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 13, 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 $\frac{1}{4} n^2 h \log_{1+k} \alpha$ 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 $\frac{1}{2} h^{3}(1+ \log_{1+k} \gamma_{k/2})$. 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 $B = [b_1, \ldots, b_n] \in \mathbb{R}^{m \times n}$ of $n$ linear independent vectors $b_1, \ldots, b_n$ 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. $\lambda_1(L) = \min_{b \in \mathcal{L}, b \neq 0} \langle b, b \rangle^{1/2}$ is the minimal length of nonzero $b \in \mathcal{L}$. The determinant of $\mathcal{L}$ is $\det \mathcal{L} = (\det B^t B)^{1/2}$. The Hermite bound $\lambda_1(L)^2 \leq \gamma_n(\det \mathcal{L})^{2/n}$ 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 $\|b_1\| \leq \alpha^{-\frac{1}{2\alpha}} \lambda_1$, 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 [SS87] 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 $\|b_1\|/\lambda_1 \leq (1+\varepsilon)\gamma_{k/2}$ 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 $\text{size}(B)$ 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 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 $\frac{1}{8} n^2 h \log_{1+k} \alpha$. 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 $\frac{1}{8} n^2 h^{3}(1+ \log_{1+k} \gamma_{k/2})$, 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 \(\frac{1}{12} \log_2 \text{size}(B)\) 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 \(1 - \delta \leq 2^{n-2}2^{-\text{size}(B)}\) satisfies the property \(\max_i |\|b_i^*\||^2/|\|b_i^*\||^2 \leq \frac{4}{5}\) 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 \(R = [r_{i,j}]_{1 \leq i \leq j \leq kt}\) 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 \(R'_\ell = [r_{i,j}]_{k-\ell+2 \leq i,j \leq kt}\) for the \(\ell\)-th block sliding by one unit. \(R'^* = (R'^*)^*\) is the dual of \(R'_\ell\). \(R'^* = U^j U^i R'^* U_k\) 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 \(\max_{\ell \in T} R_{\ell+1,k+1} = 1/\lambda_1(L(R'^*_{\ell+1}))\). Let \(\pi : \mathbb{R}^n \rightarrow \text{span}(b_1,\ldots,b_{i-1})^\perp\) 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 \(\delta = 1/4 < \delta \leq 1\) if
- \(|r_{i,j}| \leq 1/2r_{i,i}\) holds for all \(j > i\),
- \(\delta r_{i,i}^2 \leq r_{i,i+1} + r_{i+1,i+1}\) holds for \(i = 1,\ldots,n-1\).

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

\[|\|b_i\|| \leq \alpha^{-1/n}(\det L)^{1/n}, \quad |\|b_i\|| \leq \alpha^{-n/(n-1)}\lambda_i.\]

**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. \(r_{k-\ell+k+1,k+1} = \lambda_1(L(R_\ell))\) for \(\ell = 1,\ldots,h\),
2. \(\max_{\ell \in T} k\ell + 1, k\ell + 1 \leq \sqrt{1 + \varepsilon} \cdot r_{k\ell+1,k+1}\) 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. \(|\|b_i\|| \leq (1 + \varepsilon)(\gamma_\ell)^{-\frac{1}{k\ell+1}}(\det L)^{1/n},\)
4. \(|\|b_i\|| \leq (1 + \varepsilon)(\gamma_\ell)^{-\frac{k\ell}{k\ell+1}}\lambda_i.\)

**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. \(r_{k\ell-k+1,k\ell-k+1} = \lambda_1(L(R_\ell))\) for \(\ell = 1,\ldots,\ell_{\max}\),
2. \(\max_{\ell \in T} k\ell + 1, k\ell + 1 \leq \sqrt{1 + \varepsilon} \cdot r_{k\ell+1,k+1}\) 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 \(L(R_{\ell+1})\) and transform \(R_{\ell+1}\) and \(B\) such that \(r_{k\ell+1,k\ell+1} = \lambda_1(L(R_{\ell+1}))\). By an SVP-computation for \(L(R'^*_{\ell+1})\) check that 2 holds for \(\ell = \ell_{\max}\) and if 2 does not hold transform \(R'^*\) 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 \(R_{\ell+1}, B\) for \(\ell = \ell_{\max}\) and \(\ell = h-1\) until 2 holds for both \(\ell = \ell_{\max}\) and \(\ell = h-1\). Finally make sure that 1 holds for \(\ell = 1\) and size-reduce \(B\).

