds for some \( b \in \mathcal{L} \) with \( \|b\| = \lambda_1 \), otherwise we remove the last \( k \) vectors of the basis. Hence \( r_{n-k+1,n-k+1} \leq \|\pi_{n-k+1}(b)\| \leq \lambda_1 \). The latter inequalities yield the claim
\[ \|b_1\| \leq ((1 + \varepsilon)^{\frac{1+1/k}{2}} \gamma_k)^{\frac{k-1}{2}} \lambda_1. \]

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

**Time bounds for extremely small \( \varepsilon \).** We measure the slide-reducedness of a basis \( B \) by the integer \( \mu \) defined by
\[ 2^{\mu-1} < \max_{\ell}(D_\ell/D_{\ell+1}) \leq 2^\mu. \]

This integer \( \mu \) exists for \( k \geq 2 \) if and only if \( \max_{\ell}(D_\ell/D_{\ell+1}) > \frac{1}{2k} \). Next we show that every round of \( \text{ASR} \) with initial value \( \mu \) decreases \( \mathcal{D}(B) \) by a factor \( 2^{\mu-1} \).

The transform of \( R_\ell, R_{\ell+1}, B \) for \( \ell = \ell_{\text{max}} \) results in (2), (3) holding for \( \varepsilon = 0 \), i.e., \( \mathcal{D}^\text{new}_{\ell+1} / \mathcal{D}^\text{new}_\ell \leq \gamma_k^{2/\ell} \).

Multiplying this inequality with \( 2^{2^{\mu-1}2^{\frac{2}{\ell}}} < D^{\text{old}}_{\ell+1} / D^{\text{old}}_\ell \) and \( D^{\text{new}}_{\ell+1} / D^{\text{new}}_\ell = D^{\text{old}}_{\ell+1} \) yields
\[ 2^{2^{\mu - 2}} D_{\ell}^{\text{new}} \leq D_{\ell}^{\text{old}} \quad \text{hence} \quad D(B^{\text{new}}) \leq D(B^{\text{old}}) 2^{-2^{\mu - 1}}. \] (7)

We denote \( M_0 := \max(||b_1||^2, \ldots, ||b_n||^2) \) for the input basis \( B \).

**Lemma 1.** If \( B \) is almost slide-reduced for \( \varepsilon < \frac{k - 1}{k h} / (2^{2} M_0) \) then \( \max_{\ell}(D_{\ell} / D_{\ell+1}) \leq \frac{2^k}{\varepsilon} \).

**Proof.** Let \( \varepsilon > 0 \) be minimal such that \( B \) is almost slide-reduced for \( \varepsilon \). It follows from the proof of (3) that \( D_{\ell} / D_{\ell+1} = ((1 + \varepsilon) \frac{1 + k}{2} \gamma k)^{2^{\mu}} \) holds for some \( \ell \). Then (6) implies \( (1 + \varepsilon) \frac{1 + k}{2} \gamma k \leq 2^{\mu} \), thus \( \varepsilon \leq \frac{1 + k}{2} \frac{k - 1}{2^k} 2^{\mu - 1} \).

If \( B = QR \) is not almost slide-reduced for some \( 0 < \varepsilon' < \varepsilon \) then any nearly maximal such \( \varepsilon' \) satisfies \( \max_{\ell}(D_{\ell} / D_{\ell+1}) \approx (1 + \varepsilon')^{r_{k+1, k+1}} \) for some \( \ell \).

It follows from [LLLS82, (1.28)] for the integer matrix \( B \) that \( r_{k+1, k+1} M_0^k \geq 1 \) and thus \( \varepsilon' \geq (\max_{\ell}(r_{k+1, k+1}))^{1/2} \), and thus proves that \( \mu < n \log_2 M_0 \).

(3) and (6) imply \( 2^{2^{\mu - 1}} < (1 + \varepsilon) \frac{2^k}{\varepsilon} \), and thus \( 2^{2^{\mu - 1}} < \frac{2^k}{\varepsilon} \log_2(1 + \varepsilon) < \frac{2^k}{\varepsilon} \log_2 \gamma k \).

Hence \( -\mu > n \log_2 M_0 \) which is impossible. This implies by (6) that \( \max_{\ell}(D_{\ell} / D_{\ell+1}) \leq \frac{2^k}{\varepsilon} \). \( \Box \)

Next we bound the number \( \#H_{\mu} \) of rounds until the current \( \mu \) decreases to \( \mu - 1 \) or arrives at \( D(B) < 1 \). During this reduction the \( \mu \) defined by (6) implies that (7) holds for each round.

