Progress on LLL and Lattice Reduction

Claus P. SCHNORR

Fachbereich Informatik und Mathematik
Johann Wolfgang Goethe-Universität
Frankfurt am Main

LLL+25

Caen, Normandy, France

June 29, 2007

http://www.mi.informatik.uni-frankfurt.de/research/papers.html

Surview

Covered in the talk

1. Extending the LLL to quadratic forms, to indefinite forms, to forms with polynomial entries.
2. Better approximation for the SVP, Decreasing $\|\mathbf{b}_1\|^2/\lambda_1^2 \leq \alpha^{n-1} \leq 2^{n-1}$ in polynomial time.
3. Semi-block reduction [S87],
4. Primal-dual reduction, deep insertion, random sampling reduction.

full paper:
LLL via Householder orthogonalisation,
LLL-type segment reduction.

Lattices, QR-decomposition, LLL-bases

lattice basis	$B = [\mathbf{b}_1, \ldots, \mathbf{b}_n] \in \mathbb{Z}^{m \times n}$
lattice	$\mathcal{L}(B) = \{Bx \mid x \in \mathbb{Z}^n\}$
norm	$\|\mathbf{x}\| = \langle \mathbf{x}, \mathbf{x} \rangle = (\sum_{i=1}^{m} x_1^1)^{1/2}$
SV-length	$\lambda_1(\mathcal{L}) = \min\{\|\mathbf{b}\| \mid \mathbf{b} \in \mathcal{L} \backslash \{0\}\}$
Successive minima	$\lambda_1, ..., \lambda_n$

QR-**decomposition** $B = QR \subset \mathbb{R}^{m \times n}$ such that

- the **GNF** — geom. normal form — $R = [r_{i,j}] \in \mathbb{R}^{n \times n}$ is uppertriangular, $r_{i,j} = 0$ for $j < i$ and $r_{i,i} > 0$,
- $Q \in \mathbb{R}^{m \times n}$ **isometric**: $\langle Qx, Qy \rangle = \langle x, y \rangle$.

LLL-basis $B = QR$ for $\delta \in (\frac{1}{4}, 1]$(Lenstra, Lenstra, Lovasz 82):

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

Quality of LLL-bases

Let $\delta \in (\frac{1}{4}, 1]$ be constant and $\alpha = 1/(\delta - \frac{1}{4}) \approx \frac{4}{3}$.

$\delta \approx 1$, yields $\alpha = 1/(\delta - \frac{1}{4}) \approx \frac{4}{3}$. [LLL82] focus on $\delta = \frac{1}{2}$, $\alpha = 2$

$$\det \mathcal{L} = \det(B^t B)^{1/2}$$

Theorem [LLL82]

1. $\|\mathbf{b}_1\|^2 \leq \alpha^{\frac{n-1}{2}} (\det \mathcal{L})^{2/n}$ 2. $\|\mathbf{b}_1\|^2 \leq \alpha^{n-1} \lambda_1^2$,
3. $\|\mathbf{b}_i\|^2 \leq \alpha^{i-1} r_{i,i}^2$,
4. $\alpha^{-i+1} \leq \|\mathbf{b}_i\|^2 \lambda_i^{-2} \leq \alpha^{n-1}$ for $i = 1, ..., n$.

The LLL-algorithm transforms a given basis B into an LLL-basis BT with $T \in \mathrm{GL}_n(\mathbb{Z})$.

The LLL-algorithm is polynomial time using $O(n^3 m \log_{1/\delta} \|B\|)$ arithmetic steps on integers of bit length $O(n \log \|B\|)$, where $\|B\| = \max_i \|\mathbf{b}_i\|^2$ for $B = [\mathbf{b}_1, ..., \mathbf{b}_n]$.

HKZ-bases

$B = QR$ is an **HKZ-basis** (Hermite 1850, Korkine-Zolotareff 1873) if:

1. It is size-reduced: $|r_{i,j}| \leq \frac{1}{2} r_{i,i}$ for all $j > i$
2. $r_{i,i}$ is minimal under all transforms in $\mathrm{GL}_n(\mathbb{Z})$ that preserve $\mathbf{b}_1, ...\mathbf{b}_{i-1}$, (and thus $r_{1,1}, ..., r_{i-1,i-1}$).

