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

Claus P. SCHNORR

Fachbereich Informatik und Mathematik
Goethe-Universität
Frankfurt am Main

Workshop Factoring 2009, Sept. 11,12

RUHR-UNIVERSITÄT BOCHUM

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

I Lattice notation, Time bound of new SVP/CVP algorithm

II Factoring integers via easy CVP solutions

III Outline and partial analysis of the new SVP algorithm

We survey how to use known proof elements and we focus on novel proof elements that are not covered by published work.

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	$\Vert\mathbf{x}\Vert = \langle \mathbf{x}, \mathbf{x} \rangle = (\sum_{i=1}^m x_1^1)^{1/2}$
SV-length	$\lambda_1(\mathcal{L}) = \min\{\Vert\mathbf{b}\Vert \mid \mathbf{b} \in \mathcal{L} \backslash \{0\}\}$
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 $i = 1, \ldots, n-1$.

Def. The *relative density of* $\mathcal{L}$: $rd(\mathcal{L}) := \lambda_1 \gamma_n^{-1/2} (\det \mathcal{L})^{-1/n}$

$rd(\mathcal{L}) = \lambda_1(\mathcal{L}) / \max \lambda_1(\mathcal{L}')$ holds for the maximum of $\lambda_1(\mathcal{L}')$ over all lattices $\mathcal{L}'$ such that $\dim \mathcal{L} = \dim \mathcal{L}'$ and $\det \mathcal{L} = \det \mathcal{L}'$.

The HERMITE constant $\gamma_n = \max\{\lambda_1^2 / \det(\mathcal{L})^{2/n} \mid \dim \mathcal{L} = n\}$.

We always have $\|\mathbf{b}_1\|^2 = rd(\mathcal{L})^2 \gamma_n (\det \mathcal{L})^{2/n}$.

Theorem 4.1 (GSA). Given a lattice basis such that $\|\mathbf{b}_1\| \leq \sqrt{2e\pi}\, n^b \lambda_1$, $b \geq 0$, NEW ENUM solves SVP in time $n^{O(1)} + (O(n^{2b-\varepsilon}))^{\frac{n+1}{4}}$ if $rd(\mathcal{L}) = n^{-\frac{1}{2}-\varepsilon}$, $\varepsilon > 0$.

This time bound is polynomial if $2b < \varepsilon$.

GSA : Let $B = QR = Q[r_{i,j}]$ satisfy (for $r_{i,i} = \|\mathbf{b}_i^*\|$):
$r_{i,i}^2 / r_{i-1,i-1}^2 = q$ for $i = 2, ..., n$ and some $q > 0$.

W.l.o.g. let $q < 1$, otherwise $\|\mathbf{b}_1\| = \lambda_1$.

We outline the proof of Thm 4.1 in part III.

Corollary 6.1 (GSA). Given $\mathbf{b}_1 \in \mathcal{L}$, $0 \neq \|\mathbf{b}_1\| = O(\lambda_1)$, NEW ENUM finds $\mathbf{b} \in \mathcal{L}$ such that $\|\mathbf{b} - \mathbf{t}\| = \|\mathcal{L} - \mathbf{t}\|$ in time

$$n^{O(1)} + O(\sqrt{n}\, rd(\mathcal{L})\, \|\mathcal{L} - \mathbf{t}\|^2\, \lambda_1^{-2})^{\frac{n+1}{4}}.$$

This time bound is polynomial if

$$\|\mathcal{L} - \mathbf{t}\| = O(\lambda_1) \text{ and } rd(\mathcal{L}) \leq n^{-\frac{1}{2}-\varepsilon} \text{ for } \varepsilon > 0.$$

The required short vector $\mathbf{b}_1$ can in practice be added to the basis, extending the lattice by a short vector preserving $rd(\mathcal{L})$.

An example will be given in part II for factoring integers using the 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 $(\ln N)^\alpha$. Then

$$n = (\ln N)^\alpha / (\alpha \ln\ln N)(1 + O(1)/\alpha \ln\ln N).$$

Let the prime factors p of N satisfy $p > p_n$.