Moreover, initially \( \max_{\ell}(D_{\ell} / D_{\ell+1}) \leq \frac{2^k}{\varepsilon} \gamma k \). This shows for the initial and final bases for the reduction of \( \mu \) to \( \mu - 1 \):

\[ \#H_{\mu} \leq \log_2(D(B^{\text{in}})/D(B^{\text{fin}}))/2^{\mu - 1} \leq \frac{k - h^2 - k}{3} 2^{\mu - 1} + 2^{2^{\mu - 1}} \frac{2^k}{\varepsilon} \log_2 \gamma k. \] (9)

Thus within O\( (nh^2 \log_2 k) \) rounds \( \text{ASR} \) either decreases \( \mu \geq 0 \) to \( \mu - 1 \) or arrives at \( D(B) < 1 \).

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

**Early Termination (ET).** Terminate as soon as \( D(B) < \frac{2^k}{\varepsilon} \gamma k \).

\[ D(B) < \frac{2^k}{\varepsilon} \gamma k \quad \text{imply} \quad \text{E}[\ln(D_{\ell+1})] < \frac{2^k}{\varepsilon} \ln \gamma k \text{ holds for random } \ell, \text{ with probability} \]

\[ \text{Pr}(\ell) = \frac{6}{h^2 - k^2 - h}. \] In this sense (3), (4) and 3 hold for \( \varepsilon = 0 \) "on the average".

**Corollary 2.** \( \text{ASR} \) terminates under ET for arbitrary \( \varepsilon \geq 0 \) in \( \frac{k^3 - h^2 - k}{3} (m + |m_0|) \) rounds, where \( \mu, \mu_0 \) are the \( \mu \)-value of the input and final basis defined by (6). Moreover |\( m_0 | \leq n \log_2 M_0 \).

**Proof.** Consider \( \#H_{\mu} \) the number of rounds until the current \( \mu \) decreases to \( \mu - 1 \). During this reduction the \( \mu \) of (6) satisfies \( \max_{\ell}(D_{\ell} / D_{\ell+1}) \geq 2^{2^{\mu - 1}} \frac{2^k}{\varepsilon} \gamma k \). This implies by (7) and ET for the initial and final bases for the reduction of \( \mu \) to \( \mu - 1 \):

\[ \#H_{\mu} \leq \log_2(D(B^{\text{in}})/D(B^{\text{fin}}))/2^{\mu - 1} \leq \log_2(2^{\mu} \frac{h^2 - k^2 - h}{3})/2^{\mu - 1} \]

Thus within \( \frac{k^3 - h^2 - k}{3} \) rounds \( \text{ASR} \) either decreases \( \mu \) to \( \mu - 1 \) or arrives at \( D(B) < \frac{2^k}{\varepsilon} \gamma k \).

Hence \( \text{ASR} \) terminates within \( \frac{k^3 - h^2 - k}{3} (\mu + |\mu_0|) \) rounds, where \( |\mu_0| \leq n \log_2 M_0 \) holds by the proof of Lemma 1. \( \Box \)

**Accelerated LLL-reduction (ALR).** We accelerate LLL-reduction by performing either Gaussian reductions or LLL-swaps on \( b_\ell, b_{\ell+1} \) for an \( \ell \) that promises maximal reduction progress.

We associate to a basis \( B \) satisfying \( \max_{\ell} ||b_\ell||^2 / ||b_{\ell+1}||^2 > \frac{1}{4} \) the integer \( \mu \) defined by
\[ 2^{2^{\mu - 1}} < \max_r \|b_0^r\|^2/\|b_{r+1}^*\|^2 \leq 2^{2^{\mu}}. \]  \hspace{1cm} (10)

If \( \bar{\mu} \geq 0 \) we transform in the current round \( b_r, b_{r+1} \) for an \( \ell \) that maximizes \( \|b_0^r\|^2/\|b_{r+1}^*\|^2 \) by Gaussian-reducing the basis \( \pi_r(b_r), \pi_r(b_{r+1}) \) of dimension \( 2 \). (Gaussian-reducing the basis \( \pi_r(b_r), \pi_r(b_{r+1}) \) means to LLL-reduce \( \pi_r(b_r), \pi_r(b_{r+1}) \) with \( \delta = 1 \).) This decreases \( \|b_0^r\|^2 \) by a factor less than \( 2^{-2^{\delta}} < \frac{1}{2} \).

If \( \bar{\mu} < 0 \) or \( \bar{\mu} \) does not exist, we transform in the current round \( b_r, b_{r+1} \) for an \( \ell \) that maximizes \( \|b_0^r\|^2/\|b_{r+1}^*\|^2 \) after size-reducing \( b_{r+1}^* \) against \( b_r \) by setting \( b_{r+1} := b_{r+1} - [r_{r+1}/r_r] b_r \). If \( \|\pi_r(b_{r+1})\|^2 \leq \|b_0^r\|^2 \) we swap \( b_r, b_{r+1} \) and otherwise we terminate.

