Average Time Fast SVP and CVP Algorithms: Factoring Integers in Polynomial Time

Claus P. SCHNORR

Fachbereich Informatik und Mathematik
Goethe-Universität
Frankfurt am Main

Rump session Eurocrypt 2009

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

New average time fast CVP/ SVP algorithms

Main Theorem.

Given a lattice vector of length $\leq \sqrt{2e\pi}\, n^b \lambda_1$ NEW ENUM finds under **GSA** a shortest lattice vector in linear space and

$$n^{O(1)} + (n^{b+o(1)} rd(\mathcal{L})^4)^{n/8} \text{ time.}$$

Here n is the dimension of lattice $\mathcal{L}$, the *relative density* of $\mathcal{L}$:

$$rd(\mathcal{L}) =_{def} \lambda_1 \gamma_n^{-1/2} (\det \mathcal{L})^{-1/n} \leq 1$$

relates to the first successive minimum λ_1 and the HERMITE constant γ_n which satisfies for all $\mathcal{L}$: $\lambda_1^2 \leq \gamma_n (\det \mathcal{L})^{2/n}$.

The time bound is polynomial if $rd(\mathcal{L})$ is not nearly maximal.

GSA: assumes, for simplicity, that the quotients of the lengths of two consecutive orthogonalized basis vectors all coincide.

The assumption **GSA** has been used previously in theory and practice [S03, S07]. It is the **Geometrical Series Assumption**.

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, Lovàsz 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

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

The Schnorr Adleman Prime Number Lattice

Let N be a positive integer that is not a prime power. Let $p_1 < \cdots < p_n$ enumerate all primes less than $(\ln N)^\alpha$ for some $\alpha > 1$. Let the prime factors p of N satisfy $p > p_n$.

We show how to factor N by solving easy CVP's for the lattice $\mathcal{L}(B)$ with the following basis matrix $B = [\mathbf{b}_1, \ldots, \mathbf{b}_n] \in \mathbb{R}^{(n+1)\times n}$ and the target vectors $\mathbf{N} \in \mathbb{R}^{n+1}$ for some $c > 0$ and either $N' = N$ or $N' = Np_{n+j}$ for some prime $p_{n+j} > p_n$:

$$B = \begin{bmatrix} \sqrt{\ln p_1} & & \\ & \ddots & \\ & & \sqrt{\ln p_n} \\ N^c \ln p_1 & \cdots & N^c \ln p_n \end{bmatrix}, \quad \mathbf{N} = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ N^c \ln N' \end{bmatrix}.$$

Constructing Nearly Shortest Lattice Vectors

Lemma 5.3 [Micciancio, Goldwasser 02] $\lambda_1(B)^2 \geq 2c \ln N$.

For a nearly shortest lattice vector we need two smooth integers u, v that are very close, e.g., $|u - v| = 1$.

Problem is not known to be polynomial time.

We extend the prime basis by irreducible algebraic numbers $a \pm \omega_s^j$ for $j = 1, ..., 2^{s-1} - 1$, where $\omega_s^{2^{s-1}} = -1$.

Note that $a^{2^s} - 1 = \prod_{j=1}^{2^s} (a + \omega_s^j)$ holds for all arbitrary a.

$s = 1$: $a^2 - 1 = (a - 1)(a + 1)$.

For $a = 2$ this yields smooth numbers $u = 2^{2^s}$, $v = 2^{2^s} - 1$.

Complex lattices: replace $\mathbb{R}$ by $\mathbb{C}$ and $\mathbb{Z}$ by $\mathbb{Z}[i]$.
LLL-reduction of $B \in \mathbb{C}^{m \times n}$ nicely extends to complex bases B

$$\mathcal{L}(B) =_{def} \{Bz \mid z \in \mathbb{Z}[i]^n\}.$$

References

Ad95 *L.A. Adleman*, Factoring and lattice reduction. Manuscript, 1995.

AEVZ02 *E. Agrell, T. Eriksson, A. Vardy and K. Zeger*, Closest point search in lattices. *IEEE Trans. on Inform. Theory*, **48** (8), pp. 2201–2214, 2002.

Aj96 *M. Ajtai*, Generating hard instances of lattice problems. In Proc. 28th Annual ACM Symposium on Theory of Computing, pp. 99–108, 1996.

AD97 *M. Ajtai and C. Dwork*, A public-key cryptosystem with worst-case / average-case equivalence. In Proc 29-th Annual ACM Symposium on Theory of Computing, pp. 284–293, 1997.

Ba86 *L. Babai*, On Lovasz' lattice reduction and the nearest lattice point problem. *Combinatorica* **6 (1)**, pp.1–13, 1986.

BL05 *J. Buchmann and C. Ludwig*, Practical lattice basis sampling reduction. eprint.iacr.org, TR 072, 2005.

Ca98 *Y.Cai*, A new transference theorem and applications to Ajtai's connection factor. ECCC, Report No. 5, 1998.

C00 *S. Cavallar et alii*, Factorization of a 512-Bit RSA modulus. In Proc. EUROCRYPT 2000, LNCS 1807, Springer-Verlag, Berlin New York, pp. 1–18, 2000.

