Accelerated Slide- and LLL-Reduction

Claus Peter Schnorr
Fachbereich Informatik und Mathematik, Goethe-Universität Frankfurt, PSF 119132, D-60054 Frankfurt am Main, Germany.
schnorr@cs.uni-frankfurt.de

May 2, 2011

Abstract. Given an LLL-basis \( B \) of dimension \( n = hk \) we accelerate slide-reduction with blocksize \( k \) to run under a reasonable assumption in \( \frac{1}{4} n^3 h \log_{1+k} \alpha \) local SVP-computations in dimension \( k \), where \( \alpha \geq \frac{1}{4} \) measures the quality of the given LLL-basis and \( \varepsilon \) 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 \( \frac{1}{4} h^3(1 + \log_{1+k} \gamma_k/2) \). 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 \( B = [b_1, \ldots, b_n] \subset \mathbb{R}^{n \times n} \) of \( n \) linear independent vectors \( b_1, \ldots, b_n \) generates the lattice \( \mathcal{L}(B) = \{Bx \mid x \in \mathbb{Z}^n\} \) of dimension \( n \). Lattice reduction algorithms transform a given basis into a basis consisting of short vectors. \( \lambda_1(\mathcal{L}) = \min_{b \in \mathcal{L}, b \neq 0} \|b\|/2 \) is the minimal length of nonzero \( b \in \mathcal{L} \). The determinant of \( \mathcal{L} \) is \( \det \mathcal{L} = (\det B)^{1/2} \). 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 \( \gamma_n \).

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 \( B \) such that \( \|b_1\| \leq \alpha^{-n} \lambda_1 \), 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. Schnorr [S87] introduced blockwise HKZ-reduction. The algorithm of [GHKN06] improves blockwise HKZ-reduction by blockwise primal-dual reduction. So far slide-reduction of [GN08] yields the smallest approximation factor \( \|b_1\|/\lambda_1 \leq (1 + \varepsilon)^2 \gamma_k \). The blocksize \( k \) is \( \alpha \) of polynomial time reduction algorithms. The algorithm for slide-reduction of [GN08] performs \( O(nh \cdot \text{size}(B)/\varepsilon) \) local SVP-computations, where \( \text{size}(B) \) is the bit-length of \( B \) and \( \varepsilon \) is the quality of slide-reduction. This bound is polynomial in \( n \) if and only if \( \text{size}(B) \) 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 \( \text{size}(B) \). To obtain this quasi-linear bit-complexity the LLL-reduction is performed on the leading 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 [GN08] 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 \( B = \{Bx \mid x \in \mathbb{Z}^n\} \) for \( \delta, \alpha \) and dimension \( n = hk \). It shows under a reasonable assumption that this number is at most \( \frac{1}{4} n^3 h \log_{1+k} \alpha \). 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 \( \frac{1}{4} \lambda_1(\mathcal{L})^2(1 + \log_{1+k} \gamma_k/2) \), 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.
Theorem 2 shows that the bounds proven in [GN08b] on $\|b_1\|/\lambda_1$ 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 $\frac{\sqrt{2}}{2} \log_2 \text{size}(B)$ 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., size($B$) = $2^{O(n)}$. Lemma 2 shows that every LLL-basis for $\delta$ such that $1 - \delta \leq 2^{-n-2} \cdot \text{size}(B)$ satisfies the property $\max_i \|b_i^*\|^2/\|b_i^*\| \leq \frac{2}{3}$ 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 $R_e = [r_{i,j}]_{k \leq i < j \leq m}$ be the submatrix of $R = [r_{i,j}] \in \mathbb{R}^{m \times n}$ for the $\ell$-th block, $D_i = (\det R_i)^{\gamma}$, and $R_e' = [r_{i,j}]_{k \leq i < j \leq m}$ be the reversed identity matrix with non-zero entries $u_{i,k-i+1} = 1$ for $i = 1, \ldots, k$. Let $\pi_i : \mathbb{R}^n \rightarrow \text{span}(b_1, \ldots, b_{i-1})^\perp$ be the orthogonal projection, and $b_i^* := \pi_i(b_i)$ thus $\|b_i^*\| = r_{i,i}$.

