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 \( B = [b_1, \ldots, b_n] \in \mathbb{Z}^{m \times n} \)
lattice \( \mathcal{L}(B) = \{ Bx \mid x \in \mathbb{Z}^n \} \)norm \( \| x \| = \langle x, x \rangle = (\sum_{i=1}^{m} x_1^i)^{1/2} \)
SV-length \( \lambda_1(\mathcal{L}) = \min\{ \| b \| \mid b \in \mathcal{L} \setminus \{0\} \} \)
Successive minima \( \lambda_1, \ldots, \lambda_n \)

**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 \( i = 1, \ldots, n-1 \).
Average time fast SVP algorithm

**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 \( \gamma_n = \max\{\lambda_1^2/\det(\mathcal{L})^{2/n} | \dim \mathcal{L} = n\} \).

We always have \( \|b_1\|^2 = rd(\mathcal{L})^2 \gamma_n (\det \mathcal{L})^{2/n} \).

**Theorem 4.1 (GSA).** Given a lattice basis such that

\[
\|b_1\| \leq \sqrt{2e\pi} n^b \lambda_1, \ b \geq 0, \ NEW\ ENUM\ solves\ SVP\ in\ time
\]

\[
n^{O(1)} + (O(n^{2b-\varepsilon}))^{\frac{n+1}{4}} \quad \text{if } rd(\mathcal{L}) = n^{-\frac{1}{2}-\varepsilon}, \ \varepsilon > 0.
\]

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

**GSA :** Let \( B = QR = Q[r_{i,j}] \) satisfy (for \( r_{i,j} = \|b_i^*\| \)):

\[
r_{i,i}^2/r_{i-1,i-1}^2 = q \quad \text{for } i = 2, \ldots, n \text{ and some } q > 0.
\]

W.l.o.g. let \( q < 1 \), otherwise \( \|b_1\| = \lambda_1 \).

We outline the proof of Thm 4.1 in part III.
Corollary 6.1 (GSA). Given \( b_1 \in \mathcal{L}, \ 0 \neq \|b_1\| = O(\lambda_1) \), \textsc{New Enum} finds \( b \in \mathcal{L} \) such that \( \|b - t\| = \|\mathcal{L} - t\| \) in time
\[
 n^{O(1)} + O(\sqrt{n} \text{rd}(\mathcal{L}) \|\mathcal{L} - t\|^2 \lambda_1^{-2})^{\frac{n+1}{4}}.
\]

This time bound is polynomial if
\[
\|\mathcal{L} - t\| = O(\lambda_1) \text{ and } \text{rd}(\mathcal{L}) \leq n^{-\frac{1}{2} - \varepsilon} \text{ for } \varepsilon > 0.
\]

The required short vector \( b_1 \) can in practice be added to the basis, extending the lattice by a short vector preserving \( \text{rd}(\mathcal{L}) \).

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 $B = [b_1, \ldots, b_n] \in \mathbb{R}^{(n+1)\times n}$:

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

and the target vector $N \in \mathbb{R}^{n+1}$, where either $N' = N$ or $N' = Np_{n+j}$ for one of the next $n$ primes $p_{n+j} > p_n$, $j \leq n$.

W.l.o.g. let $N' = N$ for the analysis.
Outline of the factoring method

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
\[
u = \prod_{e_j > 0} p_j^{e_j}, \quad v = \prod_{e_j < 0} p_j^{-e_j} \in \mathbb{N}.
\]
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 \( N \) 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
\[
\prod_{i=0}^{n} p_i^{e_{i,j} - e'_{i,j}} = 1 \mod N
\]
for \( j = 1, \ldots, n + 1 \). Any non trivial solution \( z_1, \ldots, z_{n+1} \in \mathbb{Z} \) of the equations
\[
\sum_{j=1}^{n+1} z_j (e_{i,j} - e'_{i,j}) = 0 \mod 2 \text{ for } i = 0, \ldots, n
\]
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 $|u - vN'| = o(N^c)$, $v = \Theta(N^{c-1})$, $e_1, \ldots, e_n \in \{0 \pm 1\}$ then $\|b - N\|^2 = (2c - 1) \ln N + \ln(p_{n+j}) + \Theta(|u - vN'|^2(N/N')^2)$.