We show how to factor N by solving easy CVP's for the prime number lattice $\mathcal{L}(B)$, basis matrix $B = [\mathbf{b}_1, \ldots, \mathbf{b}_n] \in \mathbb{R}^{(n+1)\times n}$:

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

and the target vector $\mathbf{N} \in \mathbb{R}^{n+1}$, where either $N' = N$ or $N' = Np_{n+j}$ for one of the next n primes $p_{n+j} > p_n$, $j \le n$. W.l.o.g. let $N' = N$ for the analysis.

We identify the vector $\mathbf{b} = \sum_{i=1}^{n} e_i \mathbf{b}_i \in \mathcal{L}(B)$ with the pair (u, v) of integers $\quad u = \prod_{e_j > 0} p_j^{e_j}, \;\; v = \prod_{e_j < 0} p_j^{-e_j} \in \mathbb{N}$.

Then u, v are free of primes larger than p_n and $\gcd(u, v) = 1$.

We compute vectors $\mathbf{b} = \sum_{i=1}^{n} e_i \mathbf{b}_i \in \mathcal{L}(B)$ close to $\mathbf{N}$ such that $|u - vN'| < u$. The prime factorizations $|u - vN'| = \prod_{i=1}^{n} p_i^{e_i'}$ and of u yield a non-trivial relation

$$\prod_{e_i > 0} p_i^{e_i} = \pm \prod_{i=1}^{n} p_i^{e_i'} \mod N. \tag{7.1}$$

Given $n+1$ independent relations (7.1) we write these relations with $p_0 = -1$ and $e_{i,j}, e_{i,j}' \in \mathbb{N}$ as $\quad \prod_{i=0}^{n} p_i^{e_{i,j} - e_{i,j}'} = 1 \mod N$ for $j = 1, ..., n+1$. Any non trivial solution $z_1, ..., z_{n+1} \in \mathbb{Z}$ of the equations $\quad \sum_{j=1}^{n+1} z_j (e_{i,j} - e_{i,j}') = 0 \mod 2$ for $i = 0, ..., n$

solves $X^2 = Y^2 \mod N$ with $X = \prod_{j=1}^{n+1} p_j^{\sum_{i=0}^{n} z_i e_{i,j}} \mod N$,

$$Y = \prod_{j=1}^{n+1} p_j^{\sum_{i=0}^{n} z_i e_{i,j}'} \mod N.$$

Lemma If $|u - vN'| = o(N^c)$, $v = \Theta(N^{c-1})$, $e_1, \dots, e_n \in \{0 \pm 1\}$ then $\|\mathbf{b} - \mathbf{N}\|^2 = (2c-1)\ln N + \ln(p_{n+j}) + \Theta(|u - vN'|^2 (N/N')^2)$.

Proof. We see from $e_1, \dots, e_n \in \{0 \pm 1\}$ that $\|\mathbf{b} - \mathbf{N}\|^2 = \ln u + \ln v + N^{2c} |\ln \frac{u}{vN'}|^2$.

Clearly, $v = \Theta(N^{c-1})$, $|u - vN'| = o(N^c)$ implies

$$\ln u + \ln v = (2c-1)\ln N + \ln(N'/N) + \Theta(1).$$

Moreover

$$|\ln \tfrac{u}{vN'}| = |\ln\left(1 + \tfrac{u - vN'}{vN'}\right)| = \tfrac{|u - vN'|}{vN'}(1 + o(1)) = \Theta\left(\tfrac{|u - vN'|}{N^{c-1}N'}\right).$$