On termination we size-reduce the basis \( B \).

**Theorem 3.** Given an LLL-basis \( B \in \mathbb{Z}^{n \times n} \) for \( \delta < 1 \), \( \alpha' = 1/(\delta' - 1/4) \) ALR with \( \delta \) satisfying \( 1 > \delta > \max(\delta', \frac{1}{2}) \) arrives within \( \frac{n^2}{\ln n} \alpha' \) rounds of Gaussian-reductions, resp. LLL-swaps either at an LLL-basis for \( \delta \), or else arrives at \( D(B) := \prod_{\ell=1}^{n} (\|b_0^\ell\|^2/\|b_{\ell+1}^*\|^2)^{(n-\ell)} < 1 \).

**Proof.** We use \( D(B) \) for blocksize 1, \( D(B) := \prod_{\ell=1}^{n-1} (\|b_0^\ell\|^2/\|b_{\ell+1}^*\|^2)^{(n-\ell)} \). Each round decreases \( \|b_0^r\|^2 \) by a factor \( \delta \), and both \( \|b_0^r\|^2/\|b_{r+1}^*\|^2 \), \( D(B) \) by a factor \( \delta^2 \). Then the number of rounds until either an LLL-basis for \( \delta \) appears or else \( D(B) \leq 1 \) is at most
\[
\frac{1}{2} \log_{1/\delta} D(B) \leq \frac{1}{2} \log_{1/\delta}(\alpha') \frac{n^2}{\ln \alpha'} \leq \frac{n^3}{12} \log_{1/\delta} \alpha'.
\]

\( \square \)

**The workload per round.** If each round completely size-reduces \( b_r, b_{r+1} \) against \( b_1, \ldots, b_{r-1} \) it requires \( O(n^2) \) arithmetic steps. If we only size-reduce \( b_{r+1} \) against \( b_r \) 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-reduction in segments, see [S06], [KS01].

**Lemma 2.** If \( B \) is LLL-basis for \( \delta \) and \( 1 - \delta < 2^{-n-2}/M_0 \) then \( \max_r \|b_0^r\|^2/\|b_{r+1}^*\|^2 \leq \frac{4}{3} \).

**Proof.** The LLL-basis \( B \) satisfies \( \|b_0^r\|^2 \leq \frac{1}{2^{1-1/4}} \|b_{r+1}^*\|^2 \). Therefore (10) implies \( 2^{2^{\mu - 1}} < \frac{1}{2^{1-1/4}} \), \( 2^{\mu - 1} < \log_2 \frac{3}{2} \). \( 2^{\mu - 1} \) \( \leq \log_2 \frac{3}{2} \) \( \leq \log_2 \frac{1}{\frac{5}{4} - \varepsilon} = \ln(1 - 4 \varepsilon)/\ln 2 \)
\( < -1.45 \frac{1}{4} \varepsilon < 2^{-n-1}/M_0 \).

This implies \( \bar{\mu} < -n \log_2 M_0 \) which is impossible (by the proof of Lemma 1). This shows that \( \bar{\mu} \) is undefined and thus \( \max_r \|b_0^r\|^2/\|b_{r+1}^*\|^2 \leq \frac{4}{3} \).

\( \square \)

**Corollary 3.** Let \( \bar{\mu} \) be the \( \bar{\mu} \)-value of the input-basis and \( c \in \mathbb{Z} \), \( c \geq 0 \) be constant. Within \( \frac{n^3}{12}(\bar{\mu} + 2.22 \cdot 2^c) \) rounds ALR either decreases the initial \( \bar{\mu} \) to \( \bar{\mu} \leq -c \) or else arrives at \( D(B) < 1 \). We have \( \bar{\mu} \leq \log_2 n + \log_2 M_0 \) and the number of rounds is polynomial in \( n \) if \( \log_2 \log_2 M_0 \leq n^{O(1)} \).