Proof. We see from $e_1, \ldots, e_n \in \{0 \pm 1\}$ that

$\|b - N\|^2 = \ln u + \ln v + N^{2c}|\ln \frac{u}{vN'}|^2.$

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

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

Combining these equations proves the claim. \hfill \square

Theorem 7.2 $\|b - N\|^2 \leq (2c - 1) \ln N + 2\delta \ln p_n$ implies

$|u - vN'| \leq p_n^{\frac{1}{\alpha} + \delta + o(1)}.$
An integer $z$ is called $y$-smooth, if all prime factors $p$ of $z$ satisfy $p \leq y$. Let $N'$ be either $N$ or $Np_{n+j}$ for one of the next $n$ primes $p_{n+j} > p_n$. We denote

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

**Theorem 7.4 [S93]** If the equation $|u - \lceil u/N \rceil N| = 1$ is for random $u$ of order $N^c$ nearly statistically independent from the event that $u, \lceil u/N \rceil$ 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 $b = \sum_{i=1}^{n} e_i b_i \in \mathcal{L}(B)$ closest to $N$ 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 $\|\mathcal{L}(B) - N\|$ in polynomial time under GSA given $b \in \mathcal{L}(B)$ such that $0 \neq \|b\| = O(\lambda_1)$.

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

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

Lemma 5.3 of [MG02] proves that $\lambda_2^2 \geq 2c \ln N - \Theta(1)$

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

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

$$= O(c \ln N)^{(1-\alpha)/2} = O((\ln N)^{1-\alpha}).$$

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

$$n^{-\frac{1}{2}-\varepsilon} = n^{-1+1/\alpha} \approx (\alpha \ln \ln N)^{1-1/\alpha} (\ln N)^{1-\alpha} > rd(\mathcal{L}).$$
Providing a nearly shortest vector of $\mathcal{L}(B)$

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 $\| \sum_i e_i b_i - b_{n+1} \|^2 = 2c \ln N + O(1)$ holds for $u = \prod_i p_i^{e_i}$ the additional basis vector $b_{n+1}$ corresponding to $\bar{p}_{n+1}$. $\sum_i e_i b_i - b_{n+1}$ is a nearly shortest vector of $\mathcal{L}(b_1, ..., b_{n+1})$.

**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 $b_{n+1}$ 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 $\pi_t : \text{span}(b_1, ..., b_n) \to \text{span}(b_1, ..., b_{t-1})^\perp$ for $t = 1, ..., n$ denote the orthogonal projections and let $L_t = L(b_1, ..., b_{t-1})$.

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

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

where $\zeta_t := b - \pi_t(b) = Qv_t \in \text{span} L_t$ is the orthogonal projection in $\text{span} L_t$ of the given $b = \sum_{i=t}^n u_i b_i$ and $v_t = (v_1, ..., v_{t-1}, 0^{n-t+1})^t$ for $v_i = \sum_{i=t}^n r_{i,j} u_j$. Stage $(u_t, ..., u_n)$ exhaustively enumerates $B_{t-1}(\zeta_t, \rho_t) \cap L_t$, the intersection of the lattice $L_t$ and the sphere $B_{t-1}(\zeta_t, \rho_t) \subset \text{span} L_t$ of dimension $t - 1$ with radius $\rho_t := (A - \| \pi_t(b) \|^2)^{1/2}$ and center $\zeta_t$. 