CEP83 E.R. Canfield, P. Erdös and C. Pomerance, On a problem of Oppenheim concerning "Factorisatio Numerorum". *J. of Number Theory*, **17**, pp. 1–28, 1983.

C093 *H. Cohen*, A Course in Computational Algebraic Number Theory, Springer-Verlag, Berlin New York, 1993.

CS93 *J.H. Conway and N.J.A. Sloane*, Sphere Packings, Lattices and Groups. third edition, Springer-Verlag, Berlin New York, 1998.

FP85 *U. Fincke and M. Pohst*, Improved methods for calculating vectors of short length in a lattice, including a complexity analysis. *Math. of Comput.*, **44**, pp. 463–471, 1985.

HS07 *G. Hanrot and D. Stehlé*, Improved analysis of Kannan's shortest lattice vector algorithm. In Proc. CRYPTO 2007, LNCS 4622, Springer-Verlag, Berlin New York, pp. 170–186, 2007.

HS08 *G. Hanrot and D. Stehlé*, Worst-case Hermite-Korkine-Zolotarev reduced lattice bases. CoRR, abs/0801.3331, http://arxix.org/abs/0801.3331.

HPS98 *J. Hoffstein, J. Pipher and J. Silverman*, NTRU: A ring-based public key cryptosystem. In Proc. ANTS III, LNCS, Springer-Verlag, Berlin New York, 1423, pp. 267–288, 1998.

Ka87 *R. Kannan*, Minkowski's convex body theorem and integer programming. *Math. Oper. Res.*, **12**, pp. 415–440, 1987.

KL78 *G.A.Kabatiansky and V.I. Levenshtein*, Bounds for packing on a sphere and in space. *Problems of Information Transmission*, **14**, pp. 1–17, 1978.

KS01 *H. Koy and C.P. Schnorr*, Segment LLL-reduction with floating point orthogonalization. In Proc. CaLC 2001, LNCS 2146, Springer-Verlag, Berlin New York, pp. 81–96, 2001. //www.mi.informatik.uni-frankfurt.de/research/papers.html

LLL82 H. W. Lenstra jun., A. K. Lenstra, and L. Lovász, *Factoring polynomials with rational coefficients*, Mathematische Annalen 261 (1982), pp. 515–534.

MO90 *J. Mazo and A. Odlydzko*, Lattice points in high-dimensional spheres. Monatsh. Math. 110, pp. 47–61, 1990.

MG02 *D. Micciancio and S. Goldwasser*, Complexity of Lattice Problems: A Cryptographic Perspective. Kluwer Academic Publishers, Boston, London, 2002.

NS06 *P. Nguyen and D. Stehlé*, LLL on the average. In Proc. ANTS-VII, LNCS 4076, Springer-Verlag, Berlin New York, pp. 238–356, 2006.

NV07 *P. Nguyen and T. Vidick*, Sieve algorithms for the shortest vector problem are practical. To appear in *J. Math. Crypt.* 2008.

S87 *C.P. Schnorr*, A Hierarchy of Polynomial Time Lattice Basis Reduction Algorithms. *Theoret. Comput. Sci.*, **53**, pp. 201–224, 1987.

S88 S88 *C.P. Schnorr*, A More Efficient Algorithm for Lattice Reduction. *J. of Algor.* **9**, 47–62, 1988.
S93 S93 *C.P.Schnorr*, Factoring integers and computing discrete logarithms via Diophantine approximation. In *Advances in Computational Complexity*, AMS, *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, **13**, pp. 171–182, 1993. Preliminary version in Proc. EUROCRYPT'91, LNCS 547, Springer-Verlag, Berlin New York, pp. 281–293, 1991. //www.mi.informatik.uni-frankfurt.de.
S94 S94 *C.P.Schnorr*, Block reduced lattice bases and successive minima. *Comb. Prob. and Comp.* **3**, pp. 507–522, 1994.
SE94 SE94 *C.P. Schnorr and M. Euchner*, Lattce basis reduction: Improved practical algorithms and solving subset sum problems. Mathematical Programming **66**, pp. 181–199, 1994. //www.mi.informatik.uni-frankfurt.de.

SH95 *C.P. Schnorr and H.H. Hörner*, Attacking the Chor–Rivest cryptosystem by improved lattice reduction. In Proc. EUROCRYPT'95, LNCS 921, Springer-Verlag, Berlin New York, pp. 1–12, 1995. //www.mi.informatik.uni-frankfurt.de.

S03 *C.P. Schnorr*, Lattice reduction by sampling and birthday methods. Proc. STACS 2003: 20th Annual Symposium on Theoretical Aspects of Computer Science, LNCS 2007, Springer-Verlag, Berlin New York, pp. 146–156, 2003. //www.mi.informatik.uni-frankfurt.de

S06 *C.P. Schnorr*, Fast LLL-type lattice reduction. Information and Computation, **204**, pp. 1–25, 2006. //www.mi.informatik.uni-frankfurt.de

S07 *C.P. Schnorr*, Progress on LLL and lattice reduction, Proceedings LLL$+$25, Caen, France, June 29–July 1, 2007, Final version to appear; //www.mi.informatik.uni-frankfurt.de.