Accelerated and Improved 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
February 9, 2012

Abstract. We accelerate the slide-reduction algorithm of [GN08] with blocksize \( k \) to run for a given LLL-basis \( B \) of dimension \( n = hk \) under reasonable assumptions within \( \frac{1}{2} n^2 h \log_{1+\varepsilon} \alpha \) local SVP-computations of dimension \( k \), where \( \alpha \geq \frac{1}{2} \) is 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 \( k/2 \) the \( \frac{1}{2} n^2 h \log_{1+\varepsilon} \alpha \) bound further decreases to \( nh^2(1+\log_{1+\varepsilon} \gamma_{k/2}) \), where \( \gamma_{k/2} \) is the Hermite constant. These bounds are polynomial in \( n \) for arbitrary bit-length of \( B \). Slide-reduced bases for which the approximation factor \( \|b_1\|/\lambda_1 \) is nearly maximal can easily be improved. If \( \|b_1\|/\lambda_1 = \frac{\gamma_k}{\alpha} \) is maximal we can easily find a shortest lattice vector. 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 \( \mathcal{L}(B) = \{ Bx \mid x \in \mathbb{Z}^n \} \) of dimension \( n \). Lattice reduction algorithms transform a given basis into a basis consisting of short vectors. The length of \( b \in \mathbb{R}^m \) is \( \|b\| = (b^*b)^{1/2} \). \( \lambda_1(\mathcal{L}) = \min_{b \in \mathcal{L} \setminus \{0\}} \|b\| \) is the minimal length of nonzero \( b \in \mathcal{L} \). The determinant of \( \mathcal{L} \) is \( \det \mathcal{L} = \det B^*B \). 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 \( \hat{B} \) such that \( \|b_1\| \leq \alpha^{-\frac{1}{n-1}} \lambda_1 \), 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 \( k \geq 2 \) generalizing 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 proven approximation factor \( \|b_1\|/\lambda_1 \leq (1 + \varepsilon)\gamma_k \frac{2}{\alpha} \) 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 the overall workload. [NSV10] shows that the bit complexity of LLL-reduction is quasi-linear in \( \text{size}(B) \). 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] by choosing the blocks for the next local reduction step as to maximize its progress. We first analyze this strategy in minimizing \( \|b_1\|/(\det \mathcal{L})^{1/n} \) by the concept of almost slide reduction and then extend this analysis to minimize \( \|b_1\|/\lambda_1(\mathcal{L}) \). Theorem 1 studies the maximal number of local SVP-computations during almost slide-reduction with blocksize \( k \) for an input LLL-basis \( B \in \mathbb{Z}^{n \times n} \) 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 is independent of the bit-length of \( B \). Corollary 1 shows that if the given basis is almost slide-reduced for blocksize \( k/2 \) the number of local SVP-computations for almost slide-reduction with blocksize \( k \) further decreases to \( nh^2(1+\log_{1+\varepsilon} \gamma_{k/2}) \), halving the bound of Theorem 1 for \( k = 32 \). For the first time this qualifies the advantage of first performing block reduction with half
the blocksize. Theorem 4 shows that given a slide-reduced basis for blocksize \( k \) and \( \varepsilon = 0 \) such that \( \|b_1\|/\lambda_1 = \gamma_{\frac{k+1}{k}} \) is maximal, we can easily find a shortest lattice vector. More generally, this indicates that the closer \( \|b_1\|/\lambda_1 \) is to the maximum for slide-reduced bases of dimension \( n \) and blocksize \( k \) the easier it is to find a nonzero lattice vector \( b \) that is substantially shorter than \( b_1 \).

We point to such an algorithm.

We also accelerate LLL-reduction. Corollary 3 shows, under a reasonable assumption, that accelerated LLL-reduction computes an LLL-basis within \( n^3 \log_2 \log \text{size}(B) / 3 \) local LLL-reductions of dimension 2. This bound is polynomial in \( n \) if \( \log_2 \text{size}(B) = n^{O(1)} \). Lemma 2 shows that every LLL-basis for \( \delta \) such that \( 1 - \delta \leq 2^{-4\text{size}(B)} \) is an ideal LLL-basis for \( \delta = 1 \).

**Notation.** Let \( B = [b_1, \ldots, b_n] \in \mathbb{R}^{m \times n} \) be a basis matrix of rank \( n = \text{rk}(B) \) and \( B = QR \) be its QR-decomposition, where \( R = [r_{i,j}]_{1 \leq i,j \leq n} \in \mathbb{R}^{n \times n} \) is upper triangular with positive diagonal entries \( r_{i,i} > 0 \) and \( Q \in \mathbb{R}^{m \times n} \) is isometric with pairwise orthogonal column vectors of length 1. We denote \( \text{GNF}(B) = R \). Let \( R_{\ell} = [r_{i,j}]_{\ell \leq i < j \leq \ell + k} \in \mathbb{R}^{k \times k} \) be the submatrix of \( R = [r_{i,j}]_{1 \leq i,j \leq n} \in \mathbb{R}^{n \times n} \) for the \( \ell \)-th block of blocksize \( k \geq 2 \), \( D_{\ell} = (\det R_{\ell})^2 \). Let \( R_{\ell}^* = [r_{i,j}]_{\ell \leq i < j \leq \ell + k} \in \mathbb{R}^{k \times k} \) denote the \( \ell \)-th block slid by one unit. \( R_{\ell}^* = U_k R_{\ell}^* U_k \) is the dual of \( R_{\ell} \in \mathbb{R}^{k \times k} \), where \( R_{\ell}^* \) is the inverse transpose of \( R_{\ell} \) and \( U_k \) is the reversed identity matrix with nonzero entries \( u_{i,k-i+1} = 1 \) for \( i = 1, \ldots, k \).