Note that $B = QR$ is an LLL/HKZ-bases if and only if R is an LLL/HKZ-basis.

Theorem [LLS90]
An HKZ-basis $B \in \mathbb{R}^{m \times n}$ of lattice $\mathcal{L}$ satisfies

$$4/(i+3) \leq \|\mathbf{b}_i\|^2 \lambda_i^{-2} \leq (i+3)/4 \quad \text{for } i = 1, ..., n.$$

Strongly regular quadratic LLL- forms

We identify sym. matrices $A = A^t \in \mathbb{R}^{n\times n}$ with n-ary quadratic forms $\mathbf{x}^t A\mathbf{x}$. We call $A = A^t = [a_{i,j}]$ **strongly regular** (s.r.) if $\mathcal{D}(A) := \prod_{\ell=1}^{n} \det([a_{i,j}]_{1\le i,j\le \ell}) \neq 0$. Let $D_\sigma \in \{0, \pm 1\}^{n\times n}$ denote the diagonal matrix with diagonal entries $\sigma_1, ..., \sigma_n \in \{\pm 1\}$.

Proposition. Every s.r. $A = A^t = [a_{i,j}] \in \mathbb{R}^{n\times n}$ has a unique decomposition $A = R^t D_\sigma R \in \mathbb{R}^{n\times n}$ with a GNF $R = [r_{i,j}] \in \mathbb{R}^{n\times n}$

Definition. A s.r. $A = A^t = R^t D_\sigma R \in \mathbb{R}^{n\times n}$ is an **LLL- form** if R is an LLL-basis.

The classical LLL-bound $a_{1,1}^2 = \|\mathbf{b}_1\|^2 \le \alpha^{\frac{n-1}{2}} |\det(A)|^{\frac{2}{n}}$ holds for all s.r. LLL-forms $A = [a_{i,j}]$.

The LLL-algorithm extends to s.r. forms. This is obvious as long as A remains s.r. during LLL-reduction, see Simon, Math. of Comp. 2005. Otherwise the following Lemma applies:

The LLL- algorithm for regular/singular LLL- forms

Lemma. Given a non s.r. $A = A^t \in \mathbb{Z}^{n\times n}$ the LLL finds in poly-time an equivalent $A' = [a'_{i,j}]$, $0 \le a'_{2,2} \le 2a'_{1,2}$, that is a direct sum $\begin{bmatrix} 0 & a'_{1,2} \\ a'_{1,2} & a'_{2,2} \end{bmatrix} \oplus [a'_{i,j}]_{3\le i,j\le n}$.

Hence $a'_{1,2} \in \{0, 1\}$ if $\det(A) \neq 0$ is square-free.

Theorem. The LLL transforms in poly-time a form A into a direct sum $\oplus_{i=1}^{k} A^{(i)}$ of an LLL-form $A^{(k)}$ and binary forms $A^{(i)} = \begin{bmatrix} 0 & a_i \\ a_i & b_i \end{bmatrix}$, $0 \le b_i < 2a_i$ for $i = 1, ..., k-1$.

Hence $k = 1$ for positive definite A.

Corollary. The LLL-algorithm transforms an input matrix $B \in \mathbb{R}^{m\times n}$ of rank n' into $[\mathbf{0}, ..., \mathbf{0}, \mathbf{b}'_1, ..., \mathbf{b}'_{n'}] \in \mathbb{R}^{m\times n}$ where $[\mathbf{b}'_1, ..., \mathbf{b}'_{n'}]$ is an LLL-basis. Similarly, an adjusted LLL transforms an input form $A \in \mathbb{Z}^{n\times n}$ of rank n' into an equivalent regular form $A' \in \mathbb{Z}^{n'\times n'}$ with $\det(A') \neq 0$.

Polynomial lattices and polynomial LLL- forms

Polynomial lattices are of the form $\{B\mathbf{x} \mid \mathbf{x} \in \mathbb{Z}\}$ for some $B \in \mathbb{Z}[x]^{m\times n}$ with polynomial entries $B_{i,j}$ and coefficients in $\mathbb{Z}$
A symmetric matrix $A = A^t \in \mathbb{Z}[x]^{n\times n}$ is a **polynomial form**.

