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 11, 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 $\frac{1}{4} n^2 h \log_{1+\varepsilon} \alpha$ local SVP-computations in dimension $k$, where $\alpha \geq \frac{1}{2}$ 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 $\frac{1}{2} h^3 (1 + \log_{1+\varepsilon} \gamma_k / 2)$. 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 $B = [b_1, \ldots, b_n] \in \mathbb{R}^{m \times n}$ of $n$ linear independent vectors $b_1, \ldots, b_n$ generates the lattice $L(B) = \{ b x \mid x \in \mathbb{Z}^n \}$ of dimension $n$. Lattice reduction algorithms transform a given basis into a basis consisting of short vectors. $\lambda_1(L) = \min_{b \in L, b \neq 0} (b' b)^{1/2}$ is the minimal length of nonzero $b \in L$. The determinant of $L$ is $\det L = (\det B'B)^{1/2}$. 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 $B$ such that $\|b_1\| \leq \alpha^{-\frac{1}{2\gamma}} \lambda_1$, 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 $\|b_1\|/\lambda_1 \leq (1 + \varepsilon)^{\frac{1}{\gamma_k}}$ of polynomial time reduction algorithms. The algorithm for slide-reduction of [GN08b] 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 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 $\delta, \alpha$ and dimension $n = hk$. It shows under a reasonable assumption that this number is at most $\frac{1}{5} n^2 h \log_{1+\varepsilon} \alpha$. 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 $\frac{1}{2} 2^{\frac{2}{3} k^2 h^3} (1 + \log_{1+\varepsilon} \gamma_k / 2)$, reducing the number by a factor $2k^{-2} \ln \gamma_k / \ln \alpha$. 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., 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 $\max_j \|b_j\|^2/\|b_j^*\|^2 \leq \frac{1}{2}$ 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 $R' = [r_{i,j}]_{k \leq i \leq k+1}$ be the submatrix of $R = [r_{i,j}] \in \mathbb{R}^{m \times n}$ for the $\ell$-th block, $D_\ell = (\det R)_{\ell}$, and $R'_k = [r_{i,j}]_{k \leq i \leq k+1} \subseteq \mathbb{R}^{k \times k}$ for the $\ell$-th block sliding by one unit. $R'_k^* = (R'_k)^*$ is the dual of $R'_k$. $(R'_k)^* = U_k R'_k^\top U_k$ for $R'_k \in \mathbb{R}^{k \times k}$, where $R_k^{-1}$ 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 $i = 1, \ldots, k$. Let max$_{R'_k \in \mathbb{R}^{k \times k}}$ denote the maximum of $\|R'_k\|_\ell$ for all $T \in \text{GL}_k(\mathbb{Z})$ with QR-decomposition $R'_k = Q' \cdot \text{GNF}(R'_k)$.

### Definition 1
1. [GN08] An LLL-basis $B = QR \in \mathbb{R}^{m \times n}$, $n = kh$ is slide-reduced for $\varepsilon \geq 0$ if
   1. $r_{k-\ell-k+1,k-\ell+1} = \lambda_\ell(L(R))$ for $\ell = 1, \ldots, h$,
   2. $\max_{R'_k \in \mathbb{R}^{k \times k}} \leq \sqrt{1 + \varepsilon} \cdot r_{k-\ell-k+1,k-\ell+1}$ holds for $\ell = 1, \ldots, h-1$.

2. 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. $\|b_i\| \leq \left((1 + \varepsilon)\gamma_\ell\right)^{\frac{1}{2}} (\det L)^{1/n}$,
   4. $\|b_i\| \leq \left((1 + \varepsilon)\gamma_\ell\right)^{\frac{1}{2}} (\det L)^{1/n}$.

