Average Time Fast SVP and CVP Algorithms for Low Density Lattices and the Factorization of Integers

Claus P. SCHNORR

Fachbereich Informatik und Mathematik
Goethe-Universität
Frankfurt am Main

B-IT Bonn, 27-29.5. 2010

60 Birthday of Joachim von zur Gathen

Road map

I Outline of the new **SVP** / **CVP** algorithm

II Time bound of **SVP**/**CVP** algorithm for low density lattices

III Factoring integers via "easy" **CVP** solutions

IV Partial analysis of the new **SVP** / **CVP** algorithm

References

There is a TR available at
http://www.mi.informatik.uni-frankfurt.de/research/papers.html

We focus on novel proof elements that are not covered by published work and outline sensible heuristics towards polynomial time factoring of integers.

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

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

- the **GNF** — geom. normal form — $\mathbf{R} = [r_{i,j}] \in \mathbb{R}^{n \times n}$ is uppertriangular, $r_{i,j} = 0$ for $j < i$ and $r_{i,i} > 0$, $\quad (r_{i,i} = \|\mathbf{b}_i^*\|)$
- $\mathbf{Q} \in \mathbb{R}^{m \times n}$ **isometric**: $\mathbf{Q}^t\mathbf{Q} = \mathbf{I}_n$.

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

1. $|r_{i,j}| \le \frac{1}{2} r_{i,i}$ for all $j > i$ (**size-reduced**) $\quad (r_{i,j}/r_{i,i} = \mu_{j,i})$
2. $\delta\, r_{i,i}^2 \le r_{i,i+1}^2 + r_{i+1,i+1}^2$ for $i = 1, \dots, n-1$.
3. $\alpha^{-i+1} \le \|\mathbf{b}_i\|^2 \lambda_i^{-2} \le \alpha^{n-1}$ for $i = 1, ..., n$,
4. $\|\mathbf{b}_1\|^2 \le \alpha^{\frac{n-1}{2}} (\det \mathcal{L})^{2/n}$, where $\alpha = 1/(\delta - \frac{1}{4})$.

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

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 some $A \geq \lambda_1^2$. Obviously

$$\underbrace{\| \sum_{i=1}^n u_i \mathbf{b}_i \|^2}_{\text{goal: } \leq A} = \underbrace{\|\zeta_t + \sum_{i=1}^{t-1} u_i \mathbf{b}_i \|^2}_{\text{to be minimized}} + \underbrace{\|\pi_t(\mathbf{b})\|^2}_{\text{spent}},$$

where $\zeta_t := \mathbf{b} - \pi_t(\mathbf{b}) \in \mathrm{span}\, \mathcal{L}_t$ is the orthogonal projection of the given $\mathbf{b} = \sum_{i=t}^n u_i \mathbf{b}_i$.

Stage $(u_t, ..., u_n)$ exhausts $\mathcal{B}_{t-1}(\zeta_t, \rho_t) \cap \mathcal{L}_t$ where $\mathcal{B}_{t-1}(\zeta_t, \rho_t) \subset \mathrm{span}\, \mathcal{L}_t$ is the sphere of dimension $t-1$ with center ζ_t and radius $\rho_t := (A - \|\pi_t(\mathbf{b})\|^2)^{1/2}$.

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

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

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

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

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

If ζ_t mod $\mathcal{L}_t$ is uniformly distributed over the parallelepiped

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

then $\mathrm{E}_{\zeta_t}[\, |\mathcal{B}_{t-1}(\zeta_t, \rho_t) \cap \mathcal{L}_t| \,] = \beta_t$ for $\zeta_t \in_R \mathcal{P}_t$, because $1/\det \mathcal{L}_t$ is the number of points of $\mathcal{L}_t$ per volume.

The center $\zeta_t = \mathbf{b} - \pi_t(\mathbf{b}) \in \mathrm{span}\, \mathcal{L}_t$ changes rapidly within NEW ENUM. It is natural to assume that $\zeta_t \in \mathrm{span}(\mathcal{L}_t)$ distributes nearly randomly, and thus the estimate $|\mathcal{B}_{t-1}(\zeta_t, \rho_t) \cap \mathcal{L}_t| \approx \mathrm{vol}\, \mathcal{B}_{t-1}(\zeta_t, \rho_t) / \det \mathcal{L}_t$ of the vol. heur. holds on the average.