III: A novel enumeration of short lattice vectors 12
The success rate $\beta_t$ of stages

The **GAUSSIAN** volume heuristics estimates $|B_{t-1}(\zeta_t, \rho_t) \cap L_t|$ for $t > 1$ to

$$\beta_t = \text{def} \ \frac{\text{vol } B_{t-1}(\zeta_t, \rho_t)}{\det L_t}.$$ 

Here $\text{vol } B_{t-1}(\zeta_t, \rho_t) = V_{t-1}\rho_t^{t-1}$, $V_{t-1} = \pi^{\frac{t-1}{2}}/\left(\frac{t-1}{2}\right)!$ is the volume of the unit sphere of dimension $t - 1$, $\det L_t = \prod_{i=1}^{t-1} r_{i,i}$, $\rho_t^2 := A - \|\pi_t(\sum_{i=t}^n u_i b_i)\|^2$. We call $\beta_t$ the **success rate** of stage $(u_t, \ldots, u_n)$.

If $\zeta_t \mod L_t$ is uniformly distributed over

$$\left\{\sum_{i=1}^{t-1} r_i b_i \mid 0 \leq r_1, \ldots, r_{t-1} < 1\right\}$$

then $E_{\zeta_t}[|B_{t-1}(\zeta_t, \rho_t) \cap L_t|] = \beta_t$, where $E_{\zeta_t}$ refers to a random $\zeta_t \mod L_t$. This holds because $1/\det L_t$ is the number of lattice points of $L_t$ per volume in $\text{span } L_t$. The formal analysis of **NEW ENUM** by Theorem 4.1 uses a proven version of the volume heuristics without assuming that $\zeta_t \mod L_t$ 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 $b \in \mathcal{L}(B)$ of decreasing length $\|b\|^2 \leq A$ terminating with $\|b\| = \lambda_1$.

1. $s := 1$, $L_s := \emptyset$, (we call $s$ the level)

2. *Perform algorithm ENUM [SE94] pruned to stages with $\beta_t \geq 2^{-s}$*: Upon entry of stage $(u_t, ..., u_n)$ compute $\beta_t$. 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 $\beta_t \geq 2^{-s}$ perform stage $(u_t, ..., u_n)$ on level $s$, and as soon as some non-zero $b \in \mathcal{L}$ of length $\|b\|^2 \leq A$ has been found give out $b$ and set $A := \|b\|^2 - 1$.

3. $L_{s+1} := \emptyset$, perform the stages $(u_t, ..., u_n)$ of $L_s$ with $\beta_t \geq 2^{-s-1}$ in increasing order of $t$ and for fixed $t$ in order of decreasing $\beta_t$. Collect the appearing substages $(u_{t'}, ..., u_t, ..., u_n)$ with $\beta_{t'} < 2^{-s-1}$ in $L_{s+1}$.

4. IF $L_{s+1} \neq \emptyset$ THEN [ $s := s + 1$, GO TO 3 ]
ELSE  terminate by exhaustion.
Proof of Theorem 4.1

**Thm 4.1** NEW ENUM solves SVP in time \( n^{O(1)} + (O(n^{2b-\epsilon}))^{\frac{n+1}{4}} \) if \( rd(\mathcal{L}) = n^{-\frac{1}{2}} - \epsilon, \epsilon > 0 \) and if \( b_1 \| \leq \sqrt{2e\pi} n^b \).

NEW ENUM essentially performs stages in decreasing order of the success rate \( \beta_t \). Let \( b' = \sum_{i=1}^{n} u_i' b_i \in \mathcal{L} \) denote the unique vector of length \( \lambda_1 \) that is found by NEW ENUM.

Let \( \beta'_t \) 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 \( \rho_t^2 = A - \| \pi_t(b) \|^2 \) and \( \rho'_t^2 = A - \| \pi_t(b') \|^2 \).