Theorem 1. Accelerated slide-reduction transforms a given LLL-basis \(B \in \mathbb{Z}^{m \times n}\) for \(\delta \leq 1\), \(\alpha = 1/\delta - 1/4\), \(n = hk\), within \(\frac{1}{12} \log_2 \lambda_1(B) \alpha n^2 \log_2 \alpha \approx n^2 \log_2 \alpha \approx \alpha n^2 \log_2 \alpha \) in \(\alpha\) rounds of 2 local SVP-computations either into an almost slide-reduced basis for \(\varepsilon > 0\), or else arrives at \(D(B) < 1\), where
\[D(B) = \det \prod_{\ell=1}^{n-1} (D_\ell/D_{\ell+1})^{k\ell-\ell^2} = (\det L)^{2h}/\prod_{\ell=1}^{h} D_{\ell+1}^{2h}.\]

Proof. We use the novel version \(D(B)\) of the Lovász invariant to measure \(B\)’s reduction. Note that \(h^2/4 - (\ell - h/2)^2 = h\ell - \ell^2\) is symmetric to \(\ell = h/2\) with maximal point \(\ell = [h/2]\).

The input LLL-basis \(B'(\alpha)\) for \(\delta \leq 1\) satisfies for \(\alpha = 1/\delta - 1/4\) that \(D_\ell/D_{\ell+1} \leq \alpha^2\) and thus
\[ \mathcal{D}(B^{(\pi)}) \leq \alpha ^{s^2} \quad \text{for} \quad s := \sum_{t=1}^{h} h \ell - \ell^2 = \frac{h^2 - h}{6}. \]

**Fact.** Each round that does not lead to termination results in
\[ \mathcal{D}'^{(\text{new})} \leq \mathcal{D}_t/(1 + \varepsilon) \]
\[ \mathcal{D}(B^{(\text{new})}) \leq \mathcal{D}(B)/(1 + \varepsilon)^2. \]

This is because the round changes merely the factor \( \prod_{t=t-1,t,t+1} (\mathcal{D}_t/\mathcal{D}_{t+1})^{h-t} = (\mathcal{D}_t/\mathcal{D}_{t+1}) \mathcal{D}_t^2 \) of \( \mathcal{D}(\mathcal{D}) \), where \( \mathcal{D}_t/\mathcal{D}_{t+1} \) does not change. Hence, after at most
\[ \frac{1}{2} \log_{1+\varepsilon} \mathcal{D}(B^{(\text{new})}) \leq \frac{1}{2} \log_{1+\varepsilon} (\alpha ^{s^2}) = \frac{1}{2} k^2 \log_{1+\varepsilon} \alpha \leq \frac{2^h}{12} \log_{1+\varepsilon} \alpha \]
rounds either \( B \) is almost slide-reduced for \( \varepsilon \) or else \( \mathcal{D}(B) \leq 1 \). The \( \frac{2^h}{12} \log_{1+\varepsilon} \alpha \) bound includes the rounds on termination. Clearly \( \log_{1+\varepsilon} \alpha = \ln \alpha / (1 + \varepsilon) \) and \( 1/\ln(1 + \varepsilon) = 1/(1 + \varepsilon) = 1 + O(\varepsilon^3) \).