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

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

We efficiently approximate β_t using floating point arithmetic.

The space reservations for the list L are quite expensive compared to the modest arithmetic costs per stage.

The condition $\beta_t < n^{-s}$ has been tested in practice. It replaces our original condition $\beta_t < 2^{-s}$. This reduces the list L and the number of list operations.

For the final exhaustive search that proves $\|\mathbf{b}\| = \lambda_1$ the success rate and the list operations can be suppressed, they merely slows down the computation.

The start of the final exhaustion can be guessed: if no shorter vector comes up for an extended period then most likely the last output $\mathbf{b}$ has length λ_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 $\mathcal{L}'$ of $\dim \mathcal{L}' = n$ 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 $\lambda_1^2 = rd(\mathcal{L})^2 \gamma_n (\det \mathcal{L})^{2/n}$.

Theorem 1 Given a lattice basis satisfying **GSA** and $\|\mathbf{b}_1\| \leq \sqrt{e\pi}\, n^b \lambda_1$, $b \geq 0$, NEW ENUM solves **SVP** in time $2^{O(n)} (n^{1/2+b} rd(\mathcal{L}))^{n/4}$. In particular in time $2^{O(n)} n^{n/8}$ for $b = 0$.

The $2^{O(n)}$ factor disappears under the volume heuristics.

GSA : Let $\mathbf{B} = \mathbf{QR} = \mathbf{Q}[r_{i,j}]$ 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 $\|\mathbf{b}_1\| = \lambda_1$.
The condition $\|\mathbf{b}_1\| \leq \sqrt{e\pi}\, n^b \lambda_1$ can "easily" be met for **CVP**.

Finding an unproved shortest vector $\mathbf{b}'$ is easier than proving $\|\mathbf{b}'\| = \lambda_1$. We study the time to find an **SVP**-solution $\mathbf{b}'$ without proving $\lambda_1 = \|\mathbf{b}'\|$ under the assumption:

SA $\|\pi_t(\mathbf{b}')\|^2 \approx \frac{n-t+1}{n}\lambda_1^2$ holds for all t and New Enum's **SVP**-solution $\mathbf{b}'$, where $\pi_t(\mathbf{b}') \in \mathrm{span}(\mathbf{b}_1, ..., \mathbf{b}_{t-1})^\perp$.

Proposition 1. Let a lattice basis be given that satisfies **GSA**, $\|\mathbf{b}_1\| \leq \sqrt{e\pi/2}\, n^b \lambda_1$ and $rd(\mathcal{L}) \leq n^{-\frac{1+2b}{4}}$. If New Enum finds a shortest lattice vector $\mathbf{b}'$ satisfying **SA** it finds $\mathbf{b}'$, without proving $\|\mathbf{b}'\| = \lambda_1$, under the vol. heuristics in polynomial time.

Polynomial time holds for $b = 0$, $rd(\mathcal{L}) \leq n^{-1/4}$. But the time to prove $\|\mathbf{b}'\| = \lambda_1$ is under the vol. heuristics $\Theta(n^{\frac{1}{2}} rd(\mathcal{L}))^{n/4}$.

Corollary 1. Given $\mathbf{t} \in \mathbb{R}^n$ and B of $\mathcal{L}(B)$ satisfying **GSA**, if $\|\mathbf{b}_1\| = \lambda_1$ and $rd(\mathcal{L}) \leq n^{-1/2}$ then NEW ENUM solves the **CVP** $\|\mathbf{t} - \mathbf{b}\| = \|\mathbf{t} - \mathcal{L}\|$ under the volume heuristics in poly-time.

A random center $\zeta = \pi_t(\mathbf{t})$ of $\mathcal{B}_n(\zeta, \rho)$ provides a good basis for the volume heuristics, much better than for solving SVP where the center $\zeta = \mathbf{0}$ nearly maximizes $|\mathcal{B}_n(\zeta, \rho) \cap \mathcal{L}|$.

We adjust the assumption **SA** from **SVP** to **CVP**:

CA Let $\|\pi_t(\mathbf{t} - \ddot{\mathbf{b}})\|^2 \approx \frac{n-t+1}{n} \|\mathbf{t} - \mathcal{L}\|^2$ hold for all t and NEW ENUM's **CVP**-solution $\ddot{\mathbf{b}}$.