**LLL-bases.** [LLL82] A basis $B = QR \in \mathbb{R}^{m \times n}$ is LLL-basis for $\delta$, $\frac{1}{2} < \delta \leq 1$ if

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

An LLL-basis for $\delta$ satisfies $\|b_i^*\|^2/\|b_i^*\| \leq \alpha$ for all $\ell = 1, \ldots, n - 1$.

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

1. $r_{k-\ell-k+1,k-\ell+1} = \lambda_1(\mathcal{L}(R_{\ell}))$ for $\ell = 1, \ldots, h$,
2. $\max_{R_{\ell+1}'T} r_{k\ell+1,k,\ell+1} \leq \sqrt{1+\varepsilon} \cdot r_{k\ell+1,k+1}$ holds for $\ell = 1, \ldots, h - 1$.

1 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:

3. $\|b_i\| \leq ((1+\varepsilon)\gamma_\lambda)^{\frac{1}{2}} (\det L)^{1/n}$,
4. $\|b_1\| \leq ((1+\varepsilon)\gamma_\lambda)^{\frac{1}{2-k}} \lambda_1$.

**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 $D_{\ell}/D_{\ell+1}$,

1. $r_{k\ell-k+1,k-\ell+1} = \lambda_1(\mathcal{L}(R_{\ell}))$ for $\ell = 1$ and $\ell = \ell_{\max}$,
2. $\max_{R_{\ell+1}'T} r_{k\ell+1,k,\ell+1} \leq \sqrt{1+\varepsilon} \cdot r_{k\ell+1,k+1}$ 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 $D_{\ell}/D_{\ell+1}$. Compute a shortest vector of $\mathcal{L}(R_{\ell+1})$ and transform $R_{\ell+1}$ and $B$ such that $r_{k\ell-k+1,k-\ell+1} = \lambda_1(\mathcal{L}(R_{\ell+1}))$. By an SVP-computation for $\mathcal{L}(R_{\ell})$ check that 2 holds for $\ell$ and if 2 does not hold transform $R_{\ell}'$ and $B$ such that 2 holds for $\varepsilon = 0$ (this decreases $D_{\ell}$ by a factor $(1+\varepsilon)^{-1}$) 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 $\frac{\sqrt{2}}{2} h^2 \log_2 \alpha \alpha = n^2 h^{1+O(\varepsilon)}$ of 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

$$\mathcal{D}(B) = \min \prod_{\ell=1}^{h-1} \left( D_{\ell}/D_{\ell+1} \right)^{h-\ell} = (\det L)^{2h} / \prod_{\ell=1}^{h} D_{\ell}^h.$$
Let \( D(B^{(m)}) \leq \alpha^{k^2} \) for \( s := \sum_{t=1}^{h-1} h \ell - \ell^2 = \frac{h^3 - h}{6} \).

**Fact.** Each round that does not lead to termination results in
\[
D_{B^{(m)}} \leq \mathcal{D}_F((1 + \varepsilon)^2) \quad D(B^{(m)}) \leq D(B)/(1 + \varepsilon)^2.
\]
This is because the round changes merely the factor \( \prod_{t=t-1, t+1} (D_t/D_{t+1})^{(h-\ell)} = (D_tD_{t+1})D_t^2 \) of
of \( D(B) \), where \( D_tD_{t+1} \) does not change. Hence, after at most
\[
\frac{1}{2} \log_{1+a} D(B^{(m)}) \leq \frac{1}{2} \log_{1+a}(\alpha^{k^2}) = \frac{1}{2} k^2 \frac{h^3 - h}{6} \log_{1+a} \alpha < \frac{2h}{1 + \varepsilon} \log_{1+a} \alpha
\]
rounds either \( B \) is almost slide-reduced for \( \varepsilon \) or else \( D(B) \leq 1 \). The \( \frac{2h}{1 + \varepsilon} \log_{1+a} \alpha \) bound includes the
rounds on termination. Clearly \( \log_{1+a} \alpha = \ln \alpha/\ln(1 + \varepsilon) \) and \( 1/\ln(1 + \varepsilon) = \frac{1 + O(\varepsilon)}{\varepsilon} \).