### 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 $\ell = \ell_{\max}$ that maximizes $D_\ell/D_{\ell+1}$,

1. $r_{k-\ell-k+1,k-\ell+1} = \lambda_\ell(L(R))$ for $\ell = 1, \ldots, h$,
2. $\max_{R'_k \in \mathbb{R}^{k \times k}} \leq \sqrt{1 + \varepsilon} \cdot r_{k-\ell-k+1,k-\ell+1}$ holds for $\ell = \ell_{\max}$ 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 $\ell = \ell_{\max}$ that maximizes $D_\ell/D_{\ell+1}$. Compute a shortest vector of $\ell(L(R))$ and transform $R_{\ell+1}$ and $B$ such that $r_{k-\ell-k+1,k-\ell+1} = L(R_{\ell+1})$. By an SVP-computation for $L(R_{\ell+1})$ check that 2 holds for $\ell$ and if 2 does not hold transform $R'_k$ and $B$ such that 2 holds for $\varepsilon = 0$ (this decreases $D_\ell$ by a factor $\leq (1 + \varepsilon)^{\varepsilon} - 1$) otherwise terminate.

On termination continue with this transform on $R_\ell, R_{\ell+1}, B$ for $\ell = \ell_{\max}$ and $h = h - 1$ until 2 holds for both $\ell = \ell_{\max}$ 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 $B \in \mathbb{Z}^{m \times n}$ for $\delta \leq 1$, $\alpha = 1/(\delta - 1/4)$, $n = hk$, within $\frac{1}{2} n^2 h \log_2 \alpha n = n^2 h \frac{1}{4^\varepsilon} \ln \alpha$ rounds of 2 local SVP-computations either into an almost slide-reduced basis for $\varepsilon > 0$, or else arrives at $D(B) < 1$,

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

**Fact.** Each round that does not lead to termination results in
$$\mathcal{D}_{t+1}^{new} \leq \mathcal{D}_t(1 + \varepsilon) \quad \mathcal{D}(B^{new}) \leq \mathcal{D}(B)/(1 + \varepsilon)^2.$$  
This is because the round changes merely the factor \( \prod_{t=t-1,t,t+1} (D_t/D_{t+1})^{(h-t)} = (D_t/D_{t+1}) D_t^2 \) of \( \mathcal{D}(B) \), where \( D_tD_{t+1} \) does not change. Hence, after at most
$$\frac{1}{\varepsilon} \log_1 \mathcal{D}(B^{(in)}) \leq \frac{1}{\varepsilon} \log_1 (\alpha^{s^2/2}) = \frac{1}{\varepsilon} k^2 \frac{k^3 - 3k}{6} \log_1 \alpha \leq \frac{3k}{12} \log_1 \alpha$$
rounds either \( B \) is almost slide-reduced for \( \varepsilon \) or else \( \mathcal{D}(B) \leq 1 \). The \( \frac{3k}{12} \log_1 \alpha \) bound includes the rounds on termination. Clearly \( \log_1 \alpha = \log \alpha / \log(1 + \varepsilon) \) and \( 1/\log(1 + \varepsilon) = \frac{1 + O(\varepsilon)}{\varepsilon} \). \( \square \)

**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 \( \Pr(t) = D_{t+1}^{h-1}/D_t^h \). (We have \( \sum_{t=1}^{n-1} \Pr(t) = 1 \).) 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 exponential 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 \( t = 1, \ldots, h \) 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 \( \frac{3k}{12} \log_1 \alpha \) 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 bitlength of \( B \) and requires only minor conditions on the input and output basis. As \( \text{size}(B) \approx \sum_{i=1}^n \log_2 \| b_i \| \) our \( \frac{3k}{12} \log_1 \alpha \) bound is better than the \( O(nh(\text{size}(B))/\varepsilon) \) bound of [GN08] if \( \frac{1}{\varepsilon} \log \alpha < \frac{1}{12} \sum_{i=1}^n \log_2 \| b_i \| \). 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 \( \delta, \alpha, n = h k \) 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 \( D_t/D_{t+1} \leq ((1 + \varepsilon)\gamma_{k/2})^{\frac{k^3 - 3k}{6} / 2} \) as follows from (3) with blocksize \( k/2 \). Hence
$$\mathcal{D}(B) \leq ((1 + \varepsilon)\gamma_{k/2})^{\frac{k^3 - 3k}{6} / 2}.$$  
As each round decreases \( \mathcal{D}(B) \) by a factor \( (1 + \varepsilon)^{-2} \) we see that
$$\#H \leq \frac{1}{\varepsilon} \log_1 \mathcal{D}(B) \leq \frac{1}{\varepsilon} \frac{k^3 - 3k}{6} \log_1 \alpha \leq \frac{3k}{12} \log_1 \alpha$$
provided that \( \mathcal{D}(B) \geq 1 \) holds on termination. Here \( \log_1 \gamma_{k/2} = \log \gamma_{k/2} / \log(1 + \varepsilon) = \frac{1 + O(\varepsilon)}{\varepsilon} \gamma_{k/2} \).