Corollary 2. Let $B = [\mathbf{b}_1, ..., \mathbf{b}_n]$ in $\mathbb{Z}^{m \times n}$ satisfy **GSA**, $\|\mathbf{b}_1\| = O(\lambda_1)$ and let $\ddot{\mathbf{b}}$ satisfy **CA** for $B, \mathbf{t}$. If $rd(\mathcal{L}) = o(n^{-1/4})$ and $\|\mathbf{t} - \mathcal{L}\| = O(\lambda_1)$ then NEW ENUM finds the **CVP**-solution $\ddot{\mathbf{b}} \in \mathcal{L}$ under the volume heuristics in polynomial time, but without proving $\|\mathbf{t} - \ddot{\mathbf{b}}\| = \|\mathbf{t} - \mathcal{L}\|$.

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

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

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

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

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

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

Lemma 5.3 [MG02] $\lambda_1^2 \geq 2c \ln N$.

$rd(\mathcal{L}) = o(n^{-1/4})$ for $c = (\ln N)^\beta$, some $\alpha > 2\beta + 2, \beta > 0$.

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

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

We compute vectors $\mathbf{b} = \sum_{i=1}^{n} e_i \mathbf{b}_i \in \mathcal{L}(\mathbf{B})$ close to $\mathbf{N}$ such that $|u - vN'| < p_n$. The prime factorizations $|u - vN'| = \prod_{i=1}^{n} p_i^{e_i'}$ and $u = \prod_{e_j > 0} p_j^{e_j}$ yield for "suitable" α, c 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 $j = 1, ..., n+1$. Any non-trivial solution $z_1, ..., z_{n+1} \in \mathbb{Z}$ of

$$\sum_{j=1}^{n+1} z_j (e_{i,j} - e'_{i,j}) = 0 \mod 2, \quad i = 0, ..., n$$

solves $X^2 = 1 \mod N$ by $X = \prod_{i=0}^{n} p_i^{\frac{1}{2} \sum_{j=1}^{n+1} z_j (e_{i,j} - e'_{i,j})} \mod N$.
Hence $\gcd(X \pm 1, N)$ factors N if $X \neq \pm 1 \mod N$.

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

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

Theorem 4 [S93/91] 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 $M_{\alpha,c,N} \neq \emptyset$ holds if $\frac{\alpha}{\alpha - 2\beta - 2} < c \leq (\ln N)^\beta$ and $\alpha > 2\beta + 2$.

Theorem 4 extends the result of [S93/91] from a constant $c > 0$ to $c = (\ln N)^\beta$, required for $rd(\mathcal{L}) = o(n^{1/4})$.

Theorem 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 6 If $\|\mathbf{b}_1\| = O(\lambda_1)$ and $M_{\alpha,c,N} \neq \emptyset$ for $c = (\ln N)^\beta$, $\alpha > 2\beta + 2$ we can minimize $\|\mathcal{L}(B) - \mathbf{N}\|$ under **GSA, CA** and the volume heuristics in polynomial time.

Proof. 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 $\lambda_1^2 \geq 2c\ln N - \Theta(1)$

[$\lambda_1^2 = 2c\ln N + O(1)$ holds if $0 < \frac{\alpha}{\alpha-2\beta-2} < c \leq (\ln N)^\beta$.]

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

We have for $c = (\ln N)^\beta$, $\alpha > 2\beta + 2$ that $\frac{2c\ln N}{(\ln n)^\alpha} = o(n^{-1/2})$

Hence $rd(\mathcal{L}) = o(n^{-1/4})$. $\square$

For solving $\|\mathbf{t} - \ddot{\mathbf{b}}\| = \|\mathbf{t} - \mathcal{L}\|$ heur. in poly-time Theorem 6 requires some $\|\mathbf{b}_1\| = O(\lambda_1)$.

We extend the prime number basis $\mathbf{B}$ and $\mathcal{L}(\mathbf{B})$ by a nearly shortest lattice vector for 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 $u = \prod_i p_i^{e_i}$ and 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 random $u = \prod_i p_i$ and test the nearby $\bar{p}$ for primality. $\bar{p}_{n+1}$ and $\mathbf{b}_{n+1}$ can be found in probabilistic polynomial time if the density of primes near the u is not exceptionally small. A single $\bar{p}_{n+1}$ can be used to solve all **CVP**'s for the factorization of all integers of order $\Theta(N)$.