Combining these equations proves the claim. $\square$

Theorem 7.2 $\|\mathbf{b} - \mathbf{N}\|^2 \le (2c-1)\ln N + 2\delta \ln p_n$ implies

$$|u - vN'| \le p_n^{\frac{1}{\alpha} + \delta + o(1)}.$$

An integer z is called *y-smooth*, if all prime factors p of z satisfy $p \le y$. Let N' be either N or Np_{n+j} for one of the next n primes $p_{n+j} > p_n$. We denote

$$M_{\alpha,c,N} = \left\{ (u,v) \in \mathbb{N}^2 \middle| \begin{array}{l} u \le N^c, |u - vN'| = 1, N^{c-1}/2 < v < N^{c-1} \\ u, v \text{ are squarefree and } (\ln N)^\alpha-\text{smooth} \end{array} \right\}.$$

Theorem 7.4 [S93] If the equation $|u - \lceil u/N \rfloor N| = 1$ is for random u of order N^c nearly statistically independent from the event that $u, \lceil u/N \rfloor$ are squarefree and $(\ln N)^\alpha$-smooth then $\# M_{\alpha,c,N} = N^{\varepsilon + o(1)}$ holds if $\alpha > \frac{2c-1}{c-1}, c > 1$.

We will use this theorem for $c = \ln N$ and $\alpha > 4$.

Theorem 7.5 The vector $\mathbf{b} = \sum_{i=1}^{n} e_i \mathbf{b}_i \in \mathcal{L}(B)$ closest to $\mathbf{N}$ provides a non-trivial relation (7.1) provided that $M_{\alpha,c,N} \neq \emptyset$.

Theorem 7.6 If $M_{\alpha,c,N} \neq \emptyset$ for $c = \ln N$ and $\alpha > 4$ then we can minimize $\|\mathcal{L}(B) - \mathbf{N}\|$ in polynomial time under GSA given $\mathbf{b} \in \mathcal{L}(B)$ such that $0 \neq \|\mathbf{b}\| = O(\lambda_1)$.

It follows from $M_{\alpha,c,N} \neq \emptyset$ for $N' \in \{N, Np_{n+j}\}$ that

$$\|\mathcal{L} - \mathbf{N}\|^2 \leq (2c - 1)\ln N' + 1 = (2c - 1 + o(1))\ln N.$$

Lemma 5.3 of [MG02] proves that $\lambda_1^2 \geq 2c \ln N - \Theta(1)$

Claim $\lambda_1^2 = 2c \ln N + O(1)$.

$$rd(\mathcal{L}) = \lambda_1 / (\sqrt{\gamma_n} (\det \mathcal{L})^{\frac{1}{n}}) \lesssim \left(\frac{2e\pi\, 2c \ln N}{(\ln N)^{\alpha}}\right)^{\frac{1}{2}}$$
$$= O(c \ln N)^{(1-\alpha)/2} = O((\ln N)^{1-\alpha}).$$

Moreover, we have for $c = \ln N$, $\alpha > 4$ and $\varepsilon = \frac{1}{2} - 1/\alpha > 0$ that

$$n^{-\frac{1}{2} - \varepsilon} = n^{-1+1/\alpha} \approx (\alpha \ln \ln N)^{1-1/\alpha} (\ln N)^{1-\alpha} > rd(\mathcal{L}).$$

We extend the prime number basis B and $\mathcal{L}(B)$ by a nearly shortest lattice vector of the extended lattice, preserving $rd(\mathcal{L})$, $\det(\mathcal{L})$ and the structure of the lattice.

We extend the prime base by a prime $\bar{p}_{n+1}$ of order $\Theta(N^c)$ such that $|u - \bar{p}_{n+1}| = O(1)$ holds for a squarefree $(\ln N)^\alpha$-smooth u. Then $\| \sum_i e_i \mathbf{b}_i - \mathbf{b}_{n+1} \|^2 = 2c \ln N + O(1)$ holds for $u = \prod_i p_i^{e_i}$ the additional basis vector $\mathbf{b}_{n+1}$ corresponding to $\bar{p}_{n+1}$. $\sum_i e_i \mathbf{b}_i - \mathbf{b}_{n+1}$ is a nearly shortest vector of $\mathcal{L}(\mathbf{b}_1, ..., \mathbf{b}_{n+1})$.