**Corollary.** 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 \( \mathcal{E}[\ln(\mathcal{D}_t/\mathcal{D}_{t+1})] < 0 \) holds for the expectation \( \mathcal{E} \) for random \( \ell \) with \( \Pr(\ell) = 6/(h^2 \ell^2) \). (We have \( \sum_{\ell=1}^{n} \Pr(\ell) = 1 \).) In this sense \( \mathcal{D}_t < \mathcal{D}_{t+1} \) would hold "on the average" if \( \mathcal{D}(B) < 1 \) whereas such \( \mathcal{D}_t, \mathcal{D}_{t+1} \) 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 by at best a factor \( h-1 \) because the [GN08] algorithm iterates all rounds for \( \ell = 1, ..., h \) 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 \( \frac{2^h}{12} \log_{1+\varepsilon} \alpha \) 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 \( \text{size}(B) \approx \sum_{i=1}^{n} \log_b ||b|| \) our \( \frac{2^h}{12} \log_{1+\varepsilon} \alpha \) bound is better than the \( O(nh \text{size}(B)/\varepsilon) \) bound of [GN08] if \( \frac{1}{6} \ln \alpha < \frac{1}{6} \sum_{i=1}^{n} \log_b ||b|| \). The latter holds in most cases.

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

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

We bound the number \#It of rounds of the last ASR-call with blocksize \( k = 2^\ell \). The input \( B \) of this final ASR-call satisfies
\[ \mathcal{D}_t/\mathcal{D}_{t+1} \leq ((1 + \varepsilon) \gamma_{k/2})^{1/2-\ell/4} \]
as follows from (3) with blocksize \( k/2 \). Hence
\[ \mathcal{D}(B) \leq ((1 + \varepsilon) \gamma_{k/2})^{1/2-\ell/4}. \]

As each round decreases \( \mathcal{D}(B) \) by a factor \( (1 + \varepsilon)^{-2} \) we see that
\[ \#It \leq \frac{1}{2} \log_{1+\varepsilon} \mathcal{D}(B) \leq \left( \frac{k}{k^2} - \frac{k^3 - h}{12} \log_{1+\varepsilon} ((1 + \varepsilon) \gamma_{k/2}) = \frac{h^2}{12} \log_{1+\varepsilon} (1 + \varepsilon) \gamma_{k/2}. \]

provided that \( \mathcal{D}(B) \geq 1 \) holds on termination. Here \( \log_{1+\varepsilon} \gamma_{k/2} = \ln \gamma_{k/2} / (1 + \varepsilon) = 1 + O(1) \gamma_{k/2}. \)

For \( k = 4 \), resp. \( k = 8 \) this is less than a 0.603, resp. 0.201 fraction of the number of rounds \( \frac{2^h}{12} \log_{1+\varepsilon} \alpha \) 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 \( k = 2^\ell \) 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 \( \frac{1}{2} \left( \frac{h^2}{12} \right) \log_{1+\varepsilon} ((1 + \varepsilon) \gamma_{k/2}) \) rounds of two local SVP-computations either an almost slide-reduced basis for blocksize \( k \) and \( \varepsilon \) or else arrives at \( \mathcal{D}(B) < 1 \).

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

**Proof.** We see from 2 and the Hermite bound on \( \lambda_1(L(R'_s)^*) = 1/\tau_{k,t+1,k,t+1} \) that

3
\[ D'_\ell/r^2_{k\ell+1,k\ell+1} \leq ((1 + \varepsilon)\gamma_k)^{\frac{2(k-1)}{k}} D'_\ell/k \tag{1} \]

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

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

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

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

Next we prove

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

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

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

We see from (2) that

\[ D_{\ell} = r^2_{k\ell-k+1,k\ell-k+1} D'_\ell/r^2_{k\ell-k+1,k\ell-k+1} \leq ((1 + \varepsilon)\gamma_k)^{\frac{2(k-1)}{k}} D'_\ell. \tag{4} \]

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

\[ D_{\ell} \leq ((1 + \varepsilon)\gamma_k)^{\frac{2k^2}{k}} ((1 + \varepsilon)^{\frac{1+1/k}{k}} \gamma_k)^{\frac{2k^2}{k}} D_{\ell+1} \]

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

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

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

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

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

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

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

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

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

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

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

Thus we get

\[ \|b_1\|^2 \leq \gamma_k ((1 + \varepsilon)^{\frac{1+1/k}{k}} \gamma_k)^{\frac{2(k-1)}{k}} r_{n-k+1,n-k+1}^2 \]

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

\[ \|b_1\| \leq ((1 + \varepsilon)^{\frac{1+1/k}{k}} \gamma_k)^{\frac{2(k-1)}{k}} \lambda_1. \]