**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 \( E[\ln(D_t/D_{t+1})] < 0 \) holds for the expectation \( E \) for random \( t \) with \( \Pr(t) = 6 \varepsilon h^2 / \ln k \). (We have \( \sum_{t=1}^{h-1} \Pr(t) = 1 \).) In this sense \( D_t < D_{t+1} \) would hold
"on the average" if \( D(B) < 1 \) whereas such \( D_t, D_{t+1} \) 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 \( \text{size}(B) \) 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 \( \text{ASR} \) can accelerate the [GN08] algorithm at best by a factor \( h \) because the [GN08] algorithm
iterates all rounds for \( t = 1, \ldots, h \) which also covers \( \ell_{\max} \), whereas \( \text{ASR} \) iterates all rounds
for the current \( \ell_{\max} \). Theorem 1 decreases the \( O(nh \text{size}(B)/\varepsilon) \) bound of [GN08] to \( \frac{2h}{1 + \varepsilon} \log_{1+a} \alpha \) and requires only minor conditions on the input and output basis. In general it decreases the
\( O(nh \text{size}(B)/\varepsilon) \) bound of [GN08] by the factor \( \frac{2}{\varepsilon} \ln \alpha/\text{size}(B) = O(1/(6n \max \lambda \log_{2} \|b_t\|)) \).

**Iterative slide-reduction with increasing blocksize.** Consider the given LLL-basis \( B \subset \mathbb{Z}^{m \times n} \) for \( \delta, \alpha, n = hk \) iteratively as follows:

\[ \text{FOR } i = 1, \ldots, j \quad \text{DO transform } B \text{ by calling } \text{ASR} \text{ with blocksize } 2^i \text{ and } \varepsilon. \]

We bound the number \#I of rounds of the last \( \text{ASR} \) call with blocksize \( k = 2^i \). The input \( B \) of this
final \( \text{ASR} \)-call satisfies \( D_t/D_{t+1} \leq ((1 + \varepsilon)\gamma_{k/2})^{\frac{1}{k/2 + 4}} \) as follows from (3) with blocksize \( k/2 \). Hence
\[
D(B) \leq ((1 + \varepsilon)\gamma_{k/2})^{\frac{1}{k/2 + 4}} = \left( \frac{1}{2} \right)^{\frac{1}{k/2 + 4}}\frac{k^3}{h^3 - h}.
\]
As each round decreases \( D(B) \) by a factor \( (1 + \varepsilon)^{-2} \) we see that
\[
\#I \leq \frac{1}{2} \log_{1+a} D(B) \leq \frac{1}{2 + k/2} \frac{1}{2} \log_{1+a}((1 + \varepsilon)\gamma_{k/2}) = \frac{k^3}{h^3 - h} \ln \gamma_{k/2}
\]
provided that \( D(B) \geq 1 \) holds on termination. Here \( \log_{1+a} \gamma_{k/2} = \ln \gamma_{k/2}/\ln(1 + \varepsilon) = \frac{1 + O(\varepsilon)}{\varepsilon} \gamma_{k/2} \). For \( k = 4 \), resp. \( k = 8 \) this is less than a 0.603, resp. 0.201 fraction of the number of rounds \( \frac{\gamma_{k/2}}{\log_{1+a} \alpha} \) of Theorem 1, where the input is an LLL-basis for \( \delta, \alpha \). The final \( \text{ASR} \)-call dominates the workload of all other calls together, including the workload for the \( \text{LLL} \)-reduction of the input basis. We see that iterative slide-reduction for \( k = 2^i \) requires only an \( O(k^{-2}) \ln(\gamma_{k/2})/\varepsilon \)-fraction of the
workload of the direct \( \text{ASR} \)-call as in Theorem 1. In particular we have