Let \( \text{max}_{\ell=1}^{n-1} R_{\ell+k-1,\ell+1} \) denote the maximum of \( \text{rank}_{\ell+k-1,\ell+1} \{ [r_{i,j}]_{\ell \leq i < j \leq \ell + k} \} := \text{GNF}(R_{\ell}^T T) \) over all \( T \in \text{GL}_k(\mathbb{Z}) \). Note that \( \text{max}_{\ell=1}^{n-1} R_{\ell+k-1,\ell+1} = 1/\lambda_1 \left( \text{det}(R_{\ell}^*) \right) \). Let \( \pi_\varepsilon : \mathbb{R}^n \to \text{span}(b_1, \ldots, b_{n-1})^\perp \) be the orthogonal projection, and \( b_\varepsilon^* := \pi_\varepsilon(b_1) \) thus \( \|b_\varepsilon^*\| = r_{1,1} \).

**LLL-bases.** \([\text{LLL82}]\) A basis \( B = QR \in \mathbb{R}^{m \times n} \) is LLL-basis for \( \delta \), \( \frac{1}{2} < \delta \leq 1 \), \( \alpha = 1/(\delta - 1/4) \) if

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

An LLL-basis \( B \) for \( \delta \) satisfies \( \|b_1^*\|^2 / \|b_\varepsilon^*\|^2 \leq \alpha \) for all \( \ell = 1, \ldots, n-1 \) and

\[
\|b_1\| \leq \alpha \frac{n}{\delta - 1}(\det L)^{1/n}, \quad \|b_1\| \leq c_1 \lambda_1.
\]

**Definition 1.** \([\text{GN08}]\) A basis \( B \in \mathbb{R}^{m \times n} \), \( n = \text{rk}(B) \) is slide-reduced for \( \varepsilon \geq 0 \) and \( k \geq 2 \) if

1. \( \|b_{\ell+1}^*\| = r_{\ell+1,\ell+1} = \lambda_1(L(R_{\ell+1})) \) for \( \ell = 0, \ldots, h-1 \),
2. \( \text{max}_{\ell=1}^{n-1} R_{\ell+k-1,\ell+1} \leq \sqrt{1+\varepsilon} : \|b_{\ell+1}^*\| \) holds for \( h = 1, \ldots, h-1 \).

1 slightly relaxes the condition of \([\text{GN08}]\) that all bases \( R_{\ell} \) are HKZ-reduced. The following bounds have been proved by Gama and Nguyen in \([\text{GN08}, \text{Theorem 1}]\) for slide-reduced bases:

3. \( \|b_1\| \leq ((1 + \varepsilon)\gamma_k)^{\frac{3}{2}} (\det L)^{1/n} \),
4. \( \|b_1\| \leq ((1 + \varepsilon)\gamma_k)^{\frac{3}{2}} \lambda_1 \).

Almost slide-reduced (asr-) bases. We call a basis \( B = QR \in \mathbb{R}^{m \times n} \), \( n = \text{rk}(B) \), an asr-basis for \( \varepsilon \geq 0 \) and blocksize \( k \) if clause 2 of Def. 1 holds for some \( \ell = \ell_{\text{max}} \) that maximizes \( D_{\ell}/D_{\ell+1} \) and clause 1 of Def. 1 holds for \( R_{\ell}, R_{\ell+1} \).

Theorem 2 shows that a slightly stronger inequality 3 holds for all asr-bases.

**Accelerated almost slide reduction (ASR)**

**Input** LLL-basis \( B = QR \in \mathbb{Z}^{m \times n} \), \( R = [r_{i,j}] \in \mathbb{R}^{n \times n}, n = \text{rk}(B), \) \( h > \varepsilon < 1, k \geq 2 \)

**Loop** Choose some \( \ell = \ell_{\text{max}} \) that maximizes \( D_{\ell}/D_{\ell+1} \). By SVP-computations on \( L(R_{\ell}), L(R_{\ell+1}) \) transform \( R_{\ell}, R_{\ell+1} \) and \( B \) such that 1 of Def. 1 holds for \( R_{\ell}, R_{\ell+1} \).

By an SVP-computation on \( R_{\ell}^* \) verify whether 2 holds for \( \ell \) and the input \( \varepsilon \).

**IF** 2 does not hold THEN transform \( R_{\ell}^* \) and \( B \) such that 2 holds for \( \varepsilon = 0 \)

**ELSE** transform \( R_{\ell} \) and \( B \) such that \( \|b_1\| = \lambda_1(L(R_{\ell})) \) and terminate. end loop

**Output** the resulting asr-basis \( B \).

We can replace the 3 SVP-computations per round on \( L(R_{\ell}), L(R_{\ell+1}), L(R_{\ell}^*) \) by the stronger and faster two SVP-computations on \( L(R_{\ell+k-1}), L(R_{\ell}^*) \), where \( R_{\ell+k-1} = [r_{i,j}]_{\ell \leq k-1, i \leq \ell+k} \in \mathbb{R}^{(k-1)\times(k+1)} \). Alternatively we can perform two SVP-computations on \( L(R_{\ell}^*), L(R_{\ell+1}^*) \) per round, where \( R_{\ell+1}^* := [r_{i,j}]_{\ell \leq k-1 < \ell+k} \in \mathbb{R}^{(k+1)\times(k+1)} \).