Theorem 1 Given a lattice basis satisfying **GSA** and $\|\mathbf{b}_1\| \leq \sqrt{e\pi}\, n^b \lambda_1$, $b \geq 0$, NEW ENUM solves **SVP** in time

$$2^{O(n)}(n^{1/2+b} rd(\mathcal{L}))^{n/4}.$$

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 $\beta_t \leq \frac{1}{n}\beta_t'$

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 n.

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

The proof uses the method of Lemma 1 of MAZO, ODLYZKO [MO90] and follows the adjusted proof of inequality (2) in section 4.1 of HANROT, STEHLÉ [HS07].

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 $\gamma_n \ge \frac{n}{2\,e\pi}$ directly imply for $i = t, ..., n$

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

By Lemma 1 $\quad \mathcal{M}_t \le \prod_{i=t}^n \frac{e\sqrt{\pi}\, rd(\mathcal{L})^{-1}\, \lambda_1\, q^{(2i-n-1)/4} + \sqrt{8e\pi}\,\lambda_1}{\sqrt{n-t+1}\, r_{i,i}} \qquad (4.0)$

For the remainder of the proof let $t := \frac{n}{2} + 1 - c$ and $m(q,c) := [\mathtt{if}\ c > 0\ \mathtt{then}\ q^{\frac{1-c^2}{4}}\ \mathtt{else}\ 1]$. Then

$$\mathcal{M}_t \leq m(q,c)\big(\tfrac{(2+\sqrt{e})\sqrt{2e\pi}\,\lambda_1}{\sqrt{n-t+1}\,rd(\mathcal{L})}\big)^{n-t+1} / \det \pi_t(\mathcal{L}), \tag{4.1}$$

where $m(q,c) = q^{\frac{1-c^2}{4}} = q^{-\frac{1}{4}\sum_{i=0}^{c}(2i-1)}$ covers in (4.0) the factors $q^{\frac{2i-n-1}{4}} > 1$ for $t < i < \frac{n}{2} + 1$.

We see from (4.1) and $\det \pi_t(\mathcal{L}) = \|\mathbf{b}_1\|^{n-t+1} q^{\sum_{i=t}^{n} \frac{i-1}{2}}$ that

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

The [KL78] bound $\gamma_n \leq \frac{1.744\,(n+o(n))}{2e\pi} \leq \frac{n}{e\pi}$ for $n \geq n_0$ and $\frac{1}{n-1}\sum_{i=t-1}^{n-1} i = \frac{n}{2} - \frac{(t-1)(t-2)}{2(n-1)}$ and $q^{\frac{n-1}{2}} = \lambda_1^2/(\|\mathbf{b}\|^2\gamma_n\, rd(\mathcal{L})^2)$ show

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

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

$$\mathcal{M}_t \le m(q,c)\big((\sqrt{8} + \sqrt{2e})\sqrt{\tfrac{n}{n-t+1}}\big)^{n-t+1} \left(n^{\frac{1}{2}+b} rd(\mathcal{L})\right)^{\frac{n^2/4-c^2}{n-1}}$$

For $c > 0$, $t \le \frac{n}{2}$ we have
$m(q,c) = q^{\frac{1-c^2}{4}} = \left(\frac{\|\mathbf{b}_1\| \sqrt{\gamma_n}\, rd(\mathcal{L})}{\lambda_1}\right)^{\frac{c^2-1}{n-1}} \le (n^{\frac{1}{2}+b} rd(\mathcal{L}))^{\frac{c^2-1}{n-1}}$, and

thus : $\quad \mathcal{M}_t \le (4 + 2\sqrt{e})^{n-t+1} \left(n^{\frac{1}{2}+b} rd(\mathcal{L})\right)^{\frac{n^2/4-1}{n-1}} =$
$2^{O(n)} \left(n^{\frac{1}{2}+b} rd(\mathcal{L})\right)^{\frac{n+1}{4}}$, where $\frac{n^2/4-1}{n-1} \le \frac{n+1}{4}$.
For $c \le 0$, $t > \frac{n}{2}$ we have

$$\mathcal{M}_t \le \big((\sqrt{8} + \sqrt{2e})\sqrt{\tfrac{n}{n-t+1}}\,\big)^{n-t+1} \left(n^{\frac{1}{2}+b} rd(\mathcal{L})\right)^{\frac{n^2/4}{n-1}}$$

$$= 2^{O(n)} \left(n^{\frac{1}{2}+b} rd(\mathcal{L})\right)^{\frac{n+2}{4}} \quad \text{where } \frac{n^2/4}{n-1} \le \frac{n+2}{4}. \qquad \square$$