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

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

\[ 2^{m-1} < \max(D_{\ell}/D_{\ell+1}) \gamma_k^{-\frac{2k^2}{k}} \leq 2^m. \tag{6} \]

This integer \( m \) exists if and only if \( \max_{\ell}(D_{\ell}/D_{\ell+1}) \gamma_k^{-\frac{2k^2}{k}} \)

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

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

\[ D^\text{new}_{\ell+1}/D^\text{new}_{\ell+1} \leq \gamma_k^{\frac{2k^2}{k}} \]

4
\[ 2^{2m-2}D_t^{\text{new}} \leq D_t^{\text{old}} \quad \text{hence} \quad D(B^{\text{new}}) \leq D(B^{\text{old}}) 2^{-2m-1}. \]  

(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 \( \varepsilon < \frac{k-1}{k-2}2^{\log \gamma_k} \) then \( \max_{\ell} (D_t/D_t+1) \leq \gamma_k^{2k^2} \).

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

\[ \varepsilon < \frac{k-1}{k-2} \leq \frac{2k^2}{\gamma_k}. \]  

(8)

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

\[ \max_{\ell} (D_t^{\prime}/D_t^{\prime}+1) \approx (1 + \varepsilon')_{r_t+1, k_t+1} \quad \text{for some } \ell. \]

It follows from [LLL82, (1.28)] for the integer matrix \( B \) that \( r_{k+1, k_t+1} M_0^0 \geq 1 \) and thus

\[ \varepsilon' \geq (\max_{\ell} (D_t^{\prime}/D_t^{\prime}+1) - r_{k+1, k_t+1})/r_{k+1, k_t+1} \geq 1/M_0. \]

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

Next we bound the number \#\( H_m \) of rounds until the current \( m \) decreases to \( m - 1 \) or arrives at \( D(B) < 1 \).

Moreover, initially \( \max_{\ell} (D_t/D_t+1) \leq \gamma_k^{2k^2} 2^{2m} \). This shows for the initial and final bases for the reduction of \( m \) to \( m - 1 \):

\[ \#H_m \leq \log_2(D(B^{\text{fin}})/D(B^{\text{old}})) 2^{m-1} \]

\[ \leq \frac{\log_2(2^{m}/2^{m-1} + 2^{-m+1}2k^2/m \log_2 \gamma_k)}{2^{m-1}}. \]

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 \( D(B) < \gamma_k^{2k^2} \cdot \frac{k-3}{k-2} \).

\[ D(B) < \gamma_k^{2k^2} \cdot \frac{k-3}{k-2} \implies \text{ET} \]

implies \( \mathbb{E}[\ln(D_t/D_t+1)] < \frac{2k^2}{k-2} \ln \gamma_k \) holds for random \( \ell \), where \( \mathbb{E}(\ell) = 6 \log_2 \gamma_k \). 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 \( \max_{\ell} (D_t/D_t+1) \geq 2^{2m-1} \gamma_k^{2k^2} \). This implies by (7) and ET for the initial and final bases for the reduction of \( m \) to \( m - 1 \):

\[ \#H_m \leq \log_2(D(B^{\text{fin}})/D(B^{\text{old}})) 2^{m-1} \leq \log_2(2^{m} \cdot \gamma_k^{2k^2} \gamma_k^{k-3}/3). \]

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

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.

**Accelerated LLL-reduction (ALR).** We accelerate LLL-reduction by performing either Gauß-reductions or LLL-swaps on \( b_1, b_{k+1} \) for an \( \ell \) that maximizes the resulting reduction progress.