2
Theorem 1. ASR transforms a given LLL-basis \( B \in \mathbb{Z}^{m \times n} \) for \( \delta \leq 1 \), \( \alpha = 1/(\delta - 1/4), n = hk \), within \( \frac{1}{16} n^2 h \log_{1 \varepsilon} \alpha \) rounds (passes of the loop) of three local SVP-computations of dimension \( k \) either into an almost slide-reduced basis for \( \varepsilon \) and blocksize \( k \), or else arrives at \( \mathcal{D}(B) < 1 \), where

\[
\mathcal{D}(B) := \inf \prod_{t=1}^{k} (D_t/(D_t+\ell))^{h_t-\ell_t} = D_1^{h_1-\ell_1} D_2^{h_2-\ell_2} \cdots D_k^{h_k-\ell_k}. 
\]

Proof. We use the novel version \( \mathcal{D}(B) \) of the Lovász invariant to measure \( B \)'s reducedness. Note that \( h^2/4 - (\ell - h/2)^2 = h\ell - \ell^2 \) is symmetric to \( h = \ell \) with maximal point \( \ell = 1 \) if \( h = 1/2 \). The input LLL-basis \( B^{(l)} \) for \( \delta \leq 1 \) satisfies for \( \alpha = 1/(\delta - 1/4) \) that \( D_1/(D_t+\ell) \leq \alpha^\ell \) and thus

\[
\mathcal{D}(B^{(l)}) \leq \alpha^{k^2} \quad \text{for} \quad s := \sum_{t=1}^{k} h_t - \ell_t = \frac{h^2-h}{6}. 
\]

Fact. Every non-terminal round with \( \ell \) decreases \( D_t \) and \( D(B) \) as

\[
D_t^{(new)} \leq D_t/(1 + \varepsilon) \quad \text{and} \quad D(B^{(new)}) \leq D(B)/(1 + \varepsilon)^2. 
\]

This is because the round changes merely the factor

\[
\left( \prod_{t=1}^{k} (D_t/D_{t+1})^{(h_t-\ell_t)} \right) = (D_t/D_{t+1})^{h_t-2\ell_t} D_{t+1}^2, 
\]

of \( D(B) \), where \( D_t D_{t+1} \) does not change. Hence, after at most

\[
\frac{1}{2} \log_{1 \varepsilon} D(B^{(l)}) \leq \frac{1}{2} \log_{1 \varepsilon} (\alpha^{k^2}) = \frac{1}{2} \frac{h^2-h}{6} \log_{1 \varepsilon} \alpha < \frac{n^2 h}{\log(m)} \log_{1 \varepsilon} \alpha \]

rounds either \( B \) is asr-basis for \( \varepsilon \) or else \( \mathcal{D}(B) < 1 \). Our bound on the number of rounds does not count the terminal round which does not decrease \( D \). \( \square \)

Remarks. 1. We conjecture that the time bound of Theorem 1 even holds if on termination \( \mathcal{D}(B) < 1 \). This might be provable by the dynamical system method of [HPS11]. Anyway, \( \mathcal{D}(B) < 1 \) is very unlikely. If \( \mathcal{D}(B) < 1 \) then \( E[\ln(D_t/D_{t+1})] < 0 \) holds for the expectation \( E \) for random \( \ell \) with \( \Pr(\ell) = \frac{\ell / k}{k+1} \). Note that \( \sum_{t=1}^{k} \Pr(\ell) = 1 \). In this sense \( D_t \leq D_{t+1} \) would hold "on average" if \( \mathcal{D}(B) < 1 \), whereas such \( D_t, D_{t+1} \) are extremely unlikely.

2. On the other hand, if the output basis of ASR satisfies on average that \( ||b_{l}||^2/||b_{l+1}||^2 \geq \alpha^{1/l} \) then the number of rounds decreases to at most \((1 - 1/l)^{n^2 h \log_{1 \varepsilon} \alpha} \).

Theorem 2. Every asr-basis \( B \in \mathbb{Z}^{m \times n} \) for \( \varepsilon, k \) satisfies \( ||b_{l}|| \leq ((1+\varepsilon)^{1/k} \gamma_k)^{\frac{n-1}{2}} \) for \( l = \ell_{\text{max}} \).

Proof. We see from clause 2 of Def. 1 and the Hermite bound on \( \lambda_1(\mathcal{L}(R^*)^n) \leq 1/r_{k\ell+1,k\ell+1} \) that

\[
D_t/\gamma_{k\ell+1,k\ell+1} \leq ((1 + \varepsilon)^{1/k} \gamma_k)^{k} r_{k\ell+1,k\ell+1}^{2k-2} 
\]

holds for \( l = \ell_{\text{max}} \), where \( D_t := (\gamma_k R_t)^2 \). Moreover, the Hermite bound for \( R_t \) shows that

\[
r_{k\ell-k+1,k\ell-k+1} \leq \gamma_k D_t/\gamma_{k\ell-k+1,k\ell-k+1} \]

Combining these two inequalities with \( D_t/\gamma_{k\ell-k+1,k\ell-k+1} = D_t/\gamma_{k\ell-k+1,k\ell-k+1} \) yields for \( l = \ell_{\text{max}} \):

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

Next we prove

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

for \( l = 1, \ldots, h - 1 \).

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

\[
D_t \leq (1 + \varepsilon)^{k} \gamma_k r_{k\ell+1,k\ell+1} \leq (1 + \varepsilon)^{k} \gamma_k D_t+1 \]

hence (2) yields for \( l = \ell_{\text{max}} \)

\[
D_t = r_{k\ell-k+1,k\ell-k+1} D_t/\gamma_{k\ell-k+1,k\ell+1} \leq ((1 + \varepsilon)^{1+1/k} \gamma_k)^{\frac{2k-2}{k}} D_t. 
\]

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

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

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

3. 1 of Def.1 for \( R_t \) and (3) imply for \( l = 1, \ldots, h \) that

\[
||b_{l}||^2 \leq \gamma_{k} D_t^{1/k} \leq \gamma_{k} (1 + \varepsilon)^{1+1/k} \gamma_k D_t^{1/k}. 
\]
The product of these $h$ inequalities for $\ell = 1, \ldots, h$ yields
\[
\|b_1\|^2 \leq \gamma_k \left((1 + \varepsilon)\frac{1+1/k}{\gamma_k}\right)^{\frac{1}{k} \sum_{i=1}^{h} \left(\log\left(\frac{k+1}{k-1}\right)\right)} (\det L)^{2/k}.
\]
Hence the claim
\[
\|b_1\|^2/(\det L)^{2/n} \leq \gamma_k \left((1 + \varepsilon)\frac{1+1/k}{\gamma_k}\right)^{\frac{1}{k} \sum_{i=1}^{h} \left(\log\left(\frac{k+1}{k-1}\right)\right)} \left(1 + \varepsilon\right)^{\frac{1+1/k}{\gamma_k}} \gamma_k^{\frac{n}{k}}.
\]
\[\qed\]

**Strong asr-bases.** We call an asr-basis $B \in \mathbb{R}^{m \times hk}$ strong if $2$ of Def. 1 holds for $\ell = h - 1$ and $1$ of Def. 1 holds for $R_{h-1}$ and $R_h$.