For \( k = 4 \), resp. \( k = 8 \) this is less than a 0.603, resp. 0.201 fraction of the number of rounds \( \frac{3k}{12} \log_1 \alpha \) 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 \( k = 2^j \) requires only an \( O(k^{-2} \log \gamma_{k/2}) \)-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 \( k/2, n = h k \), ASR finds within
$$\frac{1}{\varepsilon} \frac{3k^3 - 3k}{6} \log_1 \alpha \leq \frac{3k}{12} \log_1 \alpha$$
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 \( 1 + \varepsilon/2 \).

**Proof.** We see from 2 and the Hermite bound on \( \lambda_1(L(R_b^{(in)})^*) = 1/r_{k/2+1}k/2+1 \) that
\[ D'_\ell / r_{2k+1, k+1}^2 \leq ((1 + \varepsilon) \gamma_k)^{2(k-1)} \eta_{k+1, k+1} \]  
holds for \( \ell = \ell_{\text{max}} \) and \( \ell = h - 1 \), where \( D'_\ell \equiv (\det R'_\ell)^2 \). Moreover, the Hermite bound for \( R_\ell \) yields

\[ r_{2k-h+1, k-h-1}^2 \leq \gamma_k D'_\ell / r_{2k-h+1, k-h-1}^2. \]

Combining these two inequalities with \( D'_\ell / r_{2k+1, k+1}^2 = D'_\ell / r_{2k+1, k+1}^2 \) yields

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

Next we prove

\[ D'_\ell / D_{\ell+1} \leq ((1 + \varepsilon) \gamma_k)^{2(k-1)} \gamma_k^{2h} \]  
for \( \ell = 0, \ldots, h - 1 \). \hspace{1cm} (3)

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

\[ D'_\ell \leq (1 + \varepsilon)^{2(k-1)} (1 + \varepsilon)^{2k} \gamma_k^{2h} D_{\ell+1}. \]

We see from (2) that

\[ D'_\ell = r_{2k+1, k+1}^2 / r_{2k+1, k+1} \leq ((1 + \varepsilon) \gamma_k)^{2(k-1)} \] \hspace{1cm} (4)

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

\[ D'_\ell \leq ((1 + \varepsilon) \gamma_k)^{2(k-1)} (1 + \varepsilon)^{2k} \gamma_k^{2h} D_{\ell+1} = ((1 + \varepsilon)^{2(k-1)} \gamma_k)^{2k^2} D_{\ell+1}. \]

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

\[ \|b_1\|^2 \leq \gamma_k D_{1/k}^1 / \gamma_k \] \hspace{1cm} (5)

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

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

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

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

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

\[ \|b_1\|^2 \leq \gamma_k ((1 + \varepsilon)^{2(k-1)} \gamma_k)^{k^2 h/(1-h)} \] \hspace{1cm} (by (4) for \( \ell = h - 1 \))

\[ \leq \gamma_k ((1 + \varepsilon)^{2(k-1)} \gamma_k)^{k^2 h/(1-h)} + (1 + \varepsilon)^{2(k-1)} \gamma_k r_{n-k+1, n-k+1}. \] \hspace{1cm} (by 2 for \( \ell = h - 1 \))

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

(\( \lambda_1 \) of \( \text{basis} \) \( b \) \( \neq 0 \) holds for some \( b \in L \) with \( \|b\| = \lambda_1 \), otherwise we remove the last \( k \) vectors of the basis. Hence \( r_{n-k+1, n-k+1} \leq \|\pi_{n-k+1}^1(b)\| \leq \lambda_1 \)). The latter inequalities yield the claim

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

We have roughly halved the exponent of \((1 + \varepsilon)\) in 3 and 4 multiplying it by at most \( 1 + \varepsilon \).