We associate to a basis \( B \) satisfying \( \max_{\ell} \|b_1\|^2, \ldots, \|b_n\|^2 \) the integer \( m \) defined by
\[ 2^{m-1} < \max \| \mathbf{b}_i^* \|^2 / \| \mathbf{b}_{i+1}^* \|^2 \leq 2^m. \]  
\[ (9) \]

If \( m \geq 0 \) we transform in the current round \( \mathbf{b}_i, \mathbf{b}_{i+1} \) for an \( \ell \) that maximizes \( \| \mathbf{b}_i^* \|^2 / \| \mathbf{b}_{i+1}^* \|^2 \) by Gauß-reducing the basis \( \pi_{\ell}(\mathbf{b}_i), \pi_{\ell}(\mathbf{b}_{i+1}) \) of dimension 2. (Gauß-reducing the basis \( \pi_{\ell}(\mathbf{b}_i), \pi_{\ell}(\mathbf{b}_{i+1}) \) means to LLL-reduce \( \pi_{\ell}(\mathbf{b}_i), \pi_{\ell}(\mathbf{b}_{i+1}) \) with \( \delta = 1 \).) This decreases \( \| \mathbf{b}_i^* \|^2 \) by a factor less than \( 2^{2m} < \frac{3}{4} \).

If \( m < 0 \) or \( m \) does not exist, we transform in the current round \( \mathbf{b}_i, \mathbf{b}_{i+1} \) for an \( \ell \) that maximizes \( \| \mathbf{b}_i^* \|^2 / \| \pi_{\ell}(\mathbf{b}_{i+1}) \|^2 \) after size-reducing \( \mathbf{b}_{i+1} \) against \( \mathbf{b}_i \) by setting \( \mathbf{b}_{i+1} := \mathbf{b}_i - \left[ r_{\ell,\ell+1}/r_{\ell,\ell}/\mathbf{b}_i \right]. \)

If \( \| \pi_{\ell}(\mathbf{b}_{i+1}) \|^2 \leq \delta \| \mathbf{b}_i^* \|^2 \) we swap \( \mathbf{b}_i, \mathbf{b}_{i+1} \) and otherwise terminate.

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

**Theorem 3.** Given an LLL-basis \( \mathbf{B} \in \mathbb{Z}^{m \times n} \) for \( \delta' < 1 \), \( \alpha' = 1/(\delta' - 1/4) \) ALR with \( \delta \) satisfying \( 1 > \delta > \max(\delta', \frac{1}{3}) \) arrives within \( n^3 \log_3 \alpha' \) rounds of Gauß-reductions, resp. LLL-swaps either at an LLL-basis for \( \delta \), or else arrives at \( \mathcal{D}(\mathbf{B}) := \prod_{i=1}^{n-1} \left( \| \mathbf{b}_i^* \|^2 / \| \mathbf{b}_{i+1}^* \|^2 \right)^{\ell(n-i)} < 1 \).

**Proof.** We use \( \mathcal{D}(\mathbf{B}) \) for blocksize 1, \( \mathcal{D}(\mathbf{B}) := \prod_{i=1}^{n-1} \left( \| \mathbf{b}_i^* \|^2 / \| \mathbf{b}_{i+1}^* \|^2 \right)^{\ell(n-i)} \). Each round decreases \( \| \mathbf{b}_i^* \|^2 \) by a factor \( \delta \), and both \( \| \mathbf{b}_i^* \|^2 / \| \mathbf{b}_{i+1}^* \|^2 \), \( \mathcal{D}(\mathbf{B}) \) by a factor \( \delta^2 \). Then the number of rounds until either an LLL-basis for \( \delta \) appears or else \( \mathcal{D}(\mathbf{B}) \leq 1 \) is at most

\[ \frac{1}{4} \log_3 \alpha' \mathcal{D}(\mathbf{B}) \leq \frac{1}{4} \log_3(\alpha') \frac{n^3}{\ell} \leq \frac{n^3}{\ell} \log_3 \alpha' . \]

**The work per round.** If each round completely size-reduces \( \mathbf{b}_1, \mathbf{b}_{i+1} \) against \( \mathbf{b}_1, \ldots, \mathbf{b}_{i+1} \) it requires \( O(n^2) \) arithmetic steps. If we only size-reduce \( \mathbf{b}_{i+1} \) against \( \mathbf{b}_i \) 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 \( \mathbf{B} \) is LLL-basis for \( \delta \) and \( 1 - \delta < 2^{-n/2}/M_0 \) then \( \max \| \mathbf{b}_i^* \|^2 / \| \mathbf{b}_{i+1}^* \|^2 \leq \frac{4}{9} \).

