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 assumption in \( \frac{1}{2} n^2 h \log_{1+\varepsilon} \alpha \) 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 \( \frac{1}{2} h^3(1 + \log_{1+\varepsilon} \gamma_\varepsilon) \). 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 \( B = [b_1, ..., b_n] \in \mathbb{R}^{m \times n} \) of \( n \) linear independent vectors \( b_1, ..., b_n \) 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. \( \lambda_1(\mathcal{L}) = \min_{\mathcal{L} \subset \mathbb{R}^n \setminus \{0\}} \| b \| \) is the minimal length of nonzero \( b \in \mathcal{L} \). The determinant of \( \mathcal{L} \) is \( \det \mathcal{L} = (\det B)^{1/n} \). 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 \( \| b_1 \| \leq \alpha^{n-1} \lambda_1 \), 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. 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 \( \| b_1 \|/\lambda_1 \leq (1 + \varepsilon) \gamma_\varepsilon \) 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 \( \varepsilon \) 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 ged-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 \( \delta, \alpha \) and dimension \( n = hk \).

It shows under a reasonable assumption that this number is at most \( \frac{1}{2} n^2 h \log_{1+\varepsilon} \alpha \). 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 \( \frac{1}{2} \frac{1}{1+\varepsilon} h^3(1 + \log_{1+\varepsilon} \gamma_\varepsilon) \), reducing the number by a factor \( 2k^3 \ln \gamma_\varepsilon/\ln \alpha \). 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 $\frac{1}{2} \log_2 \text{size}(B)$ 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., $\text{size}(B) = 2^{O(n)}$. Lemma 2 shows that every LLL-basis for $\delta$ such that $1 - \delta \leq 2^{-n-2\cdot \text{size}(B)}$ satisfies the property $\max_i \|b_i^*\|^2/\|b_i^*\|^2 \leq \frac{2}{3}$ 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 $R = [r_{i,j}]_{k \times k}$ be the submatrix of $R = [r_{i,j}] \in \mathbb{R}^{m \times n}$ for the $\ell$-th block, $D = \det(R')$, and $R' = [R_{i,j}]_{k \times k}$ is the reversed identity matrix with non-zero entries $u_{i,k,i+1} = 1$ for $i = 1, \ldots, k$. Let $\max_{R' \in T} \pi_{k+1} : \mathbb{R}^k \rightarrow (\det L)^{1/n}$.

**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

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

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

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

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

3. $\|b_i\| \leq ((1 + \varepsilon)\gamma_k)^{\frac{1}{2\cdot \lambda_1}}(\det L)^{1/n}$.
4. $\|b_i\| \leq ((1 + \varepsilon)\gamma_k)^{\frac{1}{2\cdot \lambda_1}}(\det L)^{1/n}$.

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

1. $r_{k-1,k+1,k} = \lambda_1(\mathcal{L}(R_{k}))$ for $\ell = 1$ and $\ell = \ell_{\text{max}}$.
2. $\max_{R' \in T} \pi_{k+1} \leq \sqrt{1 + \varepsilon} \cdot r_{k+1,k+1}$ holds for $\ell = \ell_{\text{max}}$ and $h = 1$.

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

**Accelerated slide-reduction (ASR).** In each round find some $\ell = \ell_{\text{max}}$ 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 $r_{k-1,k+1,k} = \lambda_1(\mathcal{L}(R_{\ell+1}))$.

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 $\ell = \ell_{\text{max}}$ and $h = 1$ until 2 holds for both $\ell = \ell_{\text{max}}$ and $h = 1$. Finally make sure that 1 holds for $\ell = 1$ and size-reduce $B$.