Without using the simplifying assumption, the proven time bound of Theorem 4.1 increases at most by the factor 2.
Consider the number $M_t$ of stages $(u_t, \ldots, u_n)$ with 
$\|\pi_t(\sum_{i=t}^n u_i b_i)\| \leq \lambda_1:
M_t := \#(B_{n-t+1}(0, \lambda_1) \cap \pi_t(L)).$
Modulo the heuristic simplifications $M_t$ covers the stages that
precede $(u'_t, \ldots, u'_n)$ and those that finally prove $\|b'\| = \lambda_1$.

**Lemma 4.2** $M_t \leq e^{\frac{n-t+1}{2}} \prod_{i=t}^n (1 + \frac{\sqrt{8\pi \lambda_1}}{\sqrt{n-t+1} r_{i,i}})$.

**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
\[ E_t = \{(x_t, \ldots, x_n)^t \in \mathbb{R}^{nt} \mid \|\pi_t(\sum_{i=t}^n x_i b_i)\|^2 \leq \lambda_1^2\}, \]
where 
\[ \|\pi_t(\sum_{i=t}^n x_i b_i)\|^2 = \sum_{i=t}^n \sum_{j=i}^n (r_{i,j} x_j)^2 = \sum_{i=t}^n \sum_{j=i}^n (\mu_{j,i} x_j)^2 \|b_i^*\|^2. \]
By definition $M_t \leq \#(E_t \cap \mathbb{Z}^{nt})$. We set
\[ \sum_i x := \sum_{j > i} \frac{r_{i,j}}{r_{i,i}} x_j \quad \text{and} \quad x'_i := x_i + \lceil \sum_i x \rceil, \]
\[ \{ \sum_i x \} := \sum_i x - \lceil \sum_i x \rceil, \]
\[ F_t := \{(x'_t, \ldots, x'_n)^t \in \mathbb{R}^{nt} \mid \sum_{i=t}^n (x'_i + \{ \sum_i x \})^2 r_{i,i}^2 \leq \lambda_1^2\}. \]
Claim \( \#(E_t \cap \mathbb{Z}^{nt}) \leq \#(F_t \cap \mathbb{Z}^{nt}) \)

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

We simplify \(E_t\) to \(E'_t = \{x' \in \mathbb{R}^n_t \mid \sum_{i=t}^n x'_i r^2_{i,i} \leq 4\lambda_1^2\}\).

Since \(\{|\sum_j x|\} \leq \frac{1}{2}, x_i \in \mathbb{Z}\) and \(|x_i + \varepsilon|^2 \geq x_i^2/4\) for \(|\varepsilon| \leq \frac{1}{2}\) we see that \(F_t \cap \mathbb{Z}^{nt} \subset E'_t \cap \mathbb{Z}^{nt}\). Hence \(M_t \leq \#(E'_t \cap \mathbb{Z}^{nt})\).

We bound \(\#(E'_t \cap \mathbb{Z}^{nt})\) using the method of [MO90, Lemma 1]. Denoting \(N_r := \#\{(k_t, \ldots, k_n)^{t} \in \mathbb{Z}^{nt} \mid \sum_{i=t}^n r^2_{i,i} k^2_i = r\}\) we have

\[
\#(E'_t \cap \mathbb{Z}^{nt}) = \sum_{0 \leq r \leq 4\lambda_1^2} N_r e^{s(4\lambda_1^2 - r)n_t} \leq e^{s4\lambda_1^2 n_t} \sum_{r \geq 0} N_r e^{-sr n_t}
\]

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

since \(\sum_{k \in \mathbb{Z}} e^{-Tk^2} = 1 + 2 \sum_{k=1}^{\infty} e^{-Tk^2} \leq 1 + 2 \int_{0}^{\infty} e^{-Tx^2} dx = 1 + \sqrt{\pi/\overline{T}}\). We get for \(s := 1/(8\lambda_1^2)\) :

\[
\#(E'_t \cap \mathbb{Z}^{nt}) \leq e^{n_t/2} \prod_{i=t}^n (1 + \frac{\sqrt{8\pi \lambda_1}}{\sqrt{n_t r_{i,i}}} ).
\]