**Corollary 1.** An almost slide-reduced basis \( B \subset \mathbb{Z}^{m \times n} \) for \( \varepsilon > 0 \) and blocksize \( k/2 \), \( n = hk \),
\( \text{ASR} \) finds within \( \frac{1}{2} h^3 - \frac{h}{2} \log_{1+a}((1 + \varepsilon)\gamma_{k/2}) \) 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 \( B \subset \mathbb{Z}^{m \times n} \) and the exponent of \( (1 + \varepsilon) \) in 3, 4 can roughly be halved, multiplying it by \( \frac{1 + 1/\varepsilon}{\varepsilon} \).

**Proof.** We see from 2 and the Hermite bound on \( \lambda_1(L(R)^*) = 1/r_{k+1, k+1} \) that
\[
\mathcal{D}_F/r_{k+1, k+1}^2 \leq (1 + \varepsilon)\gamma_k^2 r_{k+1, k+1}^{2(k-1)}.
\]
holds for \( \ell = \ell_{\max} \) and \( \ell = h - 1 \), where \( \mathcal{D}_F := (\det R)^2 \). Moreover, the Hermite bound for \( R \) yields
\[
r_{k+1, k+1}^{2(k-1)} \leq \gamma_k^2 \mathcal{D}_F/r_{k+1, k+1}^2.
\]
Combining these two inequalities with $D'_\ell/r^2_{\ell+1,k\ell+1} = D_\ell/r^2_{\ell,k\ell-k+1,k\ell}$ yields

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

for $\ell = \ell_{\text{max}}$ and $\ell = h - 1$. \hfill (2)

Next we prove

$$D'_\ell/D_{\ell+1} \leq ((1 + \varepsilon)\gamma_k)^\frac{k}{2^\ell}$$

for $\ell = 0, ..., h - 1$. \hfill (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

$$D'_\ell \leq (1 + \varepsilon)\gamma_k^{2\ell} D_{\ell+1}.$$ \hfill (4)

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

$$D'_\ell \leq ((1 + \varepsilon)\gamma_k)^\frac{k}{2^\ell}(1 + \varepsilon)\gamma_k^{2\ell} D_{\ell+1}.$$ \hfill (5)

Moreover if (3) holds for $\ell_{\text{max}}$ it clearly holds for all $\ell = 1, ..., h - 1$. \hfill (6)

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

$$\|b_1\|^2 \leq \gamma_k D_1^{1/k} \leq \gamma_k((1 + \varepsilon)\gamma_k)^\frac{2^{k(1-\ell)/k}}{k} D_1^{1/k}. \hfill (5)$$

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

$$\|b_1\|^{2h} \leq \gamma_k^{h}(1 + \varepsilon)\gamma_k^{\frac{kh}{k-1}} (\det L)^{2/k}.$$ \hfill (6)

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

$$\|b_1\|^2/(\det L)^{2/n} \leq \gamma_k((1 + \varepsilon)\gamma_k)^\frac{n-k}{k-1} = (1 + \varepsilon)\gamma_k^{\frac{n-k}{k-1}}. \hfill (7)$$

4. (5) for $\ell = h - 1$ shows that

$$\|b_1\|^{2h} \leq \gamma_k((1 + \varepsilon)\gamma_k^{\frac{2kh-2}{k-1}} D_1^{1/k}. \hfill (8)$$

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

$$\|b_1\|^2 \leq \gamma_k((1 + \varepsilon)\gamma_k^{\frac{2kh}{k-1}}) = (1 + \varepsilon)\gamma_k^{\frac{2kh-1}{k-1}}.$$ \hfill (9)

(we also used that $r_{n-k+1,n-k+1}^2 = \lambda_1^2(\mathcal{L}(R_{n-k+1}^2)) \leq \gamma_k/D_{h-1}$ holds by the Hermite bound for $R_{n-k+1}$.)