**Theorem 1.** Accelerated slide-reduction transforms a given LLL-basis $B \in \mathbb{R}^{m \times n}$ for $\delta \leq 1$, $\alpha = 1/(\delta - 1/4)$, $n = hk$, within $\frac{1}{2} n^2 h \log_{16} \alpha = n^2 h^{1+\varepsilon} \ln \alpha$ rounds of local SVP-computations either into an almost slide-reduced basis for $\varepsilon > 0$, or else arrives at $D(B) < 1$,

$$D(B) = \det \prod_{i=1}^{k-1}(D_{\ell}/D_{\ell+1})^{h_{\ell-\ell}} = (\det L)^{2h}/\prod_{i=1}^{h} \prod_{j=1}^{h} D_j^2.$$
\[ \mathcal{D}(B^{(in)}) \leq \alpha^{k^2 s}, \text{ for } s := \sum_{t=1}^{h-1} h \ell - \ell^2 = \frac{h^3 - h}{6}. \]

**Fact.** Each round that does not lead to termination results in
\[ \mathcal{D}_{\ell}^{new} \leq \mathcal{D}_{\ell}/(1 + \varepsilon) \quad \mathcal{D}(B^{new}) \leq \mathcal{D}(B)/(1 + \varepsilon)^2. \]
This is because the round changes merely the factor \( \prod_{t=0}^{h-1} (D_t/D_{t+1})^{(h-t)} = (D_t D_{t+1}) D_t^2 \) of
of \( \mathcal{D}(B) \), where \( D_t D_{t+1} \) does not change. Hence, after at most
\[ \frac{1}{h} \log_{1+i} \mathcal{D}(B^{(in)}) \leq \frac{1}{h} \log_{1+i} (\alpha^{k^2 s}) = \frac{1}{h} k^2 \frac{h^3 - h}{6} \log_{1+i} \alpha < \frac{2 k^2}{h} \log_{1+i} \alpha \]
rounds either \( B \) is almost slide-reduced for \( \varepsilon \) or else \( \mathcal{D}(B) \leq 1 \). The \( \frac{n^2}{k^2} \log_{1+i} \alpha \) bound includes the rounds on termination. Clearly \( \log_{1+i} \alpha = \ln \alpha/\ln(1 + \varepsilon) \) and \( 1/\ln(1 + \varepsilon) = \frac{1 + O(\varepsilon)}{\varepsilon^2}. \]

**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 \( E[\ln(D_t/D_{t+1})] < 0 \) holds for the expectation \( E \) for
random \( t \) with \( \Pr(t) = \frac{6 \ln^2}{n} \). (We have \( \sum_{t=1}^{h} \Pr(t) = 1 \).) In this sense \( D_t < D_{t+1} \) would hold
"on the average" if \( \mathcal{D}(B) < 1 \) whereas such \( D_t, D_{t+1} \) are extremely unlikely in practice.

**Time bound compared to [GN08].** The algorithm for slide-reduction of [GN08] is 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 \( \text{size}(B) \) 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 \( \ell = 1, \ldots, h \) which also covers \( t_{\text{max}} \), whereas ASR iterates all
rounds for the current \( t_{\text{max}} \). Thus Theorem 1 shows that the [GN08] algorithm performs at most
\( \frac{n^2 \alpha^2}{k^2} \log_{1+i} \alpha \) local SVP-computations if the input basis is an LLL-basis for \( \delta \) and the algorithm
terminates with a basis \( B \) such that \( \mathcal{D}(B) \geq 1 \). Theorem 1 eliminates from the \( O(nh \text{size}(B)/\varepsilon) \)
time bound of [GN08] the bit-length of \( B \) and requires only minor conditions on the input and output
basis. As \( \text{size}(B) \approx \sum_{i=1}^{h} \log_2 \|b_i\| \) our \( \frac{n^2 \alpha^2}{k^2} \log_{1+i} \alpha \) bound is better than the \( O(nh \text{size}(B)/\varepsilon) \)
bound of [GN08] if \( \frac{n^2}{k^2} \ln \alpha < \frac{1}{h} \sum_{i=1}^{h} \log_2 \|b_i\| \). 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 \( \delta, \alpha, n = hk \) iteratively as follows:

FOR \( i = 1, \ldots, j \) DO transform \( B \) by calling ASR with blocksize \( 2^j \) and \( \varepsilon \).