Most likely, we obtain a strong asr-basis from any asr-basis by $O(k \ln k/\varepsilon)$ ASR-rounds with $\ell = h - 1$ and $\ell = \ell_{\max}$ that can possibly change $B$. This takes at most $\frac{k}{2 \varepsilon^2} (1 + \log_2 \gamma_k)$ ASR-rounds with $\ell = h - 1$ because $D_{h-1}/D_h \leq \left((1 + \varepsilon)\gamma_k\right)^{\frac{2k^2}{k-1}}$ holds for any asr-basis and each round with $\ell = h - 1$ decreases $D_{h-1}/D_h$ by a factor $(1 + \varepsilon)^{-2}$. Similarly, we can transform an asr-basis $B$ into a slide-reduced basis by iterating ASR-rounds that can possibly change $B$. Most likely this takes only $O(n \ln k/\varepsilon)$ ASR-rounds, much fewer than to transform an LLL-basis into an asr-basis.

**Theorem 3.** Every strong asr-basis $B = [b_1, \ldots, b_n]$ for $\varepsilon \geq 0, k \geq 2, n = \frac{h}{k}$ satisfies
\[
\|b_1\| \leq (1 + \varepsilon)^{\frac{1+1/k}{\gamma_k}} \gamma_k \leq 2^{h/2} A_1
\]
provided that some $b \in \mathcal{L}(B) \setminus \mathcal{L}(b_1, \ldots, b_{n-k})$ satisfies $\|b\| = \lambda_1$.

**Proof.** (5) for $\ell = h - 1$ shows that
\[
\|b_1\|^2 \leq \gamma_k \left((1 + \varepsilon)\frac{1+1/k}{\gamma_k}\right)^{\frac{2k^2}{k-1}} \gamma_k^{\frac{n}{k}}.
\]
Clearly $2$ for $\ell = h - 1$ implies (2) and (4) for $\ell = h - 1$, and thus we get
\[
\|b_1\|^2 \leq \gamma_k \left((1 + \varepsilon)\frac{1+1/k}{\gamma_k}\right)^{\frac{2k^2}{k-1}} \gamma_k^{\frac{n}{k}} (\det L_{h-1}^{1/k})
\]
(by 4) for $\ell = h - 1$ and the Hermite bound for $R_{h-1}^*$, we have $D_{h-1}^{1/k} \leq \gamma_k r_{n-k+1,n-k+1}^2$ (since $1 + \frac{k}{k-1} < \frac{1}{k}$ for $k \geq 2$)
\[
\|b_1\|^2 \leq \gamma_k \left((1 + \varepsilon)\frac{1+1/k}{\gamma_k}\right)^{\frac{2k^2}{k-1}} \gamma_k^{\frac{n}{k}} \left(r_{n-k+1,n-k+1}^2 - \gamma_k r_{n-k+1,n-k+1}^2\right).
\]
The theorem assumes that $\|b\| = \lambda_1$ holds for some $b \in \mathcal{L}(b_1, \ldots, b_{n-k})$. Hence $r_{n-k+1,n-k+1} \leq \|\pi_{n-k+1}(b)\| \leq \lambda_1$. The latter inequalities yield the claim.
We have decreased the exponent 1 of $(1 + \varepsilon)$ in 3 and 4 to $\frac{1+1/k}{\gamma_k} \approx 1/2$ for large $k$.

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

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

The final ASR-call with blocksize $k = 2^j$ dominates the overall workload of all ASR-calls of the iteration, including the workload for the LLL-reduction of the input basis, due to the dominating workload of local SVP-computations in dimension $k$.

We bound the number $\#It$ of rounds of the last ASR-call with blocksize $k = 2^j$. Importantly, the input $B$ of this final ASR-call satisfies $D_i/D_{i+1} \leq \left((1 + \varepsilon)\gamma_k/2\right)^{\frac{2k^2}{k-1}}$, as follows from (3) with blocksize $k/2$ and $\frac{1+1/k}{\gamma_k} \leq 1$ for $k \geq 2$. In fact we have that $D_i/D_{i+1} \leq \max(D_{i,k/2}/D_{i+1,k/2})^4$, where $D_{i,k/2} = (\det R_{i,k/2})^2$ for the $i$-th block $R_{i,k/2}$ of blocksize $k/2$ of the input basis $B$. Hence
\[
D(B) \leq \left((1 + \varepsilon)\gamma_k/2\right)^{2k^2/2-1} \gamma_k^{\frac{n}{k}}
\]
holds for the input $B$. As each round prior to termination decreases $D(B)$ by a factor $(1 + \varepsilon)^{-2}$ the number $\#It$ of rounds of the last ASR-call is bounded as
\[
\#It \leq \frac{1}{2} \log_{\log_{2} \gamma_k} D(B) \leq \frac{\log_{\log_{2} \gamma_k} D(B)}{\log_{1+\varepsilon} ((1 + \varepsilon)\gamma_k/2)} \leq \frac{1}{2} \log_{\log_{2} \gamma_k} \log_{1+\varepsilon} ((1 + \varepsilon)\gamma_k/2),
\]
provided that $D(B) \geq 1$ holds on termination. This proves
Corollary 1. Given an almost slide-reduced-basis $B \in \mathbb{Z}^{m \times n}$ for $\varepsilon > 0$ and blocksize $k/2$, $n = hk$, ASR finds within $\frac{1}{2} \frac{n^2}{1 - 2\varepsilon^2} \log_{1+\varepsilon}((1+\varepsilon)\gamma_{k/2})$ rounds of three local SVP-computations an asr-basis of blocksize $k$ and $\varepsilon$ unless it terminates with $D(B) < 1$.