Efficient construction of $\bar{p}_{n+1}$. Generate u at random and test the nearby $\bar{p}$ for primality. If the density of primes near the u is not exceptionally small $\bar{p}_{n+1}$ and $\mathbf{b}_{n+1}$ can be found in probabilistic polynomial time. A single $\bar{p}_{n+1}$ can be used to solve all CVP's for the factorization of all integers of order $\Theta(N)$.

Let $\pi_t : \mathrm{span}(\mathbf{b}_1, ..., \mathbf{b}_n) \to \mathrm{span}(\mathbf{b}_1, ..., \mathbf{b}_{t-1})^\perp$ for $t = 1, ..., n$ denote the orthogonal projections and let $\mathcal{L}_t = \mathcal{L}(\mathbf{b}_1, ..., \mathbf{b}_{t-1})$.

Stage $(\mathbf{u_t}, ..., \mathbf{u_n})$ of ENUM. $\mathbf{b} := \sum_{i=t}^n u_i \mathbf{b}_i \in \mathcal{L}$ and $u_t, ..., u_n \in \mathbb{Z}$ are given. The stage searches exhaustively for all $\sum_{i=1}^{t-1} u_i \mathbf{b}_i \in \mathcal{L}$ such that $\| \sum_{i=1}^n u_i \mathbf{b}_i \|^2 \leq A$ holds for a given upper bound $A \geq \lambda_1^2$. We have

$$\| \sum_{i=1}^n u_i \mathbf{b}_i \|^2 = \| \zeta_t + \sum_{i=1}^{t-1} u_i \mathbf{b}_i \|^2 + \| \pi_t(\mathbf{b}) \|^2.$$

where $\zeta_t := \mathbf{b} - \pi_t(\mathbf{b}) = Q\mathbf{v}_t \in \mathrm{span}\, \mathcal{L}_t$ is the orthogonal projection in $\mathrm{span}\, \mathcal{L}_t$ of the given $\mathbf{b} = \sum_{i=t}^n u_i \mathbf{b}_i$ and $\mathbf{v}_t = (v_1, ..., v_{t-1}, 0^{n-t+1})^t$ for $v_i = \sum_{i=t}^n r_{i,j} u_j$. Stage $(u_t, ..., u_n)$ exhaustively enumerates $\mathcal{B}_{t-1}(\zeta_t, \rho_t) \cap \mathcal{L}_t$, the intersection of the lattice $\mathcal{L}_t$ and the sphere $\mathcal{B}_{t-1}(\zeta_t, \rho_t) \subset \mathrm{span}\, \mathcal{L}_t$ of dimension $t-1$ with radius $\rho_t := (A - \| \pi_t(\mathbf{b}) \|^2)^{1/2}$ and center ζ_t.

The success rate β_t of stages

The GAUSSIAN volume heuristics estimates $|\mathcal{B}_{t-1}(\zeta_t, \rho_t) \cap \mathcal{L}_t|$ for $t > 1$ to

$$\beta_t =_{def} \mathrm{vol}\, \mathcal{B}_{t-1}(\zeta_t, \rho_t) / \det \mathcal{L}_t .$$

Here $\quad \mathrm{vol}\, \mathcal{B}_{t-1}(\zeta_t, \rho_t) = V_{t-1} \rho_t^{t-1}, \quad V_{t-1} = \pi^{\frac{t-1}{2}} / (\frac{t-1}{2})!$
is the volume of the unit sphere of dimension $t-1$,

$$\det \mathcal{L}_t = \prod_{i=1}^{t-1} r_{i,i}, \;\; \rho_t^2 := A - \|\pi_t(\sum_{i=t}^{n} u_i \mathbf{b}_i)\|^2 .$$

We call β_t the **success rate** of stage $(u_t, ..., u_n)$.