We define LLL-bases and LLL-forms for polynomial matrices via a ring homomorphism $\phi : \mathbb{Z}[x] \to \mathbb{Z}$. For $f = \sum_{i=0}^{d} f_i x^i \in \mathbb{Z}[x]$ and $\rho \in_R [1, \tau]$ we define $\phi = \phi_\rho$ by

$$\phi(f) = f(\rho) = \sum_{i=0}^{d} \phi(f_i)\rho^i,$$

where we extend ϕ coordinatewise to $\phi : \mathbb{Z}[x]^n \to \mathbb{Z}^n$.

Then apply the LLL-alg. to forms A by performing the LLL on $\phi(A) \in \mathbb{Z}^{n\times n}$ and apply the LLL- transform $T \in \mathrm{GL}_n(\mathbb{Z})$ to A:

$$\phi(T^t A T) = T^t \phi(A) T.$$

Corollary. The LLL-algorithm extends to polynomial lattices and to polynomial forms.

Minimizing the polynomial degrees in polynomial time.

For a polynomial form $A = [a_{i,j}] \in \mathbb{Z}[x]^{n\times n}$ let $\|A\|$ denote the maximal absolute value of the integer coefficients of $a_{i,j} \in \mathbb{Z}[x]$.

Then $\frac{1}{2}\rho^{\deg(a_{i,j})} \leq |\phi(a_{i,j})| \leq \|A\| \sum_{i=0}^{\deg(a_{i,j})} \rho^i \leq 2\|A\|\rho^{\deg(a_{i,j})}$ holds for $\rho \geq 2\|A\|$. Hence, $|\det \phi(A)| \leq (2n\|A\|)^n \rho^{\deg\det(A)}$.

By Theorem 1 the LLL-form $\phi(A') = T^t \phi(A) T$ satisfies

$$\frac{1}{2}\rho^{\deg(a'_{1,1})} \leq |\phi(a'_{1,1})| \leq \alpha^{\frac{n-1}{4}} (\det \phi(A))^{1/n},$$

$$\deg(a'_{1,1}) \leq \frac{n-1}{4}\frac{\log\alpha}{\log\rho} + \frac{\log(2\|A\|)}{\log\rho} + \frac{\deg\det(A)}{n}.$$

For $\rho > 4\|A\|\alpha^n$ this minimizes $\deg(a'_{1,1})$ and likewise all $\deg(a'_{i,j})$ over $\mathrm{GL}_n(\mathbb{Z})$.

For alternatives and further applications see [MS03, SV05]. Our LLL-reduction transforms via $\mathrm{GL}_n(\mathbb{Z})$, not via $\mathrm{GL}_n(\mathbb{Z}[x])$.

Decreasing α^n within pol. time basis reduction.

blockwise HKZ-reduction [S87]	$2^{O(n(\log\log n)^2/\log n)}$
item + sieving [AKS98]	$2^{O(n\log\log n/\log n)}$
Ajtai, STOC 2003:	the [S87] analysis is optimal up to a constant factor in the exponent.

blockwise HKZ-reduction applies HKZ-reduction in dimension $k = O(\log n/\log\log n)$.

Kannan 1987, Helfrich 1985: HKZ-reduction runs in $O(mn^{n/2+o(n)}\|B\|)$ arithmetic steps.
Stehlé 2007 decreases the exponent $n/2$ to $n/2e$.

Decreasing $\alpha \approx \frac{4}{3}$ under feasible basis reduction

		reduced α
1.	Semi block $2k$-reduction [S87], $k = 24$	
	proven [GHKN06]	$(\beta_{24}/\delta)^{1/24} < 1.165$
	by heuristic, GSA	$\gamma_{48}^{1/47} \approx 1.034$
2.	Primal-dual HKZ-reduction, Koy 2004, $k = 48$	
	proven	$(\alpha\gamma_{48}^2)^{1/48} \approx 1.075$
	by heuristic, GSA	$\gamma_{48}^{1/47} \approx 1.034$
3.	LLL on the average for random lattices	
	experimentally [NS06]	1.08
4.	LLL with deep insertion [SE94] on the average	
	experimentally [NS06]	$1.012^4 \approx 1.05$
5.	Primal-dual RSR, $k = 80$	
	by heuristic, RA, GSA	1.025

The Hermite constant: $\gamma_n = \max \lambda_1^2(\mathcal{L}) / \det(\mathcal{L})^{2/n}$ over all lattices $\mathcal{L}$ of dimension n.