We bound the number \( \#H \) of rounds of the last ASR-call with blocksize \( k = 2^j \). The input \( B \) of this
final ASR-call satisfies
\[ D_t/D_{t+1} \leq ((1 + \varepsilon) \gamma_{k/2})^{k/2 - 1} \]
as follows from (3) with blocksize \( k/2 \). Hence
\[ \mathcal{D}(B) \leq ((1 + \varepsilon) \gamma_{k/2})^{k/2} \gamma_{k/2} \frac{k^2 - h}{6}. \]

As each round decreases \( \mathcal{D}(B) \) by a factor \( (1 + \varepsilon)^{-2} \) we see that
\[ \#H \leq \frac{1}{k} \log_{1+i} \mathcal{D}(B) \leq \frac{k^2 - h}{6} \log_{1+i} ((1 + \varepsilon) \gamma_{k/2}) = \frac{k^2 - h}{6} \log_{1+i} \gamma_{k/2} \]
provided that \( \mathcal{D}(B) \geq 1 \) holds on termination. Here \( \log_{1+i} \gamma_{k/2} = \ln \gamma_{k/2} / (1 + \varepsilon) = \frac{\ln \gamma_{k/2}}{\varepsilon^2} \).

For \( k = 4 \), resp. \( k = 8 \) this is less than 0.603, resp. 0.201 fraction of the number of rounds
\( \frac{k^2 - h}{6} \log_{1+i} \alpha \) of Theorem 1, where the input is an LLL-basis for \( \delta, \alpha \). 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 \( k = 2^3 \) 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 \( \frac{1}{k} \left( \frac{k^2 - h}{6} \right) \log_{1+i} ((1 + \varepsilon) \gamma_{k/2}) \) rounds of two local SVP-computations either an
almost slide-reduced basis for blocksize \( k \) and \( \varepsilon \) or else arrives at \( \mathcal{D}(B) < 1 \).

**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 \( 1/2 \).

**Proof.** We see from 2 and the Hermite bound on \( \lambda_1(L(R^*_t)) = 1/r_{k+1,t+1} \) that
\[ \mathcal{D}_f' / r_{k+1, k+1}^2 \leq ((1 + \varepsilon) \gamma_k)^k r_{k+1, k+1}^2 (1 + \varepsilon) \]

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

\[ r_{k+1, k+1}^{2(k-1)} \leq \gamma_k \mathcal{D}_f' / r_{k-1, k-1}^2. \]

Combining these two inequalities with

\[ \mathcal{D}_f' / r_{k+1, k+1}^2 = \mathcal{D}_f / r_{k-1, k-1}^2 \]

yields

\[ r_{k-1, k-1} \leq ((1 + \varepsilon) \gamma_k) \frac{2k}{\ell} r_{k+1, k+1} \quad \text{for} \quad \ell = \ell_{\text{max}} \quad \text{and} \quad \ell = h - 1. \quad (2) \]

Next we prove

\[ \mathcal{D}_f / \mathcal{D}_{t+1} \leq ((1 + \varepsilon) \frac{1 + 1/k}{\gamma_k}) \frac{2k}{\ell} \quad \text{for} \quad \ell = 0, \ldots, h - 1. \quad (3) \]

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

\[ \mathcal{D}_f \leq (1 + \varepsilon)^k \gamma_k r_{k+1, k+1} \leq (1 + \varepsilon)^k \gamma_k \mathcal{D}_t. \]

We see from (2) that

\[ \mathcal{D}_f = r_{k+1, k+1}^2 \mathcal{D}_f' / r_{k+1, k+1} \leq ((1 + \varepsilon) \gamma_k) \frac{2k}{\ell} \mathcal{D}_f'. \quad (4) \]

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

\[ \mathcal{D}_f \leq ((1 + \varepsilon) \gamma_k) \frac{2k}{\ell} \mathcal{D}_t + ((1 + \varepsilon) \frac{1 + 1/k}{\gamma_k}) \frac{2k}{\ell} \mathcal{D}_{t+1}. \]

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

\[ \|b_1\|^2 \leq \gamma_k \mathcal{D}_1^{1/k} \leq \gamma_k ((1 + \varepsilon) \frac{1 + 1/k}{\gamma_k}) \frac{2k(1-1)}{\ell} \mathcal{D}_1^{1/k}. \quad (5) \]

The product of these \( h \) inequalities for \( \ell = 1, \ldots, h \) yields

\[ \|b_1\|^{2h} \leq \gamma_k^h ((1 + \varepsilon) \frac{1 + 1/k}{\gamma_k}) \frac{2k(1-1)}{h} (\det \mathcal{L})^{2/k}. \]