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

\[ 2^{2m-1} < \max(B'/D_{\ell+1}) \gamma_k^{2k^2} \leq 2^{2m}. \] \hspace{1cm} (6)

This integer \( m \) exists if and only if \( \max(b'/D_{\ell+1}) > \gamma_k^{2k^2} \)

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

Multiplying this inequality with \( 2^{2m-1} \gamma_k^{2k^2} < D_{\ell+1}^{\text{old}} / D_{\ell+1}^{\text{old}} \) and \( D_{\ell+1}^{\text{new}} / D_{\ell+1}^{\text{new}} \) yields
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 $\varepsilon < \frac{k-1}{2\varepsilon^2}(2^m M_0)$ then $\max_{\ell}(D_{\ell}/D_{\ell+1}) \leq \frac{2k^2}{\varepsilon^2}$. 

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

$$\varepsilon \leq \frac{k-1}{2\varepsilon^2} 2^m.$$ (8)

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

$$\max_{\ell}(D'_{\ell}/D'_{\ell+1}) \approx (1 + \varepsilon')h_{\ell+1,k+1}$$ for some $\ell$. It follows from [LLL82, (1.28)] for the integer matrix $B$ that $h_{\ell+1,k+1}M_0^\varepsilon \geq 1$ and thus

$$\varepsilon' \geq \frac{(\max_{\ell}(D'_{\ell}/D'_{\ell+1} - h_{\ell+1,k+1})/h_{\ell+1,k+1})}{1/M_0^\varepsilon}.$$ (3) and (6) imply $2^{m-1} < (1 + \varepsilon')\frac{2k^2}{\varepsilon^2}$, and thus $2^{m-1} < \frac{2k^2}{\varepsilon^2} \log_2(1 + \varepsilon) < \frac{2k^2}{\varepsilon^2} \frac{\varepsilon}{\varepsilon}. \log_2 2^m$. Hence $n > |\log_2 M_0|$ which is impossible. This implies by (6) that $\max_{\ell}(D_{\ell}/D_{\ell+1}) \leq \frac{2k^2}{\varepsilon^2}$. \square

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

$$\#H_m \leq \log_2(D(B^{(m)})/D(B^{(f\ell)}))2^{m-1} \leq \log_2(\frac{2m^3}{\varepsilon^2})/2^{m-1} = \frac{h^{3-h}}{3}.$$ (9)

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 $m < 0$ 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 $D(B) \leq \frac{2k^2}{\varepsilon^2} \frac{h^{3-h}}{3}$. $D(B) < \frac{2k^2}{\varepsilon^2} \frac{h^{3-h}}{3}$ implies that $E[\ln(D_{\ell}/D_{\ell+1})] \leq \frac{2k^2}{\varepsilon^2} \ln \gamma_k$ holds for random $\ell$, where $\Pr(\ell) = 6^{h_{\ell+1,k+1}}/\varepsilon$ \square. 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 $\frac{h^{3-h}}{3}(m + |m_0|)$ 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 $\max_{\ell}(D_{\ell}/D_{\ell+1}) \geq \frac{2k^2}{\varepsilon^2}$ holds for each round. Thus by (7) and ET for the initial and final bases for the reduction of $m$ to $m - 1$:

$$\#H_m \leq \log_2(D(B^{(m)})/D(B^{(f\ell)}))2^{m-1} \leq \log_2(\frac{2m^3}{\varepsilon^2})/2^{m-1} = \frac{h^{3-h}}{3}.$$ (9)