If $\zeta_t \mod \mathcal{L}_t$ is uniformly distributed over

$$\{\sum_{i=1}^{t-1} r_i \mathbf{b}_i \,|\, 0 \le r_1, ..., r_{t-1} < 1\}$$

then $\mathrm{E}_{\zeta_t}[\, |\mathcal{B}_{t-1}(\zeta_t, \rho_t) \cap \mathcal{L}_t| \,] = \beta_t$, where E_{ζ_t} refers to a random $\zeta_t \mod \mathcal{L}_t$. This holds because $1/\det \mathcal{L}_t$ is the number of lattice points of $\mathcal{L}_t$ per volume in $\mathrm{span}\, \mathcal{L}_t$. The formal analysis of NEW ENUM by Theorem 4.1 uses a proven version of the volume heuristics without assuming that $\zeta_t \mod \mathcal{L}_t$ is random.

INPUT LLL-basis $B = QR \in \mathbb{Z}^{m\times n}$, $R \in \mathbb{R}^{n\times n}$, $A := \frac{n}{4}(\det B^t B)^{2/n}$,
OUTPUT a sequence of $\mathbf{b} \in \mathcal{L}(B)$ of decreasing length
$\|\mathbf{b}\|^2 \le A$ terminating with $\|\mathbf{b}\| = \lambda_1$.

1. $s := 1$, $L_s := \emptyset$, (we call s the *level*)
2. *Perform algorithm* ENUM *[SE94] pruned to stages with* $\beta_t \ge 2^{-s}$:
   Upon entry of stage $(u_t, ..., u_n)$ compute β_t. If $\beta_t < 2^{-s}$ delay this stage and store $(\beta_t, u_t, ..., u_n)$ in the list L_s of *delayed stages*
   If $\beta_t \ge 2^{-s}$ perform stage $(u_t, ..., u_n)$ on level s, and as soon as some non-zero $\mathbf{b} \in \mathcal{L}$ of length $\|\mathbf{b}\|^2 \le A$ has been found give out $\mathbf{b}$ and set $A := \|\mathbf{b}\|^2 - 1$.
3. $L_{s+1} := \emptyset$, perform the stages $(u_t, ..., u_n)$ of L_s with $\beta_t \ge 2^{-s-1}$ in increasing order of t and for fixed t in order of decreasing β_t.
   Collect the appearing substages $(u_{t'}, ..., u_t, ..., u_n)$
   with $\beta_{t'} < 2^{-s-1}$ in L_{s+1}.
4. IF $L_{s+1} \ne \emptyset$ THEN [$s := s + 1$, GO TO 3]
   ELSE *terminate by exhaustion*.

Thm 4.1 NEW ENUM solves SVP in time $n^{O(1)} + (O(n^{2b-\varepsilon}))^{\frac{n+1}{4}}$ if $rd(\mathcal{L}) = n^{-\frac{1}{2}-\varepsilon}$, $\varepsilon > 0$ and if $\mathbf{b}_1\| \leq \sqrt{2e\pi}\, n^b$.

NEW ENUM essentially performs stages in decreasing order of the success rate β_t. Let $\mathbf{b}' = \sum_{i=1}^{n} u_i'\mathbf{b}_i \in \mathcal{L}$ denote the unique vector of length λ_1 that is found by NEW ENUM.

Let β_t' be the success rate of stage $(u_t', ..., u_n')$.
NEW ENUM performs stage $(u_t', ..., u_n')$ prior to all stages $(u_t, ..., u_n)$ of success rate $\beta_t \leq \frac{1}{2}\beta_t'$

Simplifying assumption. We assume that NEW ENUM performs stage $(u_t', ..., u_n')$ prior to all stages of success rate $\beta_t < \beta_t'$, (i.e., $\rho_t < \rho_t'$).
By definition $\rho_t^2 = A - \|\pi_t(\mathbf{b})\|^2$ and ${\rho_t'}^2 = A - \|\pi_t(\mathbf{b}')\|^2$.

Without using the simplifying assumption, the proven time bound of Theorem 4.1 increases at most by the factor 2.