W.l.o.g $\pi_{n-k+1}(b) \neq 0$ holds for some $b \in L$ 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

$$\|b_1\| \leq ((1 + \varepsilon)\gamma_k^{\frac{2kh}{k-1}} \gamma_k^{\frac{2kh-1}{k-1}}.$$ \hfill (10)

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

**Time bounds for extremely small $\varepsilon$.** We measure the reducedness of a basis $B$ by the integer $m$ defined by

$$2^{m-1} < \max(D'_\ell/D_{\ell+1}) \gamma_k^{\frac{2^{\ell+1}}{k}} \leq 2^m.$$

This integer $m$ exists if and only if $\max(D'_\ell/D_{\ell+1}) > \gamma_k^{\frac{2^{\ell+1}}{k}}$. \hfill (6)

Next we show that every round of ASR with initial value $m$ decreases $D(B)$ by a factor $2^{-2^{m-1}}$. The transform of $R_{\ell}, R_{\ell+1}, B$ for $\ell = \ell_{\text{max}}$ results in (2), (3) holding if $\varepsilon = 0$, i.e., $D'_\ell/D_{\ell+1} \leq \gamma_k^{\frac{2^{\ell+1}}{k}}$. \hfill (7)

Multiplying this inequality with $2^{m-1} \gamma_k^{\frac{2^{\ell+1}}{k}} < D'_\ell/D_{\ell+1}$ and $D'_\ell/D_{\ell+1} \leq D_{\ell+1}/D_{\ell+1}$ yields

$$2^{m-2} D_{\ell+1} \leq D_{\ell+1} \leq D_{\ell+1}.$$ \hfill (7)

We denote $M_0 := \max(\|b_1\|^2, ..., \|b_n\|^2)$ for the input basis $B$. \hfill (7)
Lemma 1. If $B$ is almost slide-reduced for $\varepsilon < \frac{k^{-1}}{\log b} (2^m M_0)$ then $\max \varepsilon(D_\ell/D_{\ell+1}) \leq \gamma_k^{2k^2}$.  

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

$$\varepsilon < \frac{k^{-1}}{2k^2} 2^{m}.$$  

(8) 

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

It follows from [LLLS2, (1.28)] for the integer matrix $B$ that $r_{k+1,k+1} M_0^6 \geq 1$ and thus 

$$\varepsilon' \geq (\max H_{\ell}^{\varepsilon} r_{k+1,k+1} - r_{k+1,k+1})/r_{k+1,k+1} \geq 1/M_0^6.$$  

This contradicts (8) if $\frac{k^{-1}}{2k^2} 2^{m} < 1/M_0^6$, and thus excludes that $-m > n \log_2 M_0$. 

(3) and (6) imply $2^{m-1} < (1 + \varepsilon)^{\frac{2k^2}{k-1}}$, and thus $2^{m-1} < \frac{2k^2}{k-1} \log_2 (1 + \varepsilon) < \frac{2k^2}{k-1} \varepsilon$. Hence $-m > n \log_2 M_0$ which is impossible. This implies by (6) that $\max_2 D_\ell/D_{\ell+1} \leq \gamma_k^{2k^2}$. □ 

Next we bound the number $\# I_m$ of rounds until the current $m$ either decreases to $m-1$ or arrives at $D(B) < 1$. During this reduction the $m$ defined by (6) holds for each round. Moreover, initially $\max_2 D_\ell/D_{\ell+1} \leq \gamma_k^{2k^2} 2^m$. This shows for the initial and final bases for the reduction of $m$ to $m-1$: 

$$\# I_m \leq \log_2 (D(B)_{\text{in}})/(D(B)_{\text{fin}}))/2^{m-1} \leq \frac{\gamma_k^{2k^2}}{3} (2^m/2^{m-1} + 2^{-m+1} k^2 \log_2 \gamma_k).$$ 

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

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 $D(B) < 1$ ? We can exclude this by the following rule of 