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

**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 $\max_{\ell}(\|b_\ell\|^2, \|b_{\ell+1}\|^2 > \frac{1}{\varepsilon})$ the integer $m$ defined by
\[
2^{m-1} < \max \|b_i^*\|^2/\|b_{i+1}^*\|^2 \leq 2^m. \quad (9)
\]
If \(m \geq 0\) we transform in the current round \(b_i, b_{i+1}\) for an \(\ell\) that maximizes \(\|b_i^*\|^2/\|b_{i+1}^*\|^2\) by Gauß-reducing the basis \(\pi_i(b_i), \pi_{i+1}(b_{i+1})\) of dimension 2. (Gauß-reducing the basis \(\pi_i(b_i), \pi_{i+1}(b_{i+1})\) means to LLL-reduce \(\pi_i(b_i), \pi_{i+1}(b_{i+1})\) with \(\delta = 1\).) This decreases \(\|b_i^*\|^2\) by a factor less than \(2^{-2^m} < \frac{1}{2}\).

If \(m < 0\) or \(m = 0\) does not exist, we transform in the current round \(b_i, b_{i+1}\) for an \(\ell\) that maximizes \(\|b_i^*\|^2/\|\pi_{i+1}(b_{i+1})\|^2\) after size-reducing \(b_{i+1}\) against \(b_i\) by setting \(b_{i+1} := b_{i+1} - \lfloor r_{i+1}/\ell \rfloor b_i\). If \(\|\pi_{i+1}(b_{i+1})\|^2 \leq \delta\|b_i^*\|^2\) we swap \(b_i, b_{i+1}\) 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 \(\delta\) satisfying \(1 > \delta > \max(\delta', \frac{1}{2})\) arrives within \(\frac{n^3}{12} \log_4\alpha'\) rounds of Gauß-reductions, resp. LLL-swaps either at an LLL-basis for \(\delta\), or else arrives at \(\mathcal{D}(B) := \prod_{t=1}^{n-1}(\|b_i^*\|^2/\|b_{i+1}^*\|^2)^{(n-t)} < 1\).

**Proof.** We use \(\mathcal{D}(B)\) for blocksize 1, \(\mathcal{D}(B) := \prod_{t=1}^{n-1}(\|b_i^*\|^2/\|b_{i+1}^*\|^2)^{(n-t)}\). Each round decreases \(\|b_i^*\|^2\) by a factor \(\delta\), and both \(\|b_i^*\|^2/\|b_{i+1}^*\|^2\), \(\mathcal{D}(B)\) by a factor \(\delta^2\). Then the number of rounds until either an LLL-basis for \(\delta\) appears or else \(\mathcal{D}(B) \leq 1\) is at most
\[
\frac{1}{2} \log_{1/\delta} \mathcal{D}(B) \leq \frac{1}{2} \log_{1/\delta}(\alpha') \frac{n^3}{12} \log_4\alpha'.
\]

**The work per round.** If each round completely size-reduces \(b_i, b_{i+1}\) 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 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 \(\max \|b_i^*\|^2/\|b_{i+1}^*\|^2 \leq \frac{4}{3}\).

**Proof.** The LLL-basis \(B\) satisfies \(\|b_i^*\|^2 \leq \frac{1}{8 \times 1/4} \|b_{i+1}^*\|^2\). Therefore (9) implies \(2^{m-1} < \frac{1}{8 \times 1/4} \frac{3}{4}\).

Setting \(\delta = 1 - \varepsilon\) this shows that
\[
2^{m-1} < \log_2 \frac{3}{4} - \log_2 \frac{1}{8} = \log(1 - 4^{-\varepsilon})/\log 2
\]
\[
< -1.45 \frac{\varepsilon}{4} < 2^{-n/2}/M_0,
\]
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 \(\max \|b_i^*\|^2/\|b_{i+1}^*\|^2 \leq \frac{4}{3}\).