Consider the number $\mathcal{M}_t$ of stages $(u_t, ..., u_n)$ with $\|\pi_t(\sum_{i=t}^n u_i \mathbf{b}_i)\| \le \lambda_1$: $\qquad \mathcal{M}_t := \#\big(\mathcal{B}_{n-t+1}(\mathbf{0}, \lambda_1) \cap \pi_t(\mathcal{L})\big)$.
Modulo the heuristic simplifications $\mathcal{M}_t$ covers the stages that precede $(u'_t, ..., u'_n)$ and those that finally prove $\|\mathbf{b}'\| = \lambda_1$.

Lemma 4.2 $\mathcal{M}_t \le e^{\frac{n-t+1}{2}} \prod_{i=t}^n (1 + \frac{\sqrt{8\pi}\,\lambda_1}{\sqrt{n-t+1}\, r_{i,i}})$.

Proof. We use the method of Lemma 1 of [MO90] and follow the adjusted proof of (2) in section 4.1 of [HS07]. We abbreviate $n_t = n - t + 1$. Consider the ellipsoid

$$\mathcal{E}_t = \{(x_t, ..., x_n)^t \in \mathbb{R}^{n_t} \mid \|\pi_t(\textstyle\sum_{i=t}^n x_i b_i)\|^2 \le \lambda_1^2\}, \text{ where}$$

$\|\pi_t(\sum_{i=t}^n x_i b_i)\|^2 = \sum_{i=t}^n \sum_{j=i}^n (r_{i,j} x_j)^2 = \sum_{i=t}^n \sum_{j=i}^n (\mu_{j,i} x_j)^2 \|\mathbf{b}_i^*\|^2$.
By definition $\mathcal{M}_t \le \#(\mathcal{E}_t \cap \mathbb{Z}^{n_t})$. We set

$$\textstyle\sum_i \mathbf{x} := \sum_{j>i} \frac{r_{i,j}}{r_{i,i}} x_j \ \text{ and } \ x'_i := x_i + \lceil \sum_i \mathbf{x} \rfloor,$$

$$\{\textstyle\sum_i \mathbf{x}\} := \sum_i \mathbf{x} - \lceil \sum_i \mathbf{x} \rfloor,$$

$$\mathcal{F}_t := \{(x'_t, ..., x'_n)^t \in \mathbb{R}^{n_t} \mid \textstyle\sum_{i=t}^n (x'_i + \{\sum_i \mathbf{x}\})^2 r_{i,i}^2 \le \lambda_1^2\}.$$

Proof. The transformation $(x_t, ..., x_n) \mapsto (x'_t, ..., x'_n)$ is injective.
[If $i \ge t$ is the least index such that $(y_i, ..., y_n)$ and $(z_i, ..., z_n)$ differ then $y'_i \ne z'_i$. Moreover $(x'_i + \{\sum_i \mathbf{x}\})r_{i,i} = \sum_{j=i}^n r_{i,j}x_j$.]

We simplify $\mathcal{E}_t$ to $\quad \mathcal{E}'_t = \{\mathbf{x}' \in \mathbb{R}^{n_t} \mid \sum_{i=t}^n {x'_i}^2 r_{i,i}^2 \le 4\lambda_1^2\}$.

Since $|\{\sum_i \mathbf{x}\}| \le \frac{1}{2}$, $x_i \in \mathbb{Z}$ and $|x_i + \varepsilon|^2 \ge x_i^2/4$ for $|\varepsilon| \le \frac{1}{2}$ we see that $\mathcal{F}_t \cap \mathbb{Z}^{n_t} \subset \mathcal{E}'_t \cap \mathbb{Z}^{n_t}$. Hence $\mathcal{M}_t \le \#(\mathcal{E}'_t \cap \mathbb{Z}^{n_t})$.
We bound $\#(\mathcal{E}'_t \cap \mathbb{Z}^{n_t})$ using the method of [MO90, Lemma 1].
Denoting $N_r := \#\{(k_t, ..., k_n)^t \in \mathbb{Z}^{n_t} \mid \sum_{i=t}^n r_{i,i}^2 k_i^2 = r\}$ we have