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

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

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

Proof. Consider $\# I_m$ the number of rounds until the current $m$ decreases to $m-1$. During this reduction the $m$ of (6) satisfies $\max_2 D_\ell/D_{\ell+1} > 2^{m-1} \gamma_k^{2k^2}$. This implies by (7) and ET for the initial and final bases for the reduction of $m$ to $m-1$: 

$$\# I_m \leq \log_2 (D(B)_{\text{in}})/(D(B)_{\text{fin}}))/2^{m-1} \leq \log_2 (2^{m+1} \gamma_k^{2k^2})/2^{m-1} = \frac{h^3}{k}.$$ 

Thus within $\frac{h^3}{k} \gamma_k^{2k^2}$ rounds ASR either decreases $m$ to $m-1$ or arrives at $D(B) < \gamma_k^{\frac{2k^2}{k-1} h^3}$. Hence ASR terminates within $\frac{h^3}{k} (m + |m_0|)$ rounds, where $|m_0| \leq n \log_2 M_0$ holds by the proof of Lemma 1. □ 

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

We associate to a basis $B$ satisfying $\max \|b_\ell^*\|^2/\|b_{\ell+1}^*\|^2 > \frac{k}{2}$ the integer $m$ defined by 

$$2^{m-1} < \max \|b_\ell^*\|^2/\|b_{\ell+1}^*\|^2 < \frac{4}{3} 2^m.$$  

(9) 

If $m \geq 0$ we transform in the current round $b_\ell, b_{\ell+1}$ for an $\ell$ that maximizes $\|b_\ell^*\|^2/\|b_{\ell+1}^*\|^2$ by
Theorem 3. Given an LLL-basis \( B \in \mathbb{Z}^{m \times n} \) for \( \delta' < 1 \), \( \alpha' = 1/(\delta' - 1/4) \) ALR with \( \delta' \) satisfying \( 1 > \delta > \max(\delta', 1/2) \) arrives within \( \frac{n^2}{12} \log_2 \alpha' \) rounds of LLL-reductions, resp. LLL-swaps either at an LLL-basis for \( \delta \), or else arrives at \( D(B) = \left[ \prod_{r=1}^{n-1} \left( \frac{\|b_r^*\|^2}{\|b_{r+1}^*\|^2} \right)^2 \right]^{(n-\ell)}/\delta' \). Each round decreases \( \|\pi_r(b_{r+1})\|^2 \) by a factor \( \delta \), and both \( \|b_r^*\|^2/\|b_{r+1}^*\|^2 \), \( D(B) \) by a factor \( \delta' \). Then the number of rounds until either an LLL-basis for \( \delta' \) appears or else \( D(B) \leq 1 \) is at most
\[
\frac{1}{2} \log_{1/\delta} D(B) \leq \frac{1}{4} \log_{1/\delta}(\alpha')^{3^2/9} \leq \frac{n^3}{12} \log_2 \alpha' \].

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 explodes. 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 \( \max_r \|b_r^*\|^2/\|b_{r+1}^*\|^2 \leq \frac{4}{\delta} \).

Proof. The LLL-basis \( B \) satisfies \( \|b_1^*\|^2 \leq \frac{1}{1+4\varepsilon} \|b_{1}^*\|^2 \). Therefore (9) implies \( 2^{2^m-1} < \frac{1}{3/12} \). Setting \( \delta = 1 - \varepsilon \) this shows that
\[
2^{m-1} - \log_2 \frac{3}{1+4\varepsilon} < \log_2 \frac{1}{3} = \ln(1 - 4/3\varepsilon)/\ln 2 < -1.45 \frac{4}{3} < 2^{-n-1}/M_0.
\]
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 \( \max_r \|b_r^*\|^2/\|b_{r+1}^*\|^2 \leq \frac{4}{\delta} \). \( \square \)

Corollary 3. Let \( m \) be the \( m \)-value of the input basis and \( c \in \mathbb{Z}, c \geq 0 \) be constant. Within
\[
\frac{2^3}{17}(m+2.22 \cdot 2^c) \text{ rounds ALR}\]
either decreases the initial \( m \) to \( m \leq -c \) or else arrives at \( D(B) < 1 \). Moreover \( m \leq \log_2 n + \log_2 \log_2 M_0 \).