**Corollary 3.** Let \(m\) be the \(m\)-value of the input basis and \(c \in \mathbb{Z}\) \(c \geq 0\) be constant. Within \(\frac{2^m}{3}(m + 222 \cdot 2^m)\) rounds ALR either decreases the initial \(m\) to \(m \leq -c\) or else arrivers at \(\mathcal{D}(B) < 1\). 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
\[
\frac{n/2^m}{3} (2^m/2^{m-1} + 2^{-m+1} \log_2 \sqrt{1/3})
\]
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
\[
\frac{n}{3} (2^m + 2^m \log_2 \sqrt{1/3}) \sum_{n-e} 2^{-i} < \frac{n}{3} (m + 2^m \log_2 \sqrt{1/3}) < \frac{n}{12} (m + 2.22 \cdot 2^m)
\]
rounds to \(m = -|c|\) or else arrives at \(\mathcal{D}(B) < 1\)

The bound \(m \leq \log_2 n + \log_2 \log_2 M_0\) follows from (9) and \(\|b_{i+1}^*\|^2 \geq 1/M_0^2\).
The number of rounds in Cor. 3 is independent of \( M_0 \). This is because \textsc{ALR} maximizes the reduction progress per round. To minimize the workload of size-reduction \textsc{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 \( \pi(b_\ell), \pi_\ell(b_{\ell+1}) \) is quasi-linear in size(\( B \)) [NSV10]. Therefore we do not split up this Gauß-reduction into \textsc{LLL}-swaps. If the current \( m \) is large then Gauß-reduction of \( \pi_\ell(b_\ell), \pi_\ell(b_{\ell+1}) \) for \( \ell = \ell_{\text{max}} \) decreases \( \mathcal{D}(B) \) be the factor \( 2^{-m} \) while \textsc{LLL}-swaps guarantee only a decrease by the factor \( \frac{3}{2} \).

The algorithm for \textsc{LLL-reduction} with fixed complexity iterates all possible \textsc{LLL}-swaps of \( b_\ell, b_{\ell+1} \) for \( \ell = 1, ..., n-1 \). If this algorithm would not just do \textsc{LLL}-swaps but Gauß-reductions of \( \pi_\ell(b_\ell), \pi_\ell(b_{\ell+1}) \) for all \( \ell \) its number of rounds would be at most \( n-1 \) times the number of rounds \( \frac{n^3}{17} \log_3/3 A' \) of \textsc{ALR}.

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

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

**Corollary 4.** \textsc{ALR} terminates under \textsc{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 \#1 \( m \) of rounds until either the current \( m \) decreases to \( m-1 \) or else \( \mathcal{D}(B) \) becomes less than \( (4/3)^{\frac{n^3-n}{2}} \). As in the proof of Corollary 2 each round with \( m \) results in Gauß-reduction under \( \pi_\ell \) if \( m_\ell \geq 0 \), resp. an \textsc{LLL}-swap if \( m_\ell < 0 \), results in

\[ ||b_\ell^{\text{new}}||^2 < ||b_\ell^{\text{old}}||^2 2^{-2m-2} \] hence \( \mathcal{D}(B^{\text{new}}) < \mathcal{D}(B^{\text{old}})/2^{-2m-1} \).

Under \textsc{ET} this shows as in the proof of Cor. 1 that

\[ \#1 \leq \log_2 \mathcal{D}(B^{\text{init}})/(\mathcal{D}(B^{\text{fin}}))/2^{-m-1} \leq (2^m n^3/6)^{2m-1} = \frac{n^3}{3} \]

Hence \( m \) decreases to \( m-1 \) under \textsc{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 \textsc{ALR} realize max \( \max \pi_\ell ||b_\ell||^2 ||b_{\ell+1}||^2 \leq \left( \frac{3}{4} \right)^{\frac{n^3-n}{2}} \) in a polynomial number of rounds ? Can \textsc{ALR} perform for \( m \leq 0 \) without \textsc{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 \textsc{ET} also for \( m < 0 \).

**References**