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

\[ \|b_1\|^2 / (\det \mathcal{L})^{2/n} \leq \gamma_k ((1 + \varepsilon) \frac{1 + 1/k}{\gamma_k}) \frac{2k}{n} = (1 + \varepsilon) \frac{1 + 1/k}{\gamma_k} \gamma_k^\frac{n-1}{k}. \]

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

\[ \|b_1\|^2 \leq \gamma_k ((1 + \varepsilon) \frac{1 + 1/k}{\gamma_k}) \frac{2k(1-1)}{h} \mathcal{D}_{h-1}^{1/k}. \]

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

\[ \|b_1\|^2 \leq \gamma_k ((1 + \varepsilon) \frac{1 + 1/k}{\gamma_k}) \frac{2k(1-1)}{h} \left( \sum_{m=1}^{k} \mathcal{D}_{m-1}^{1/k} \right) \quad \text{for} \quad \ell = h - 1 \]

\[ \leq \gamma_k ((1 + \varepsilon) \frac{1 + 1/k}{\gamma_k}) \frac{2k(1-1)}{h} \left( 1 + \varepsilon \right) \gamma_k r_{n-k+1,n-k-1,1}. \quad \text{by (2) for} \quad \ell = h - 1. \]

We also used that

\[ r_{n-k+1,k-1,n-k-1} = \lambda_1(\mathcal{L}(R_{t_{n-k+1}})) \leq \gamma_k / \mathcal{D}_{n-k+1,1} \text{ holds by the Hermite bound for } R_{t_{n-k+1}}. \]

W.l.o.g. \( \pi_{n-k+1}(b) \neq 0 \) 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

\[ \|b_1\| \leq ((1 + \varepsilon) \frac{1 + 1/k}{\gamma_k}) \gamma_k^\frac{n-1}{k} \lambda_1. \]

We have roughly halved the exponent of \((1 + \varepsilon) / \gamma_k^\frac{n-1}{k} \lambda_1 \).

\[ \square \]

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

\[ 2^{2^{m-1}} < \max_t(\mathcal{D}_t / \mathcal{D}_{t+1}) \gamma_k^{\frac{2k^2}{\ell}} \leq 2^{2^{m}}. \quad (6) \]

This integer \( m \) exists if and only if \( \max_t(\mathcal{D}_t / \mathcal{D}_{t+1}) > \gamma_k^{\frac{2k^2}{\ell}} \).

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 \( R_t, R_{t+1} \) for \( \ell = \ell_{\text{max}} \) results in (2), (3) holding \( f \) or \( \varepsilon = 0 \), i.e.,

\[ \mathcal{D}_{n \rightarrow \text{new}, n \rightarrow \text{new}} \leq \gamma_k^{\frac{2k^2}{\ell}}. \]

Multiplying this inequality with \( 2^{-2^{m}} \gamma_k^{\frac{2k^2}{\ell}} < \mathcal{D}_{t \rightarrow \text{old}, t \rightarrow \text{old}} \) and \( \mathcal{D}_{n \rightarrow \text{new}, n \rightarrow \text{new}} \leq \mathcal{D}_{t \rightarrow \text{old}, t \rightarrow \text{old}} \) yields

**4**
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 \( \varepsilon < \frac{1}{256}/(2^p M_0) \) then \( \max_{\ell}(D_{\ell}/D_{\ell+1}) \leq \gamma_k^{\frac{256}{m}}. \)

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

\[ \varepsilon < \frac{1}{k^2}. \quad (8) \]

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

It follows from \([\text{LLL82}, (1.28)]\) for the integer matrix \( B \) that \( r_{k+1, k+1} M_0^a \geq 1 \)

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

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

Hence \( -m > n \log_2 M_0 \) which is impossible. This implies by (6) that \( \max_{\ell}(D_{\ell}/D_{\ell+1}) \leq \gamma_k^{\frac{256}{m}}. \)

Next we bound the number \#\( H_m \) 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) implies that (7) holds for each round. Moreover, initially \( \max_{\ell}(D_{\ell}/D_{\ell+1}) \leq \gamma_k^{\frac{256}{m}} 2^{m} \). This shows for the initial and final bases for the reduction of \( m \) to \( m - 1 \): \[ \#\( H_m \) \leq \log_2(D(B^{(in)})/D(B^{(fin)}))/2^{m-1} \leq \frac{k^2 h}{\gamma_k} + 2^{m-1} \frac{k^2 h}{\gamma_k} \log_2 \gamma_k. \]

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

**Open problem.** Can \( \text{ASR} \) perform for \( m < 0 \) 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 \( D(B) < \gamma_k^{\frac{256}{m-1}} \).