Semi block $2k$-reduction [S87]

Notation. $B = QR \in \mathbb{R}^{m\times n}$, $R = [r_{i,j}]_{1\le i,j\le n}$, $n = hk$

$$R_\ell := [r_{i,j}]_{k\ell-k<i,j\le k\ell} \in \mathbb{R}^{k\times k}$$

$$R_{\ell,\ell+1} = [r_{i,j}]_{k\ell-k<i,j\le k\ell+k} = \begin{bmatrix} R_\ell & R'_\ell \\ O & R_{\ell+1} \end{bmatrix}$$

$$\mathcal{D}_\ell = (\det R_\ell)^2, \quad \det(\mathcal{L})^2 = \prod_{\ell=1}^{h} \mathcal{D}_\ell.$$

$$\beta_k =_{def} \max(\mathcal{D}_1/\mathcal{D}_2)^{1/k} \text{ over all HKZ-reduced}$$

$$R = R_{1,2} = \begin{bmatrix} R_1 & R'_1 \\ O & R_2 \end{bmatrix} \in \mathbb{R}^{2k\times 2k}.$$

Def. $B = QR \in \mathbb{R}^{m\times n}$ is **semi block $2k$-reduced** for $\delta \in (\frac{1}{4}, 1]$, $\alpha = 1/(\delta - \frac{1}{4})$ if $R = [r_{i,j}]$ satisfies

1. $R_1, ..., R_h \subset R$ are HKZ-reduced,
2. $r_{i,i}^2 \le \alpha\, r_{i+1,i+1}^2$ for $i = k, 2k, ..., (h-1)k$,
3. $\delta\, \mathcal{D}_\ell \le \beta_k^k\, \mathcal{D}_{\ell+1}$ for $\ell = 1, ..., h-1$.

Quality of semi block $2k$–reduced bases

Theorem

A semi block $2k$-reduced $B = QR$ satisfies

1. $\|\mathbf{b}_1\|^2 \leq \gamma_k(\beta_k/\delta)^{\frac{n/k-1}{2}}(\det \mathcal{L}(B))^{2/n}$,
2. $\|\mathbf{b}_1\|^2\lambda_1^{-2} \leq k^{\ln k + o(\ln k)}(\beta_k/\delta)^{n/k-2}$.

This replaces α by $(\beta_k/\delta)^{1/k} + o(1)$ for $n/k \to \infty$.

loop of semi block $2k$-reduction (essentials only)

1. HKZ–reduce $R_{\ell,\ell+1}$ into $R_{\ell,\ell+1}T$
2. Compute $\mathcal{D}_\ell^{\text{new}} := (\det R_\ell^{\text{new}})^2$
3. IF $\mathcal{D}_\ell^{\text{new}} \leq \sqrt{\delta}\mathcal{D}_\ell$
   THEN $[B_\ell, B_{\ell+1}] := [B_\ell, B_{\ell+1}]T$,
   $\ell := \max(\ell - 1, 1)$ ELSE $\ell := \ell + 1$.

Semi block $2k$-reduction performs $O(nh \log_{1/\delta} \|B\|)$ HKZ-reductions in dim. $2k$. Here $\|B\| =_{def} \max_i \|\mathbf{b}_i\|^2$.

Primal-dual reduction, Koy 2004

Notat. For a basis $B = QR \in \mathbb{R}^{m\times n}$ let $\bar{r}_{k\ell,k\ell}$ denote $\max \tilde{r}_{k\ell,k\ell}$ over the GNF's $[\tilde{r}_{i,j}]_{k\ell-k<i,j\le k\ell} = \mathrm{GNF}(R_\ell T)$ for all $T \in \mathrm{GL}_k(\mathbb{Z})$.
$r_{k\ell,k\ell} = \bar{r}_{k\ell,k\ell}$ holds for HKZ-reduced $R^*_\ell = U_k R_\ell^{-t} U_k$.
$R^*_\ell = [r^*_{i,j}]$ is the **dual** of $R_\ell = [r_{i,j}]$, $r^*_{1+i,1+i} = 1/r_{n-i,n-i}$ for

$$i = 0, ..., n-1, \quad U_k = \begin{bmatrix} & & 1 \\ & . & \\ 1 & & \end{bmatrix} \in \mathbb{Z}^{k\times k}.$$

Def. $B = QR$ is a **primal–dual** basis for k, δ if

1. $R_1, \ldots, R_h \subset R$ are HKZ–reduced,
2. $\bar{r}^2_{k\ell,k\ell} \le \alpha r^2_{k\ell+1,k\ell+1}$ for $\ell = 1, \ldots, h-1$.