This shows that the upper bound on the number of rounds of ASR with blocksize $k$ and $\varepsilon$ of Theorem 1 decreases for $\varepsilon \leq 0.01$ and $\alpha \approx 4/3$ by a factor

$$4/(1 - 2/k) \ln \alpha / \ln((1 + \varepsilon)\gamma_{k/2}) \approx 4(k - 2)^{-1} \ln \gamma_{k/2} / \ln(4/3)$$

if the input basis $B$ is an asr-basis with blocksize $k/2$. For $k = 32$ this is less than half the bound from Theorem 1, where the input is an LLL-basis for $\delta, \alpha$. Here we assume that $\gamma_{16} \approx 2\sqrt{2}$. Moreover, within only half of these rounds ASR achieves $D(B) \leq ((1 + \varepsilon)\gamma_k)^{\frac{2\varepsilon^2}{1 - 2\varepsilon^2}} / \varepsilon$, a bound on the final $B$ that follows from (3). Interestingly, this bound on $D(B)$ is sharp on the average.

Fast slide-reduction for extremely small $\varepsilon$. Instead of running ASR with a very small $\varepsilon$ and some $k$ on an input LLL-basis it is faster to first run ASR for some $\varepsilon' > \varepsilon$ and $k' > k$ such that

$$(1 + \varepsilon)\gamma_{k'}^{k' - 1} > ((1 + \varepsilon')\gamma_{k'}^{k' - 1}.$$ (6)

Then perform on this asr-basis ASR-rounds for $\varepsilon, k$ for such $\ell$ that the ASR-round can possibly change $B$, and terminate when $B$ can no more change. (6) implies that the upper bound 3 on $\|b_i\|/(\det L)^{1/n}$ is smaller for an asr-basis with $\varepsilon', k'$ than for an asr-basis with $\varepsilon, k$. This suggests that there are most likely only a few ASR-rounds for $\varepsilon, k$.

Lemma 1. Any asr-basis $B = [b_1, \ldots, b_n] \in \mathbb{Z}^{m \times n}$ for $\varepsilon < 1/M_0^{2n}$, $M_0 := \max(\|b_1\|^2, \ldots, \|b_n\|^2)$, is asr-basis for $\varepsilon = 0$.

Proof. Let $\varepsilon > 0$ be minimal such that $B$ is asr-basis for $\varepsilon, k$. We see from the proof of (3) that the inequality 2 of Def. 1 holds with equality for some $\ell = \ell_{\max}$. Consider an artificial ASR-round performed on $B$ with $\ell = \ell_{\max}$ resulting in $r_{k\ell+1,k\ell+1}^\text{new} = \max(r_{i\ell,\ell}^\text{old})$. Let $D_{\ell} := (\det[b_1, \ldots, b_{k\ell}])^2 \in \mathbb{Z}$ denote the value before and $D_{\ell}^\text{new}$ after this round. Then $D_{\ell}^\text{new} < D_{\ell}$ because $\det R_{\ell}$ decreases in that round. Importantly, the values $(r_{k\ell+1,k\ell+1}^\text{new})^2 D_{\ell}, (r_{k\ell+1,k\ell+1}^\text{new})^2 D_{\ell}^\text{new}$ before and after this round are integers – this claim is analogous to [LLL82, (1.28)]. As 2 of Def. 1 holds with equality we have $(r_{k\ell+1,k\ell+1}^\text{new})^2 = (1 + \varepsilon) (r_{k\ell+1,k\ell+1})^2$ and thus $\varepsilon, (r_{k\ell+1,k\ell+1})^2, (r_{k\ell+1,k\ell+1}^\text{new})^2 \in \mathbb{Z}/(D_{\ell} D_{\ell}^\text{new})$.

Hence $\varepsilon \geq 1/(\sqrt{\text{det} D_{\ell}^\text{new}}) \geq 1/M_0^{n-2k}$ since $D_{\ell}^\text{new} < D_{\ell} \leq M_0^{k}\leq M_0^{n-k}$. Therefore, the minimality of $\varepsilon$ implies that either $\varepsilon = 0$ or $\varepsilon > 1/M_0^{2n}$. This proves the claim.

Improving worst case slide-reduced bases. We characterize slide-reduced bases for $k$ and $\varepsilon = 0$ for which $\|b_i\|/\lambda_1$ is maximal. A shortest lattice vector can easily be found for such a basis.

Theorem 4. Let the basis $R = \text{GNF}(R) = [b_1, \ldots, b_n] \in \mathbb{R}^{n \times n}$, $n =hk$ be slide-reduced for $k$ and $\varepsilon = 0$. If $\|b_i\|/\lambda_1 = \gamma_k^\frac{1}{k}$ then there exists $b_{\min} \in 0^{n-k}\mathbb{R}^k \cap L(R)$ with $\|b_{\min}\| = \lambda_1$. Any such $b_{\min}$ can be found from its projection $\pi_{n-k+1}(b_{\min})$ in $O(n^2)$ arithmetic steps.

Proof. Let $R = [r_{i,j}] \in \mathbb{R}^{n \times n}$ then $\pi_{n-k+1}(R) = L([r_{i,j}]_{n-k<i,j\leq n})$ is a lattice of dimension $k$. By (2) the slide-reduced $R$ satisfies

$$\pi_{k\ell+1,k\ell+1} \leq \gamma_k^{\frac{1}{k}} \pi_{k\ell+1,k\ell+1}$$

for $\ell = 1, \ldots, h - 1$.