\( D(B) < \gamma_k^{\frac{256}{m-1}} \) implies \( E[\ln(D_{\ell}/D_{\ell+1})] < \frac{256}{m-1} \log_2 \gamma_k \) holds for random \( \ell \), where \( \Pr(\ell) = 6^{\frac{\ln n+\ell}{\ln k}}. \) In this sense, (3), (4) and 3 hold for \( \varepsilon = 0 \) "on the average".

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

**Proof.** Consider \#\( H_m \) the number of rounds until the current \( m \) decreases to \( m - 1 \). During this reduction the \( m \) of (6) satisfies \( \max_{\ell}(D_{\ell}/D_{\ell+1}) \geq 2^{m-1} \gamma_k^{\frac{256}{m}} \). This implies by (7) and ET for the initial and final bases for the reduction of \( m \) to \( m - 1 \): \[ \#\( H_m \) \leq \log_2(D(B^{(in)})/D(B^{(fin)}))/2^{m-1} \leq \log_2(2^{m\gamma_k^{\frac{256}{m}}})/2^{m-1} = \frac{h^3 - 6}{3}. \]

Thus within \( \frac{h^3 - 6}{3} \) rounds \( \text{ASR} \) either decreases \( m \) to \( m - 1 \) or arrives at \( D(B) < \gamma_k^{\frac{256}{m-1}} \).

Hence \( \text{ASR} \) terminates within \( \frac{h^3 - 6}{3} (m + |m_0|) \) 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 \( \max_{\ell}(\|b_\ell\|^2/\|b_{\ell+1}\|^2) > \frac{1}{4} \) the integer \( m \) defined 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 $1 > \delta = \max(\delta', \frac{1}{2})$ arrives within $\frac{n^3}{4} \log_{1/\delta} \alpha'$ rounds of Gauß-reductions, resp. LLL-swaps either at an LLL-basis for $\delta$, or else arrives at $D(B) := \prod_{t=1}^{n-1} \|b_i^t\|^2/\|b_{i+1}^t\|^2)^{(n-t)} < 1$.

Proof. We use $D(B)$ for blocksize 1, $D(B) := \prod_{t=1}^{n-1} \|b_i^t\|^2/\|b_{i+1}^t\|^2)^{(n-t)}$. Each round decreases $\|b_i^t\|^2$ by a factor $\delta$, and both $\|b_i^t\|^2/\|b_{i+1}^t\|^2$, $D(B)$ 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
\[
\frac{1}{2} \log_{1/\delta} D(B) \leq \frac{1}{2} \log_{1/\alpha'} \left( \frac{n^3}{4} \right) \leq \frac{n^3}{4} \log_{1/\delta} \alpha'.
\]

The work per round. If each round completely size-reduces $b_1, b_{i+1}$ against $b_1, ..., b_{i+1}$, it requires $O(n^2)$ arithmetic steps. If we only size-reduce $b_{i+1}$ against $b_i$, 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 size-reduction in segments, see [S06], [K01].

Lemma 2. If $B$ is LLL-basis for $\delta$ and $1 - \delta < 2^{-n/2}/M_0$ then $\max_t \|b_i^t\|^2/\|b_{i+1}^t\|^2 \leq \frac{4}{3}$.

Proof. The LLL-basis $B$ satisfies $\|b_i^t\|^2 \leq \frac{1}{2^{n-t}} \|b_{i+1}^t\|^2$. Therefore (9) implies $2^{2m-1} < \frac{1}{2^{n-1/4}} \cdot \frac{3}{4}$. Setting $\delta = 1 - \varepsilon$ this shows that
\[
2^{m-1} < \log_2 \frac{3}{2^{n-t}} < \log_2 \frac{1}{1-\varepsilon} = (1 - \frac{1}{4} \varepsilon)/\ln 2 < -1.45 \frac{1}{4} \varepsilon < 2^{-n-1}/M_0.
\]
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 $\max_t \|b_i^t\|^2/\|b_{i+1}^t\|^2 \leq \frac{4}{3}$.