\(\square\)
Now \( r_{i,i}^2 = \|b_1\|^2 q^{i-1} \), \( \lambda_1^2/(\gamma_n rd(L)^2) = (\det L)^{\frac{2}{n}} = \|b_1\|^2 q^{\frac{n-1}{2}} \)
hold by GSA and thus \( \gamma_n \geq \frac{n}{2e\pi} \) directly imply for \( i = t, \ldots, n \)
\[
\sqrt{n-t+1} r_{i,i} \leq \sqrt{2e\pi} rd(L)^{-1} \lambda_1 q^{(2i-n-1)/4}.
\]
By Lemma 4.2
\[
\mathcal{M}_t \leq \prod_{i=t}^n \frac{e^{e\pi rd(L)^{-1} \lambda_1 q^{(2i-n-1)/4}}} {\sqrt{n-t+1} r_{i,i}}.
\]
For \( \bar{\eta} := 2 + \sqrt{e}, \ t := \frac{n}{2} + 1 - c \),
\[
m(q, c) := [\text{if } c > 0 \text{ then } q^{\frac{1-c^2}{4}} \text{ else } 1] \text{ we get}
\]
\[
\mathcal{M}_t \leq m(q, c) \left( \frac{\bar{\eta}\sqrt{2e\pi} \lambda_1}{\sqrt{n-t+1} rd(L)} \right)^{n-t+1} / \det \pi_t(L), \tag{4.1}
\]
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
\[
\det \pi_t(L) = \|b_1\|^{n-t+1} q^{\sum_{i=t-1}^{n-1} \frac{i}{2}} \text{ that}
\]
\[
\mathcal{M}_t \leq m(q, c) \left( \frac{\bar{\eta}\sqrt{2e\pi} \lambda_1}{\sqrt{n-t+1} rd(L) \|b_1\|} \right)^{n-t+1} / q^{\sum_{i=t-1}^{n-1} \frac{i}{2}} \tag{4.2}
\]
Now $\gamma_n \leq \frac{1.744(n+o(n))}{2e\pi}$ [KL78] implies via GSA
\[ e^\pi \lambda_1^2 \frac{n^{rd(\mathcal{L})^2\|b_1\|^2}}{n \leq q^{\frac{n-1}{2}}} \text{ for } n \geq n_0. \tag{4.3} \]

(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
\[ M_t \leq m(q, c) \left( \frac{\sqrt{2e\pi} \lambda_1}{\sqrt{n-t+1} \ n \ rd(\mathcal{L}) \ ||b_1||} \right)^{n-t+1} \left( \frac{\sqrt{n \ rd(\mathcal{L}) \ ||b_1||}}{\sqrt{e\pi} \ \lambda_1} \right)^{n-\frac{(t-1)(t-2)}{n-1}}. \]

The difference of the exponents
\[ \text{de}(t) = n - \frac{(t-1)(t-2)}{n-1} - n + t - 1 = (t - 1)(1 - \frac{t-2}{n-1}) \]
is positive for $t \leq n$ and maximal for $t_{\text{max}} = \frac{n}{2} + 1$,
\[ \text{de} \left( \frac{n}{2} + 1 - c \right) = \frac{n+1}{4} + \frac{1/4-c^2}{n-1}. \]
We get for $\|b_1\| \leq \sqrt{2e\pi} n^b \lambda_1$,
\[ t = \frac{n}{2} + 1 - c : \ M_t \leq m(q, c) \left( O(n^{1+b \ rd(\mathcal{L})}) \right)^{\frac{n+1}{4} + \frac{1/4-c^2}{n-1}}. \]
Hence
\[ M_t = \left( O(n^{1+2b \ rd(\mathcal{L})}) \right)^{\frac{n+1}{4}}. \]
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?


References


Refences


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