**Proof.** Note that LLL-bases for \( \delta = 1/(1 + \varepsilon) \) satisfy clause 2 of Def.1 for \( k = 2 \) and \( \varepsilon \). We have shown in (9) that \( ASR \) with \( k = 2 \) either decreases the current \( \mu \) to \( \mu \) within at most
\[
I(\mu) \leq \frac{n^2}{3} (2^{2^{\mu - 1} + 2^{-2^k+1} \log_2 \sqrt{3/2}) \]
rounds or else arrives at \( D(B) < 1 \). Similarly ALR either decreases the \( \bar{\mu} \) of the input-basis within at most
\[
\frac{n^2}{3} (2^{2^{\mu - 1} + 2^{-2^k+1} \log_2 \sqrt{3/2}) \leq \frac{n^3}{12} (\bar{\mu} + 2^{c+4} \log_2 \sqrt{3/2}) \leq \frac{n^3}{12} (\bar{\mu} + 2.22 \cdot 2^c) \]
rounds to \( -c \) or else arrives at \( D(B) < 1 \).

The bound \( \bar{\mu} \leq \log_2 n + \log_2 M_0 \) follows from (10) and \( \|b_{r+1}^*\|^2 \geq 1/M_0^2 \).

\( \square \)

**Comparison with previous algorithms for LLL-reduction.** The LLL was originally proved [LLL82] to be of bit-complexity \( O(2^{n^{5/6}(\log_2 M_0)^{2/3}}) \) performing \( O(n^2 \log_1 /3) \) rounds, each round size-reduces some \( b_r \) in \( n^2 \) arithmetic steps on integers of bit-length \( n \log_2 M_0 \); \( \varepsilon \) 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. It is
well known that the LLL-time can be reduced by 10 - 15 % by successively increasing $\delta$ from 3/4, 7/8, 15/16, 31/32, 63/64 to 0.99.

The number of rounds in Cor. 3 is independent of $M_n$. 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-reducing $\pi_\ell(b_k), \pi_\ell(b_{k+1})$ is quasi-linear in size($B$) [NSV10]. Therefore we do not split up this Gauss-reduction into LLL-swaps. If the current $\mu$ is large then Gauß-reducing $\pi_\ell(b_k), \pi_\ell(b_{k+1})$ for $\ell = \ell_{\text{max}}$ decreases $D(B)$ by the factor $2^{-\mu}$ while LLL-swaps guarantee only a decrease by the factor $\frac{4}{7}$.

A result that is very close to Cor. 3 and Cor. 4 has been proved independently in Lemma 12 of [HPS11]: $\max 20\|b_k\|^2/\|b_{k+1}\|^2 \leq \frac{4}{7} + \varepsilon$ can be achieved in polynomial time for arbitrary $\varepsilon > 0$.

**Early Termination (ET).** Terminate as soon as $D(B) < \left(\frac{4}{7}\right)^{\frac{n^3-n^2-n}{6}}$.

$D(B) < \left(\frac{4}{7}\right)^{\frac{n^3-n^2-n}{6}}$ implies that $E[\ln(\|b_k\|^2/\|b_{k+1}\|^2)] < \ln(4/3)$ holds for random $\ell$ and $Pr(\ell) = 6 \frac{\ln h^2}{b_0 \ell^{3/2}}$. In this sense the output basis approximates ”on the average” the logarithm of the inequality $\|b_1\|/(\det L)^{1/n} \leq \left(\frac{4}{7}\right)^{\frac{n^3-n^2-n}{6}}$ that holds for ideal LLL-bases with $\delta = 1$.

**Corollary 4.** ALR terminates under ET in $n^3(\bar{\mu} + \bar{\mu}_0)/3$ rounds, where $\bar{\mu}, \bar{\mu}_0$ are the $\bar{\mu}$-values of the input and output basis. Moreover $|\bar{\mu}_0| \leq n \log_2 M_0$ and $\bar{\mu} \leq \log_3 n + \log_3 \log_2 M_0$.

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

$$\|b^{\text{new}}_k\|^2 \leq \|b^{\text{old}}_k\|^2 2^{-\ell^2}$$

hence $D(B^{\text{new}}) < D(B^{\text{old}}) 2^{-\ell^2}$. Under ET this shows as in the proof of Cor. 1 that

$$\#H_m < \log_2(D(B^{\text{in}})/(D(B^{\text{fin}})))2^{\bar{\mu}-1} \leq \left(\frac{2^\delta n^3-n^2-n}{6}\right)^{\frac{1}{2^{\bar{\mu}-1}}} = \frac{n^3-n^2-n}{3}.$$

Hence $\mu$ decreases to $\mu - 1$ under ET in less than $\frac{n^3-n^2-n}{3}$ rounds. The proof of Lemma 1 shows that $|m_0| \leq n \log_2 M_0$.

**Open problem.** Does ALR realize $\max \|b_k\|^2/\|b_{k+1}\|^2 \leq \frac{4}{7}$ 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 $\mu$ decreases to $\mu - 1$ or that $D(B) \leq 1$? We can exclude this for $\mu \geq 0$ and under ET also for $\mu < 0$.

**References**