Therefore $\|b_i\|/\lambda_1 = \gamma_k^{\frac{1}{k}}$ implies $\|b_{\min}\| = r_{n-k+1,n-k+1}$. Hence $\pi_{n-k+1}(b_{\min})$ is a shortest nonzero vector of $\pi_{n-k+1}(L(R))$ of length $r_{n-k+1,n-k+1}$. Therefore $b_{\min} \in 0^{n-k}\mathbb{R}^k \cap L(R)$. Let $b_{\min} = \sum t_i b_i$. Then, given $\sum t_{n-k+1} t_i$ we find $t_{n-k}, \ldots, t_1 \in \mathbb{Z}$ from the equations

$$t_j r_{j,j} + \cdots + t_{n-k} r_{j,n-k} + \sum_i = m = k + 1^n t_i r_{j,i} = 0$$

for $j = n - k, \ldots, 1$. This proves the Theorem. \(\square\)
Note that we find all \( b_{\text{min}} \in \mathbb{Z}^{n-k} \cap \mathcal{L}(R) \) by enumerating the shortest vectors of \( \pi_{n-k+1} \mathcal{L}(R) \) and trying to extend them to some \( b_{\text{min}} \in \mathbb{Z}^{n-k} \cap \mathcal{L}(R) \). In particular, if the shortest vector \( \pm b \) of \( \pi_{n-k+1} \mathcal{L}(R) \) is unique, which is most likely the case, then we find \( b_{\text{min}} \in \mathbb{Z}^{n-k} \cap \mathcal{L}(R) \) by an SVP-computation of dimension \( k \) in \( O(n^2) \) arithmetic steps that compute \( t+1, \ldots, y_{n-k} \in \mathbb{Z} \).

**Conclusion.** Given a slide-reduced basis \( R \in \mathbb{R}^{n \times n} \) with blocksize \( k \) and \( \varepsilon = 0 \) for which \( \|b_i\|/\lambda_1 \) is maximal we can easily find a shortest vector of \( \mathcal{L} \ast R \). More generally, this suggests that the closer \( \|b_i\|/\lambda_1 \) is to the maximum of slide-reduced bases of dimension \( n \) and blocksize \( k \) the easier it is to find a nonzero lattice vector \( b \) that is substantially shorter than \( b_1 \).

Such short \( b \) can be found by random sampling reduction [S03]. This method transforms a given basis \( R = \text{GNF}(R) = [r_{i,j}] = [b_1, \ldots, b_n] \in \mathbb{R}^{n \times n} \) by checking for sufficiently many integer combinations \( b = \sum_{i=1}^n t_i b_i \), whether size-reduction of \( b \) versus \( b_1, \ldots, b_{n-u-1} \) yields a vector \( b \) that is shorter than \( b_1 \). By Theorem 1 of [S03] this method finds under reasonable assumptions a basis such that \( \|b_1\|/\lambda_1 \leq (k/6)^{2\delta} \) within time \( O(n^2(k/6)^{k/4}) \). Random sampling reduction of [S03] improves slide-reduction in that it largely improves slide-reduced bases for which \( \|b_1\|/\lambda_1 \) is maximal. It makes sense to alternate the two reduction methods iteratively as the two methods rely on independent principles.

**Improving worst case LLL-bases.** We translate Theorem 4 to LLL-bases with \( \delta = 1 \). These bases are slide-reduced for \( k = 2 \) and \( \varepsilon = 0 \) and thus \( \|b_1\|^2 \leq (\frac{1}{\delta})^{n-2} \lambda_1^2 \) holds by Theorem 3 since \( \gamma_2 = \frac{1}{4} \). If \( \|b_1\|^2 = (\frac{1}{\delta})^{n-2} \lambda_1^2 \) then by Theorem 4 a shortest lattice vector can be found by size-reducing a combination of the last two basis vectors:

**Theorem 5.** Let \( R = \text{GNF}(R) \in \mathbb{R}^{n \times n} \) be an LLL-basis for \( \delta = 1 \). If \( \|b_1\|^2 = (\frac{1}{\delta})^{n-2} \lambda_1^2 \), i.e., \( \|b_1\|/\lambda_1 \) is maximal, then there exists \( b_{\text{min}} \in (0, \ldots, 0, \pm r_{n-1, n-1}, r_{n,n})^t \in \mathcal{L}(R) \) of length \( \|b_{\text{min}}\| = \lambda_1 \) and such \( b_{\text{min}} \) can be found in \( O(n^2) \) arithmetic steps.

**Accelerating LLL-reduction (ALR).** We accelerate LLL-reduction by performing either local Gauss-reductions, i.e., LLL-reductions with \( \delta = 1 \), or LLL-swaps on \( b_i, b_{i+1} \) for an \( \ell \) that maximizes \( \|b_\ell\|/\|\pi_\ell(b_{\ell+1})\| \) and thus promises maximal reduction progress.

We value the reduction of the basis \( B \) satisfying \( \max_{\ell} \|b_\ell^*\|^2/\|b_{\ell+1}^*\|^2 > \frac{1}{4} \) the integer \( \mu \) defined by

\[
2^{\mu-1} < \max_{\ell} \|b_\ell^*\|^2/\|b_{\ell+1}^*\|^2 < 2^\mu.
\]

(7)

ALR iterates the following loop:

```plaintext
WHILE the loop changes B DO
  IF \( \mu \geq 0 \) THEN
    for an \( \ell \) that maximizes \( \|b_\ell^*\|/\|b_{\ell+1}^*\| \) LLL-reduce \( \pi_\ell(b_\ell), \pi_\ell(b_{\ell+1}) \) with \( \delta = 1 \). (this is a Gauß-reduction of \( \pi_\ell(b_\ell), \pi_\ell(b_{\ell+1}) \))
  ELSE
    choose an \( \ell \) that after the size-reduction \( b_{\ell+1} := b_{\ell+1} - \frac{r_{\ell,\ell+1}}{r_{\ell,\ell}} b_{\ell} \)
    maximizes \( \|b_\ell^*\|^2/\|\pi_\ell(b_{\ell+1})\|^2 \). If \( \|\pi_\ell(b_{\ell+1})\|^2 \leq \delta \|b_\ell^*\|^2 \) swap \( b_\ell, b_{\ell+1} \),
    and size-reduce \( b_\ell, b_{\ell+1} \) against \( b_1, \ldots, b_{\ell-1} \).
  end while
termination size-reduce the basis \( B \) to satisfy \( r_{i,j} \leq \frac{1}{4} r_{i,i} \) for all \( j > i \).
```