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

Proof. We have shown that ASR with \( k = 2 \) either decreases within at most
\[
\frac{(\sqrt{2})^3}{3} \left( \frac{2^m}{\log_2 \sqrt{1/3}} + \frac{2^m+1}{\log_2 \sqrt{1/3}}\right)
\]
rounds either the current \( m \) to \( m - 1 \) or arrives at \( D(B) < 1 \). Therefore ALR either decreases the \( m \) of the input-basis within at most
\[
\frac{2^3}{17}(2m+2^4 \log_2 \sqrt{1/3}) \leq \frac{2^3}{17}(m+2^{c+4} \log_2 \sqrt{1/3}) < \frac{2^3}{17}(m+2.22 \cdot 2^c) \text{ rounds to } m = -|c| \text{ or else arrives at } D(B) < 1
\]
The bound \( m \leq \log_2 n + \log_2 \log_2 M_0 \) follows from (9) and \( \|b_{r+1}^*\|^2 \geq 1/M_0^2 \). \( \square \)

Comparison with previous algorithms for LLL-reduction. The LLL was originally proved [LLS82] to be of bit-complexity \( O(n^{5+e}(\log_2 M_0)^{2+e}) \) performing \( O(n^2 \log_2 \log_2 M_0) \) rounds, each round size-reduces some \( b_r \) in \( n^2 \) arithmetic steps on integers of bit-length \( n \log_2 M_0 \); \( e \) in the exponent comes from the fast FFT-multiplication of integers. The 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 $\pi(b_\ell \pi(b_{\ell+1})$ is quasi-linear in size($B$) [NSV10]. Therefore we do not split this Gauß-reduction into LLL-swaps. If the current $m$ is large then Gauß-reduction of $\pi(b_\ell \pi(b_{\ell+1})$ for $\ell = \ell_{\text{max}}$ decreases $D(B)$ be the factor $2^{-m}$ while LLL-swaps guarantee only a decrease by the factor $\frac{1}{2}$.

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

**Early Termination (ET).** Terminate as soon as $D(B) < (\frac{1}{4})^{\frac{a^3-n}{4}}$.

$D(B) < (\frac{1}{4})^{\frac{a^3-n}{4}}$ implies that $E[\ln(\frac{||b_\ell||^2}{||b_{\ell+1}||^2})] < \ln(4/3)$ holds for random $\ell$ and $\Pr(\ell) = 6 \frac{m-\ell}{n-\ell}$. In this sense the output basis approximates "on the average" the logarithm of the inequality $||b_1||/(\det L)^{1/n} \leq (\frac{1}{4})^{\frac{n-3}{4}}$ 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 $\#I_m$ of rounds until either the current $m$ decreases to $m - 1$ or else $D(B)$ becomes less than $(4/3)^{\frac{a^3-n}{4}}$. As in the proof of Corollary 2 each round with $\ell$ results in Gauß-reduction under $\pi_\ell$ if $m \geq 0$, resp. an LLL-swap if $m < 0$, results in $||b_{\ell}^{\text{new}}||^2 < ||b_{\ell}^{\text{old}}||^22^{-2m-2}$ hence $D(B^{\text{new}}) < D(B^{\text{old}})2^{-2m-1}$.

Under ET this shows as in the proof of Cor. 1 that $\#I_m < \log_2(D(B^{\text{fin}})/(D(B^{\text{fin}}))/2^{m-1}) \leq (2^m \frac{n^3-n}{6n})/2^{m-1} = \frac{n^3-n}{3}$. Hence $m$ decreases to $m - 1$ under ET in less than $\frac{n^3-n}{3}$ rounds. The proof of Lemma 1 shows that $|m_0| \leq n \log_2 M_0$. \[\Box\]

**Open problem.** Does ALR realize $\max_{\ell} ||b_\ell||^2/||b_{\ell+1}||^2 \leq \frac{4}{7}$ 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 $D(B) \leq 1$? We can exclude this for $m \geq 0$ and under ET also for $m < 0$.

**References**