$$\#(\mathcal{E}'_t \cap \mathbb{Z}^{n_t}) = \sum_{0 \le r \le 4\lambda_1^2} N_r\, e^{s(4\lambda_1^2 - r)n_t} \le e^{s4\lambda_1^2 n_t} \sum_{r \ge 0} N_r\, e^{-srn_t}$$

$$\le e^{s4\lambda_1^2 n_t} \prod_{i=t}^n \sum_{k_i \in \mathbb{Z}} e^{-sr_{i,i}^2 k_i^2 n_t} \le e^{s4\lambda_1^2 n_t} \prod_{i=t}^n \left(1 + \frac{\sqrt{\pi}}{\sqrt{sn_t}\, r_{i,i}}\right)$$

since $\sum_{k \in \mathbb{Z}} e^{-Tk^2} = 1 + 2\sum_{k=1}^\infty e^{-Tk^2} \le 1 + 2\int_0^\infty e^{-Tx^2}dx = 1 + \sqrt{\pi/T}$. We get for $s := 1/(8\lambda_1^2)$:

$$\#(\mathcal{E}'_t \cap \mathbb{Z}^{n_t}) \le e^{n_t/2} \prod_{i=t}^n \left(1 + \frac{\sqrt{8\pi}\,\lambda_1}{\sqrt{n_t}\, r_{i,i}}\right). \qquad \square$$

Now $r_{i,i}^2 = \|\mathbf{b}_1\|^2 q^{i-1}$, $\lambda_1^2/(\gamma_n\, rd(\mathcal{L})^2) = (\det\, \mathcal{L})^{\frac{2}{n}} = \|\mathbf{b}_1\|^2 q^{\frac{n-1}{2}}$ hold by GSA and thus $\gamma_n \geq \frac{n}{2\,e\pi}$ directly imply for $i = t, ..., n$

$$\sqrt{n-t+1}\, r_{i,i} \leq \sqrt{2e\pi}\, rd(\mathcal{L})^{-1}\lambda_1\, q^{(2i-n-1)/4}.$$

By Lemma 4.2 $\quad \mathcal{M}_t \leq \prod_{i=t}^{n} \frac{e\sqrt{\pi}\, rd(\mathcal{L})^{-1}\,\lambda_1\, q^{(2i-n-1)/4} + \sqrt{8e\pi}\,\lambda_1}{\sqrt{n-t+1}\, r_{i,i}}$.

For $\bar{\eta} := 2 + \sqrt{e}$, $t := \frac{n}{2} + 1 - c$,
$m(q,c) := [\texttt{if } c > 0 \texttt{ then } q^{\frac{1-c^2}{4}} \texttt{ else } 1]$ we get

$$\mathcal{M}_t \leq m(q,c)\Big(\frac{\bar{\eta}\sqrt{2e\pi}\,\lambda_1}{\sqrt{n-t+1}\, rd(\mathcal{L})}\Big)^{n-t+1} / \det \pi_t(\mathcal{L}), \qquad (4.1)$$

because $m(q,c) = q^{\frac{1-c^2}{4}} = q^{-\sum_{i=0}^{c}(2i-1)/4)} \geq \prod_{i=t}^{n/2+1} \frac{\sqrt{n-t+1}\, r_{i,i}}{\bar{\eta}\sqrt{2e\pi}\,\lambda_1}$
for $c > 0$. We see from (4.1) and
$\det \pi_t(\mathcal{L}) = \|\mathbf{b}_1\|^{n-t+1} q^{\sum_{i=t-1}^{n-1} i/2}$ that

$$\mathcal{M}_t \leq m(q,c)\Big(\frac{\bar{\eta}\sqrt{2e\pi}\,\lambda_1}{\sqrt{n-t+1}\, rd(\mathcal{L})\,\|\mathbf{b}_1\|}\Big)^{n-t+1} / q^{\sum_{i=t-1}^{n-1} i/2} \qquad (4.2)$$