Thm. A primal-dual basis $B = QR$ satisfies

1. $\|\mathbf{b}_1\|^2 \le \gamma_k(\alpha\gamma_k^2)^{\frac{n/k-1}{2}}(\det \mathcal{L})^{2/n}$
2. $\|\mathbf{b}_1\|^2 \le (\alpha\gamma_k^2)^{n/k-1}\lambda_1^2$.

This reduces α to $(\alpha\gamma_k^2)^{1/k}$.

Quality Comparison

Primal-dual reduction performs $O(nh \log_{1/\delta} \|\mathcal{B}\|)$ HKZ-reductions in dim. k.

Comparison	proven red. of $\alpha \approx \frac{4}{3}$
Semi block $2k$-reduction	$(\beta_k/\delta)^{1/k} < 1.165$
primal dual reduction, $2k = 48$	$(\alpha\mu_{2k}^2)^{1/2k} < 1.075$
for both methods under **GSA**	$\gamma_{48}^{1/47} \approx 1.034$

Geometric Series Assumption (GSA)

$$r_{i+1,i+1}^2 / r_{i,i}^2 = q_i = q \quad \text{for all} \quad i$$

This is a worst case heuristic. If the q_i spread then R has segments that are easier to reduce.

Under **GSA**: $1 \leq \gamma_k q^{k-1}$ holds for HKZ-reduced R_ℓ.
Hence $q \geq \gamma_k^{-1/(k-1)}$.

LLL with deep insertion [SE94]

Let $B = QR,\ R = [r_{i,j}] = [\mathbf{r}_1, \ldots, \mathbf{r}_n] \subset \mathbb{R}^{n \times n}$.

LLL–swap IF $\delta r_{l-1,l-1}^2 > r_{l,l}^2 + r_{l-1,l}^2$
THEN swap $\mathbf{b}_{l-1}$ and $\mathbf{b}_l$

Deep insertion IF $\delta r_{j,j}^2 > \sum_{i=j}^{l} r_{j,l}^2$ for $j < l$
THEN $[\mathbf{b}_j, ..., \mathbf{b}_l] := [\mathbf{b}_l, \mathbf{b}_j, ..., \mathbf{b}_{l-1}]$
for the smallest such j

A deep insertion decreases $r_{j,j}^2$ but not $\prod_{i=j+1}^{n-1} r_{i,i}^{2(n-i)}$.
The deep insertion–LLL has no proven pol. time bound. This does not matter in practice.

Comparison	reduced $\alpha \approx \frac{4}{3}$ on average
deep insertion LLL [GN06]	$1.012^4 \approx 1.05$
LLL [GN06] experimentally	$1.04^2 \approx 1.08$

RSR: A Parallel extension of deep insertion [S03]

RSR of $R_{\nu,k} = [r_{i,j}]_{\nu<i,j\le\nu+k} \subset R = [\mathbf{r}_1, \ldots, \mathbf{r}_n] \subset \mathbb{R}^{n\times n}$:

$$T_{\mathbf{a}} =_{def} \begin{bmatrix} a_1 & 1 & & \\ \vdots & 0 & \ddots & \\ & & \ddots & 1 \\ a_{k-1} & & & \\ 1 & 0 & \cdots & 0 \end{bmatrix}$$

Transform $[\mathbf{b}_{\nu+1}, \ldots, \mathbf{b}_{\nu+k}] := T_{\mathbf{a}}[\mathbf{b}_{\nu+1}, \ldots, \mathbf{b}_{\nu+k}]$ such that $(r^{\text{new}}_{\nu+1,\nu+1})^2 \le \delta r^2_{\nu+1,\nu+1}$. Try $(11/k)^{k/4}$ of the most likely choices for $\mathbf{a} = (a_1, \ldots, a_k) \in \mathbb{Z}^k$ with $a_k = 1$.
Deep insertion is the case $a_1 = a_2 = \cdots = a_{k-1} = 0$.