**Theorem 6.** Given an LLL-basis \( B \in \mathbb{Z}^{m \times n} \) for \( \delta' < 1 \), \( \alpha' = 1/(\delta' - 1/4) \) ALR with \( \delta \) such that \( 1 > \delta > \max(\delta', \frac{1}{4}) \) terminates within \( \frac{n^2}{\delta^2} \log_{1/\delta} \alpha' \) rounds of local Gauss-reductions, resp. LLL-swaps at an LLL-basis for \( \delta \), unless it arrives at \( D(B) := \prod_{k=1}^{n-1} (\|b_k^*\|^2/\|b_{k+1}^*\|^2)^{n-k} t^2 < 1 \).

Theorem 6 proves that the number of rounds of ALR is \( O(n^3) \) for input LLL-bases of arbitrary quality \( \delta, \alpha \), a bound that is independent of size(\( B \)), whereas the number of rounds for the original LLL-algorithm [LLL82] is merely polynomial in \( \text{size}(B) \).
Proof. We use \( D(B) \) for blocksize 1, \( D(B) := \prod_{\ell=1}^{n-1} (\|b^\ell\|^2/\|b^\ell_{n+1}\|^2)^{(n-\ell)/\ell} \). Each round decreases \( \|b^\ell\|^2 \) by a factor \( \delta \), and both \( \|b^\ell\|^2/\|b^\ell_{n+1}\|^2 \), \( D(B) \) by a factor \( \delta^2 \). Then the number of rounds until either an LLL-basis for \( \delta \) appears or else \( D(B) \leq 1 \) is at most
\[
\frac{1}{2} \log_{1/\delta} D(B) \leq \frac{1}{2} \log_{1/\delta} (\alpha')^{3/2 - n/\ell} \leq \frac{3}{2\ell} \log_{1/\delta} \alpha'.
\]

The workload per round. When each round completely size-reduces \( b^\ell, b^\ell_{n+1} \) against \( b_1, \ldots, b_{n-1} \) it requires \( O(n^2) \) arithmetic steps. If we only size-reduce \( b^\ell_{n+1} \) against \( b^\ell \) then a round costs merely \( O(n) \) arithmetic steps but the length of the integers might explode. This explosion can be prevented at low costs by doing size reduction in segments, see [S06], [KS01]. Note that the bit complexity of the round can be made quasi-linear in size \( B \) by the method of [NSV10]: perform the arithmetic steps of the round on the leading bits of the entries of the basis matrix using fast integer arithmetic.

Corollary 2. The \( \mu \)-value (7) of the input basis satisfies \( \mu \leq \log_2 n + \log_2 \log_2 M_0 \), let \( c \in \mathbb{Z}, c \geq 0 \) be constant. Within \( 2^{\alpha n} (\mu + 2^c) \) rounds \( \text{ALR} \) either decreases the initial \( \mu \) to \( \mu \leq c \) or else arrives at \( D(B) < 1 \). This number of rounds is polynomial in \( n \) if \( \log_2 \log_2 M_0 \leq n^{O(1)} \).

Proof. As initially \( \frac{1}{2} 2^{2n-1} \leq \max_i \|b^\ell_i\|^2/\|b^\ell_{n+1}\|^2 \leq \frac{1}{2} 2^{2n} \). Each round of \( \text{ALR} \) with \( \ell = \ell_{\max} \) decreases \( \|b^\ell\|^2/\|b^\ell_{n+1}\|^2 \) by a factor \( 2^{-2^{c-1}} \), where \( \mu \) is the initial value of the round. Following the fact in the proof of Theorem 1 this decreases \( D(B) =_{\delta_{\ell_{\max}}} \prod_{\ell=1}^{\ell_{\max}-1} (\|b^\ell_{n+1}\|^2/\|b^\ell_{n+1}\|^2)^{(n-\ell)c} \) for \( k = 1 \) as \( D(B^{\text{new}})/D(B^{\text{old}}) \leq 2^{-2^{c-1}} \). This bounds the number \( \#I_{\ell_{\max}} \) of \( \text{ALR} \) rounds for the reduction of \( \mu \) to \( \mu \leq c \) to
\[
\#I_{\ell_{\max}} \leq \frac{\alpha n}{2 \ell} \left( 2^n + \log_2 \frac{1}{\delta} \right)^{2^{c-1}}
\]
unless \( \text{ALR} \) arrives at \( D(B) < 1 \). Similarly \( \text{ALR} \) decreases the \( \mu \) of the input-basis within at most
\[
\frac{a^2}{4} (2^\mu + \log_2 \frac{1}{\delta} \sum_{i=0}^{\ell} \|b^\ell_i\|^2/\|b^\ell_{n+1}\|^2)^{2^{c-1}} < \frac{a^2}{4} (\mu + 2^c + 1)^{2^{c+1}} \log_2 \frac{1}{\delta} < \frac{a^2}{4} (\mu + 2^c)
\]
rounds to \( -|c| \) unless it arrives at \( D(B) < 1 \).

The bound \( \mu \leq \log_2 n + \log_2 \log_2 M_0 \) follows from (7) and \( \|b^\ell_{n+1}\|^2 \geq 1/M_0^{2n} \).