Now $\gamma_n \le \frac{1.744\,(n+o(n))}{2e\pi}$ [KL78] implies via GSA

$$\frac{e\pi\,\lambda_1^2}{n\,rd(\mathcal{L})^2 \|\mathbf{b}_1\|^2} \le q^{\frac{n-1}{2}} \quad \text{for } n \ge n_0. \tag{4.3}$$

(4.2), (4.3), $\frac{1}{n-1}\sum_{i=t-1}^{n-1} i = \frac{n}{2} - \frac{(t-1)(t-2)}{2(n-1)}$ yield

$$\mathcal{M}_t \le m(q,c)\Big(\frac{\bar\eta\,\sqrt{2e\pi}\,\lambda_1}{\sqrt{n-t+1}\,rd(\mathcal{L})\,\|\mathbf{b}_1\|}\Big)^{n-t+1}\Big(\frac{\sqrt{n}\,rd(\mathcal{L})\,\|\mathbf{b}_1\|}{\sqrt{e\pi}\,\lambda_1}\Big)^{n-\frac{(t-1)(t-2)}{n-1}}.$$

The difference of the exponents

$$\mathbf{de}(t) = n - \frac{(t-1)(t-2)}{n-1} - n + t - 1 = (t-1)(1 - \frac{t-2}{n-1})$$

is positive for $t \le n$ and maximal for $t_{max} = \frac{n}{2} + 1$,

$\mathbf{de}(\frac{n}{2} + 1 - c) = \frac{n+1}{4} + \frac{1/4 - c^2}{n-1}$. We get for $\|\mathbf{b}_1\| \le \sqrt{2e\pi}\, n^b\, \lambda_1$,

$t = \frac{n}{2} + 1 - c:\quad \mathcal{M}_t \le m(q,c)\,\big(O(n^{\frac{1}{2}+b} rd(\mathcal{L}))\big)^{\frac{n+1}{4} + \frac{1/4-c^2}{n-1}}.$

Hence $\qquad \mathcal{M}_t = (O(n^{\frac{1}{2}+2b} rd(\mathcal{L})\,)^{\frac{n+1}{4}}.$ $\qquad\square$

Main open problem

Can the factoring algorithm be improved by the method of the number field sieve ?

We factor N via easy CVP-solutions that correspond to multiplicative relations $\mod N$, related to the quadratic sieve. The last coordinate of an CVP-solution yields a multiplicative relation of the factor base, under the natural logarithm ln.

How to incorporate $\mod N$ reductions under the ln transform ?

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 STOC, ACM, 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.

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.

CS93 *J.H. Conway and N.J.A. Sloane*, Sphere Packings, Lattices and Groups. third edition, Springer-Verlag1998.

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.

HHHW09 *P.Hirschhorn, J. Hoffstein, N. Howgrave-Graham, W. Whyte*, Choosing NTRUEncrypt parameters in light of combined lattice reduction and MITM approaches. In Proc. ACNS 2009, LNCS 5536, Springer-Verlag,pp. 437–455, 2009.

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

H07 *N. Howgrave-Graham*, A hybrid lattice–reduction and meet-in-the-middle attiack against NTRU. In Proc, CRYPTO 2007, LNCS 4622, Springer-Verlag, pp. 150–169, 2007.

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

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.

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

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.

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

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,pp. 281–293, 1991. //www.mi.informatik.uni-frankfurt.de.

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.

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, pp. 1–12, 1995.

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, pp. 146–156, 2003.

S06 *C.P. Schnorr*, Fast LLL-type lattice reduction. Information and Computation, **204**, pp. 1–25, 2006.

S07 *C.P. Schnorr*, Progress on LLL and lattice reduction, Proceedings LLL+25, Caen, France, June 29–July 1, 2007, Final version to appear;