Thm. [**GSA,RA**] If $\max_i r^2_{i+1,i+1}/r^2_{i,i} < (11/k)^{1/k}$ then one out of $(k/11)^{k/4}$ choices of $(a_1, \ldots, a_k)$ guarantees on average that $(r^{\text{new}}_{\nu+1,\nu+1})^2 \le \delta r^2_{\nu+1,\nu+1}$.
This decreases α to $(k/11)^{1/k} \approx 1.025$ for $k = 80$.

loop of Primal-dual RSR, essentials only

Primal RSR-step. Find $0 \le \nu \le n-k$ that nearly maximizes $r_{\nu+1,\nu+1}/(\det R_{\nu,k})^{1/k}$. Try to decrease $r_{\nu+1,\nu+1}$ by the factor δ through RSR of $R_{\nu,k} \subset R$ such that the GNF $R^{new}_{\nu,k} = [r^{new}_{i,j}]$ of $R_{\nu,k}\,T_{\mathbf{a}}$ satisfies $r^{new}_{\nu+1,\nu+1} \le \delta\, r_{\nu+1,\nu+1}$.
For such $T_{\mathbf{a}}$ perform $[\mathbf{b}_{\nu+1},\ldots,\mathbf{b}_{\nu+k}] := [\mathbf{b}_{\nu+1},\ldots,\mathbf{b}_{\nu+k}]\,T_{\mathbf{a}}$.

Dual RSR-step. Find $0 \le \nu \le n-k$ that nearly minimizes $r_{\nu+k,\nu+k}/(\det R_{\nu,k})^{1/k}$. Apply RSR to the dual GNF $R^*_{\nu,k} = U_k R^{-t}_{\nu,k} U_k$. Try to increase $r_{\nu+k,\nu+k}$ by the factor δ through RSR of $R^*_{\nu,k} \subset R^*$

From time to time BKZ-reduce the GNF R with small block length to better approximate the GSA-property.

References

AKS01 *M. Ajtai, R. Kumar, and D. Sivakumar*, A sieve algorithm for the shortest lattice vector problem, In Proc. 33th STOC, pp. 601–610, ACM, 2001.

A03 *A. Ajtai*, The worst-case behavior of Schnorr's algorithm approximating the shortest nonzero vector in a lattice. 35th STOC, pp. 396–406, 2003.

Ka87 *R. Kannan*, Minkowski's convex body theorem and integer programming. Mathematics of Operations Research, **12**, pp. 415–440, 1987.

K04 *H. Koy*, Primal/duale Segment-Reduktion von Gitterbasen, Lecture Universität Frankfurt 2000, files from Mai 2004. //www.mi.informatik.uni-frankfurt.de/research/papers.html

LLL82 *A. K. Lenstra, H. W. Lenstra and L. Lovász*, Factoring polynomials with rational coefficients. *Math. Ann.*, **261**, pp. 515–534, 1982.

References

NS06 *P. Nguyen and D. Stehlé*, LLL on the average. In Proc. ANTS VII, Berlin, 23.–28. July 2006, LNCS, Springer-Verlag, New York, (to appear) 2006.

S87 *C.P. Schnorr*, A Hierarchy of polynomial time lattice basis reduction algorithms. *Theoret. Comput. Sci.*, **53**, pp. 201–224, 1987.

SE94 *C.P. Schnorr and M. Euchner*, Lattice basis reduction: improved algorithms and solving subset sum problems. *Mathematics of Programming*, **66**, pp. 181–189, 1994.

S03 *C.P. Schnorr*, Lattice reduction by random sampling and birthday methods. in Proc. STACS 2003, Eds. H. Alt and M. Habib, LNCS 2607, Springer-Verlag, New York, pp. 145–156, 2003. //www.mi.informatik.uni-frankfurt.de.html

S06 *C.P. Schnorr*, Fast LLL-type lattice reduction. *Information and Computation*, **204**, pp. 1–25,