Corollary 3. Let $m$ be the $m$-value of the input basis and $c \in \mathbb{Z}$ $c \geq 0$ be constant. Within $\frac{3}{2} (m + 222 - 2^c)$ rounds ALR either decreases the initial $m$ to $m = -c$ 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
\[
\frac{(n/2)^3}{3} (2m/2^{m-1} + 2^{-m+4} \log_2 \sqrt{1/3})
\]
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
\[
\frac{3}{2} (2m + 2^{222} \log_2 \sqrt{1/3} \sum_{m-c}^{m-2^c}) < \frac{3}{2} (m + 2^{222+4} \log_2 \sqrt{1/3}) < \frac{3}{2} (m + 222 \cdot 2^c)
\]
rounds to $m = -|c|$ or else arrives at $D(B) < 1$.

The bound $m \leq \log_2 n + \log_2 \log_2 M_0$ follows from (9) and $\|b_{i+1}^t\|^2 \geq 1/M_0^3$.

Comparison with previous algorithms for LLL-reduction. The LLL was originally proved [LLS82] 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 $b_i$ 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.
The number of rounds in Cor. 3 is independent of $M_0$. This is because $\text{ALR}$ maximizes the reduction progress per round. To minimize the workload of size-reduction $\text{ALR}$ 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 $\pi_t(b_t),\pi_t(b_{t+1})$ 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 $\pi_t(b_t),\pi_t(b_{t+1})$ for $t \leq t_{\text{max}}$ decreases $\mathcal{D}(B)$ be the factor $2^{-m}$ while LLL-swaps guarantee only a decrease by the factor $\frac{4}{3}$.

The algorithm for LLL-reduction with fixed complexity iterates all possible LLL-swaps of $b_t, b_{t+1}$ for $t = 1, \ldots, n - 1$. If this algorithm would not just do LLL-swaps but Gauss-reductions of $\pi_t(b_t),\pi_t(b_{t+1})$ for all $t$ by its number of rounds would be at most $n - 1$ times the number of rounds
\[
\frac{n^3}{m} \log_{1/3} \alpha'
\]

of $\text{ALR}$.

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

$\mathcal{D}(B) < \left(\frac{4}{3}\right) \frac{n^3}{m}$ implies that $\mathbb{E}[\ln(\|b_t^\text{new}\|^2/\|b_{t+1}^\text{old}\|^2)] < \ln(4/3)$ holds for random $t$ and $\Pr(t) = 6 n^2 s^2 / \sqrt{m n^3}$. In this sense the output basis approximates "on the average" the logarithm of the inequality $\|b_t^\text{new}\|/(\det L)^{1/n} \leq \left(\frac{4}{3}\right) \frac{n^3}{m}$ that holds for ideal LLL-bases with $\delta = 1$.

**Corollary 4.** $\text{ALR}$ 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 $\#H_m$ of rounds until either the current $m$ decreases to $m - 1$ or else $\mathcal{D}(B)$ becomes less than $(4/3) \frac{n^3}{m}$. As in the proof of Corollary 2 each round with $m$ results in Gauß-reduction under $\pi_t$ if $m \geq 0$, resp. an LLL-swap if $m < 0$, results in
\[
\|b_t^\text{new}\|^2 < \|b_t^\text{old}\|^2 2^{-2m-2}
\]
hence $\mathcal{D}(B^\text{new}) < \mathcal{D}(B^\text{old}) 2^{-2m-1}$.

Under ET this shows as in the proof of Cor. 1 that
\[
\#H_m < \log_2 (\mathcal{D}(B^\text{in})/(\mathcal{D}(B^\text{fin}))/2^{m-1} = \left(2^m \frac{n^3}{m} \right)/2^{m+1} = \frac{n^3}{3}.
\]

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

**Open problem.** Does $\text{ALR}$ realize $\max_t \|b_t\|^2/\|b_{t+1}\|^2 \leq \left(\frac{4}{3}\right)$ in a polynomial number of rounds? Can $\text{ALR}$ perform for $m \leq 0$ without ET more than $O(n^2)$ 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**