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

\[ 2^{m-1} < \log_2 \frac{3}{n^2} < \log_2 \frac{3}{n^2} \frac{1}{4} = \log_2 \frac{1}{4} + \log_2 2 < -1.45 \frac{3}{4} < 2^{-n/2}/M_0 . \]

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 \( \max \| \mathbf{b}_i^* \|^2 / \| \mathbf{b}_{i+1}^* \|^2 \leq \frac{4}{9} . \)

**Corollary 3.** Let \( m \) be the \( m \)-value of the input basis and \( c \in \mathbb{Z} \) \( c \geq 0 \) be constant. Within \( \frac{3}{4} (m + 2.22 \cdot 2^m) \) rounds \( \mathbf{ALR} \) either decreases the initial \( m \) to \( m \leq -c \) or else arrives at \( \mathcal{D}(\mathbf{B}) < 1 \). 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 \( \mathbf{ASR} \) with \( k = 2 \) either decreases within at most

\[ \frac{n/2}{3} (2^m / 2^{m-1} + 2^{-m+1} \log_2 \sqrt{1/3}) \]

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

\[ \frac{3}{4} (2m + 2^{m+1} \log_2 \sqrt{1/3}) < \frac{3}{4} (m + 2^{m+1} \log_2 \sqrt{1/3}) < \frac{3}{4} (m + 2^{m+1} \cdot 2^m) \]

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

The bound \( m \leq \log_2 n + \log_2 \log_2 M_0 \) follows from (9) and \( \| \mathbf{b}_{i+1}^* \|^2 \geq 1/M_0^2 . \)

**Comparison with previous algorithms for LLL-reduction.** The LLL was originally proved [LLL82] to be of bit-complexity \( O(n^{5+\varepsilon}(\log_2 M_0)^{2+\varepsilon}) \) performing \( O(n^2 \log_2 \log_2 M_0) \) rounds, each round size-reduces some \( \mathbf{b}_i \) 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 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 hit-complexity of Gauß-reduction of $\pi(b_\ell), \pi(b_{\ell+1})$ is quasi-linear in size$(B)$ [NSV10]. Therefore we do not split up this Gauss-reduction into LLL-swaps. If the current $m$ is large then Gauß-reduction of $\pi(b_\ell), \pi(b_{\ell+1})$ for $\ell = \ell_{\text{max}}$ decreases $D(B)$ be the factor $2^{-m}$ while LLL-swaps guarantee only a decrease by the factor $\frac{3}{4}$.

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

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

$D(B) < \left(\frac{4}{3}\right)^{\frac{n^3-n}{6}}$ implies that $\mathbb{E}[\ln(\|b^*_\ell\|^2/\|b^*_{\ell+1}\|^2)] < \ln(4/3)$ holds for random $\ell$ and $\Pr(\ell) = \frac{\ln(\frac{4}{3})}{2\ln(\frac{4}{3})}$. In this sense the output basis approximates "on the average" the logarithm of the inequality $\|b_1\|/(\det(L))^{1/n} \leq \left(\frac{3}{4}\right)^{\frac{n^3-n}{6}}$ 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 $(4/3)^{\frac{n^3-n}{6}}$. As in the proof of Corollary 2 each round with $m$ results in Gauß-reduction under $\pi$, if $m > 0$, resp. an LLL-swap if $m < 0$, results in

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

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

$$\#I_m < \log_2(D(B^{(m)})/D(B^{(m-1)})) \times 2^{m-1} \leq (2m \frac{n^3-n}{6})/2^{m-1} = \frac{n^3-n}{3}.$$ 

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

**Open problem.** Does ALR realize $\max_\ell \|b^*_\ell\|^2/\|b^*_{\ell+1}\|^2 \leq \frac{4}{3}$ in a polynomial number of rounds? Can ALR perform for $m \ll 0$ without ET more than $O(n^3)$ rounds until either the current $m$ decreases to $m-1$ or that $D(B) \leq 1$? We can exclude this for $m \geq 0$ and under ET also for $m < 0$.

**References**