LLL-reduction for extremely small \( 1 - \delta \). It follows from Cor. 2 that LLL-reduction with \( \delta = 1 \) is in polynomial time \( n^{O(1)} \) if \( \log_2 \text{size}(B) = n^{O(1)} \). For this first compute an LLL-basis for \( \delta = 3/4 \), transform it into a strong asr-basis for \( k = 3 \) and \( \varepsilon = 0.07 \). As \( \gamma_2^2 > 1.07 \gamma_3 \) the proven bound for \( \|b_i\|/|\det L|^{1/n} \) is smaller for this asr-basis then for an LLL-basis with \( \delta = 1 \). Transform the asr-basis by iterating \( \text{ALR} \)-rounds with \( \varepsilon = 0 \) that can possibly change \( B \). The work load of the latter \( \text{LLR} \)-rounds should be negligible compared to the previous reductions.

Next we study LLL-reduction for extremely small \( 1 - \delta \) by block reduction of dimension 2.

Lemma 2. Every LLL-basis \( B = (b_1, \ldots, b_n) \) for \( \delta > 1 - 1/M_0^{2n} \), \( M_0 := \max(\|b_1\|^2, \ldots, \|b_n\|^2) \), is LLL-basis for \( \delta = 1 \) and thus max_{\ell} \( \|b^\ell\|^2/\|b^\ell_{n+1}\|^2 \leq 1/4 \).

Proof. Follow the proof of Lemma 1 for \( \varepsilon = 1 - \delta \). Let \( \delta \) be maximal such that \( B \) is LLL-basis for \( \delta \). Consider the effect of an artificial \( \text{ALR} \)-round with \( \ell = \ell_{\max} \) that maximizes \( r_{\ell,\ell}^2/r_{\ell+1,\ell+1}^2 \) performed on the LLL-basis \( B \) for \( \delta < 1 \) and resulting in \( r_{\ell,\ell}^2 = \delta r_{\ell,\ell}^2 \). This holds as \( \delta \) is maximal such that \( B \) is LLL-basis for \( \delta \). Then
\[
D^e_{\ell+1} = (r_{\ell,\ell}^2 \|b_{\ell+1}\|^2/\|b_{\ell+1}\|^2)^{2^{c-1}} \in \mathbb{Z},
\]
\[
1 - \delta \geq 1/(D_{\ell+1} D_{\ell+1}^e) > 1/M_0^{2n-2},
\]
and thus \( 1 - \delta < 1/M_0^{2n} \) implies \( \delta = 1 \).

Comparison with previous algorithms for LLL-reduction. The original LLL for \( \delta = \frac{1}{4} \) ([L78],[L82]) has bit-complexity \( O(n^{3/2+\varepsilon}(\log_2 M_0)^2) \) performing \( O(n^2 \log_2 M_0) \) 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 \( n \log_2 M_0 \) bit-length of integers has been reduced to \( n + \log_2 M_0 \) by orthogonalizing the basis in floating point arithmetic. The LLL-time can be reduced by 10 - 15 % by successively increasing \( \delta \) from 3/4, 7/8, 15/16, 31/32, 63/64 to 0.99.

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 \( \pi_e(b_k), \pi_e(b_{k+1}) \) is quasi-linear in the bit-length of
Therefore we do not split up this LLL-reduction into LLL-swaps. Gauss-reduction of \( \pi(\mathbf{b}_t) \) for \( \ell = \ell_{\text{max}} \) decreases \( \mathcal{D}(B) \) by the factor \( 2^{-2^\mu - 1} \) while LLL-swaps guarantee only a decrease by the factor \( \frac{1}{4} \).

A result that is very close to Cor. 2 and Cor. 3 has been proved independently in Lemma 12 of [HPS11]:\footnote{Early Termination (ET). Terminate as soon as \( \varepsilon > 0 \) by block reduction of dimension 2.} \( \max_{1 \leq i \leq n} \| \mathbf{b}_t^i \|^2/\| \mathbf{b}_{t+1}^i \|^2 \leq \frac{1}{4} + \varepsilon \) can be achieved in polynomial time \( n^{\mathcal{O}(1)} \text{size}(B)^{1+o(1)} \) for arbitrary \( \varepsilon > 0 \) by block reduction of dimension 2.

\[ \mathcal{D}(B) < \frac{1}{4} \left( \frac{\ln n}{\ln 2} \right)^2 \]

implies that \( \mathcal{E}(\| \mathbf{b}_t^i \|^2/\| \mathbf{b}_{t+1}^i \|^2) < \ln(4/3) \) holds for random \( \ell \) and \( \mathbb{P}(\ell = 1) = \frac{6}{n^{\ln n^2}} \). In this sense the output basis approximates "on the average" the logarithm of the inequality \( \| \mathbf{b}_1 \|/\| \det L \|^{1/n} \leq \left( \frac{4}{3} \right)^{\frac{n-1}{2}} \) that holds for ideal LLL-bases with \( \delta = 1 \).

**Corollary 3.** ALR terminates under ET in \( n^3 (\mu + |\mu_0|)/3 \) rounds, where \( \mu, \mu_0 \) are the \( \mu \)-values of the input and output basis. Moreover \( |\mu_0| \leq n \log_2 M_0 \) and \( \mu \leq \log_2 n + \log_2 \log_2 M_0 \).

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

\[ \| \mathbf{b}_t^{n+1} \|^2 < \| \mathbf{b}_t^{n} \|^{2-2^{\mu-2}} \text{ hence } \mathcal{D}(B^{n+1}) < \mathcal{D}(B^{n})^{2-2^\mu-1}. \]

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

\[ \# I_\mu < \log_2 (\mathcal{D}(B^{n+1})/(\mathcal{D}(B^{n})))^{1/2^\mu} \leq (2^{\mu} n^{6} - n)/2^{\mu-1} = \frac{n^{3} - n}{2^\mu}. \]

Hence \( \mu \) decreases to \( \mu - 1 \) under ET in less than \( \frac{n^{3} - n}{2^\mu} \) rounds. The proof of Lemma 1 shows that \( |\mu_0| \leq n \log_2 M_0 \).

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

**References**