MAZO, ODLYZKO [MO90] show for the lattice $\mathcal{L} = \mathbb{Z}^n$:

$$\#\{\mathbf{x} \in \mathbb{Z}^n \mid \|\mathbf{x}\|^2 \le an\} = 2^{\Theta(n)}$$

for $a_0 \le a \le \frac{1}{2e\pi}$ and any $a_0 > 0$,

whereas the vol. heuristics estimates this cardinality to $O(1)$.

The center $\zeta = \mathbf{0}$ of the sphere is bad for the vol. heur.:
It can nearly maximize $|\mathcal{B}_n(\zeta, \rho) \cap \mathcal{L}|$.

NEW ENUM for **SVP** tries to keep the center $\zeta_t = \mathbf{b} - \pi_t(\mathbf{b})$ $\in$span $\mathcal{L}_t$ close to $\mathbf{0} \in \mathbb{R}^{t-1}$. Can this in practice generate substantial errors of the volume heuristics?.
NEW ENUM for **CVP** keeps for center $\zeta_t = \mathbf{b} - \mathbf{t} - \pi_t(\mathbf{b} - \mathbf{t})$ close to $\pi_t(\mathbf{t})$. For random $\mathbf{t}$ this better justifies the volume heuristics in the analysis of NEW ENUM for **CVP**.

5.2 n^c-unique-SVP lattices: every lattice vector that is linearly independent of a shortest nonzero lattice vector has at least length $\lambda_1 n^c$ for some $c > 1$, i.e., $\lambda_2 \geq \lambda_1 n^c$.

Proposition 1 shows that all n^c-unique-**SVP**'s can be solved under GSA and the volume heuristics in polynomial time given a very short lattice vector.

5.3 Ajtai's worst case / average case equivalence. AJTAI [Aj96, Thm 1] solves every n^c-unique-**SVP** using an oracle that solves **SVP** for a particular random lattice. However, all n^c-unique-**SVP**'s are somewhat easy. This makes the worst case / average case equivalence suspicious.

[MR07] reduces n^c in Ajtai's reduction to $n \ln^{O(1)} n$.

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.

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

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

GN08 *N. Gama and P.Q. Nguyen*, Predicting lattice reduction, in Proc. EUROCRYPT 2008, LNCS 4965, Springer-Verlag, pp. 31–51, 2008.

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.

L86 *L. Lovász*, An Algorithmic Theory of Numbers, Graphs and Convexity, SIAM, 1986.

LM09 *V. Lubashevsky and D. Micciancio*, On bounded distance decoding, unique shortest vectors and the minimum distance problem. In Proc. CRYPTO 2009, LNCS 5677, Springer-Verlag, pp. 577–594, 2009.

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

M04 *D. Micciancio*, Almost perfect lattices, the covering radius problem, and applications to Ajtai's connection factor. SIAM J. on Computing, **37**(1), pp. 118–169, 2004.

MR07 *D. Micciancio and O. Regev*, Worst-case to average-case reduction based on gaussian measures. SIAM J. on Computing, **37**(1), pp. 267–302, 2007.

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

NS06 *P.Q. Nguyen and D. Stehlé*, LLL on the average. In Proc. of ANTS-VII, LNCS 4076, Springer-Verlag, 2006.

N10 *P.Q. Nguyen*, Hermite's Constant and Lattice Algorithms. in The LLL Algorithm, Eds. P.Q. Nguyen, B. Vallée, Springer-Verlag, Jan. 2010.

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, June 29–July 1, 2007, Final version in: The LLL Algorithm Survey and Applications. Eds. P.Q. Phong and B. Vallée, Springer Verlag, pp. 145–178, 2010.